

**TRUST NO
ONE,
ESPECIALLY
NOT US...
BECAUSE WE
KNOW THAT
NOTHING IS
TRULY
SECURITY**

Find more:
[BOOSTY.TV](#)
[SPONSR.RU](#)
[TELEGRAM](#)

Free Issue Section

The perfect starting point for those new to the world of cybersecurity without financial commitment.

Regular Issue Section

Tailored for regular readers who have a keen interest in security and wish to stay abreast of the latest trends and updates.

Pro Issue Section

Designed for IT pro, cybersecurity experts, and enthusiasts who seek deeper insights and more comprehensive resources.

SNARKY SECURITY

MONTHLY DIGEST. 2024 / 05

Welcome to the next edition of our Monthly Digest, your one-stop resource for staying informed on the most recent developments, insights, and best practices in the ever-evolving field of security. In this issue, we have curated a diverse collection of articles, news, and research findings tailored to both professionals and casual enthusiasts. Our digest aims to make our content both engaging and accessible. Happy reading!

Read more: [Boosty](#) | [Sponsr](#) | [TG](#)



SNARKY SECURITY



NEWS



FTC REFUNDS

❖ **FTC's Legal Action Against Ring:** The Federal Trade Commission (FTC) took legal action against Ring, a home security camera company owned by Amazon, for failing to protect consumer privacy. The FTC's complaint, filed in May 2023, accused Ring of allowing employees and contractors to access customers' private videos without consent and failing to implement adequate security measures. This negligence led to unauthorized access by hackers and employees, compromising the privacy and security of consumer video footage.

❖ **Settlement and Refunds:** As a result of the lawsuit, Ring agreed to a settlement that included a financial penalty and the establishment of a more robust privacy and security program. The FTC is distributing over \$5.6 million in refunds to approximately 117,044 affected Ring customers. These refunds are being issued via PayPal, and customers are advised to claim their payments within 30 days.

❖ **Details of the Settlement:** The settlement required Ring to pay \$5.8 million, delete unlawfully obtained videos, and implement stringent new privacy and security measures. These measures include multi-factor authentication and restrictions on employee access to consumer videos. The FTC emphasized that these steps were necessary to prevent future privacy breaches and to restore consumer trust in Ring's products.

❖ **Ring's Response:** Ring has stated that it addressed many of the FTC's concerns prior to the inquiry and disagreed with some of the allegations. However, the company chose to settle to avoid prolonged litigation and focus on enhancing its products and services for customers.

❖ **Consumer Information and Support:** Affected consumers can find more information about the refund process and eligibility on the FTC's website or by contacting the refund administrator, Rust Consulting. The FTC has made it clear that it never requires payment or account information for consumers to claim their refunds.



AI IN MILITARY AVIATION

The recent advancements in artificial intelligence (AI) have led to significant developments in the field of military aviation, particularly in the integration of AI with fighter jet operations.

❖ **AI Advancements in Military Aviation:** The Defense Advanced Research Projects Agency (DARPA) and the US Air Force have been at the forefront of integrating AI into fighter jets. This integration has reached a pivotal stage where AI-controlled jets, such as the X-62A VISTA, are now capable of engaging in dogfights with human-piloted jets.

❖ **First Successful AI vs. Human Dogfight:** In September 2023, a landmark event occurred when an AI-controlled X-62A VISTA engaged in a mock dogfight against a human-piloted F-16. This test, conducted at Edwards Air Force Base in California, marked the first successful in-air dogfight between an AI-controlled jet and a human pilot. The AI demonstrated the ability to perform complex combat maneuvers safely and effectively.

❖ **Safety and Control:** Despite the autonomous capabilities of the AI, human pilots were present on board the X-62A with controls to deactivate the AI system if necessary. However, during the tests, there was no need for human intervention, indicating a high level of reliability and safety in the AI's operational capabilities.

❖ **Implications for Future Combat:** The successful integration of AI into fighter jets is seen as a transformational moment in military aviation. It suggests a future where AI could potentially handle dynamic combat scenarios, allowing human pilots to focus on strategy and oversight rather than direct engagement.

❖ **Continued Development and Testing:** The ongoing development of AI in military aviation is focused on enhancing the capabilities of AI pilots, including their ability to make autonomous decisions in complex and rapidly changing combat environments. Future tests will likely explore more advanced scenarios and further refine the AI's decision-making processes.



CHANGE HEALTHCARE / UNITEDHEALTH GROUP UNDER RANSOMWARE ATTACK

Change Healthcare, a major player in the U.S. healthcare technology sector, has been grappling with significant cybersecurity challenges following a ransomware attack attributed to the BlackCat/ALPHV group.

❖ **Initial Attack and Ransom Payment:** Change Healthcare experienced a disruptive cyberattack on February 21, 2024, which led to widespread operational challenges across the U.S. healthcare system. The company, a subsidiary of UnitedHealth Group, ultimately paid a ransom of \$22 million to the BlackCat/ALPHV ransomware gang in hopes of restoring their services and securing patient data.

❖ **Subsequent Extortion Attempts:** Despite the initial ransom payment, Change Healthcare faced further extortion from a new ransomware group named RansomHub. This group claimed to possess four terabytes of data stolen during the initial BlackCat/ALPHV attack and demanded their own ransom, threatening to sell the information on the dark web if their demands were not met.

❖ **Impact on Healthcare Services:** The cyberattack severely impacted Change Healthcare's operations, affecting hospitals' ability to check insurance benefits, process patient procedures, and handle billing. Pharmacies also struggled with prescription charges due to inaccessible insurance information, significantly disrupting patient care and financial operations across healthcare providers.

❖ **Ongoing Data Breach Concerns:** There are ongoing concerns about the security of patient data handled by Change Healthcare. The company has not confirmed whether patient data was indeed stolen, but the potential for sensitive information being compromised remains a critical issue.

❖ **Government and Industry Response:** In response to the severity of the attack and its implications, the U.S. Department of State has offered a \$10 million reward for information leading to the identification or location of the members of the ALPHV/BlackCat gang.

❖ **Long-term Implications:** The attack on Change Healthcare highlights the broader vulnerabilities within the healthcare sector to ransomware attacks.



ARCANE DOOR

The ArcaneDoor cyber-espionage campaign, which began in November 2023, involved state-sponsored hackers exploiting two zero-day vulnerabilities in Cisco's Adaptive Security Appliance (ASA) and Firepower Threat Defense (FTD) firewalls.

◆ **Zero-Day Exploits Identified:** The hackers exploited two zero-day vulnerabilities, CVE-2024-20353 and CVE-2024-20359, which allowed for denial-of-service attacks and persistent local code execution, respectively.

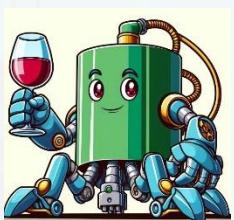
◆ **Sophisticated Malware Deployment:** The threat actors deployed two types of malwares, Line Dancer and Line Runner. Line Dancer is an in-memory shellcode loader that facilitates the execution of arbitrary shellcode payloads, while Line Runner is a persistent backdoor that enables the attackers to run arbitrary Lua code on the compromised systems.

◆ **Global Impact on Government Networks:** The campaign targeted government networks worldwide, exploiting the vulnerabilities to gain access to sensitive information and potentially conduct further malicious activities such as data exfiltration and lateral movement within the networks.

◆ **Response and Mitigation:** Cisco responded by releasing security updates to patch the vulnerabilities and issued advisories urging customers to update their devices, recommended monitoring system logs for signs of compromise such as unscheduled reboots or unauthorized configuration changes.

◆ **Attribution and Espionage Focus:** The hacking group, identified as UAT4356 by Cisco Talos and STORM-1849 by Microsoft, demonstrated a clear focus on espionage. The campaign is believed to be state sponsored, with some sources suggesting China might be behind the attacks.

◆ **Broader Trend of Targeting Network Perimeter Devices:** This incident is part of a larger trend where state-sponsored actors target network perimeter devices like firewalls and VPNs to gain initial access to target networks for espionage purposes



APT29

APT29, also known as Midnight Blizzard, BlueBravo, or Cozy Bear, has been identified using a new backdoor variant called WINELOADER to target German political parties. This campaign marks a shift in the group's focus from its traditional targets—diplomatic missions—to political entities, indicating a broader operational intent to gather political intelligence.

◆ **Target and Timing:** The campaign specifically targeted German political parties, with phishing emails sent around February 26, 2024. These emails featured a logo from the Christian Democratic Union (CDU) and included malicious links.

◆ **Technical Details:** WINELOADER is believed to be a variant of the non-public historic BURNTBATTER and MUSKYBEAT code families, which have been uniquely associated with APT29 by Mandiant. The malware employs sophisticated techniques such as DLL side-loading, RC4 encryption for payload decryption, and evasion tactics like process/DLL name checks and Ntdll usermode hook bypass.

◆ **Initial Access:** The initial access was achieved through phishing attachments leading to a compromised website, "waterforvoiceless[.]org," which hosted the ROOTSAW dropper. This dropper then facilitated the download and execution of the WINELOADER payload.

◆ **Operational Significance:** This shift to targeting political parties reflects growing interest in influencing or understanding Western political dynamics, especially in the context of ongoing geopolitical tensions. The targeting of political parties is seen as a strategic move to gather actionable intelligence that could potentially influence political outcomes or strategies in Europe and beyond.

◆ **Broader Implications:** The campaign against German political parties is not seen as an isolated incident but rather part of a broader strategy that could target other Western political entities.

EMPTY S3 BUCKET MAKES YOUR AWS BILL EXPLODE

The [article](#) discusses a significant issue where an empty, private AWS S3 bucket can lead to unexpectedly high AWS bills due to unauthorized incoming requests.

This case study serves as a cautionary tale about the potential financial risks associated with AWS services, particularly S3, and underscores the importance of understanding AWS billing practices and configuring AWS services securely to avoid unexpected charges.

◆ **Unexpected High Costs:** The author experienced a sudden spike in his AWS bill, amounting to over \$1,300, due to nearly 100,000,000 S3 PUT requests executed within a single day on an empty S3 bucket he had set up for testing.

◆ **Source of Requests:** Initially, AWS does not log requests executed against S3 buckets by default. The author had to enable AWS CloudTrail logs to identify the source of the requests. It was found that misconfigured systems were attempting to store data in his private S3 bucket.

◆ **Billing for Unauthorized Requests:** AWS charges for unauthorized incoming requests to S3 buckets. This was confirmed during the author's communication with AWS support, highlighting a critical billing policy where the bucket owner pays for incoming requests regardless of their authorization status.

◆ **Prevention and Protection:** The article notes that there is no straightforward way to prevent such incidents other than deleting the bucket. AWS does not allow the bucket to be protected by services like CloudFront or WAF when it is accessed directly through the S3 API.

◆ **AWS Investigation:** Following the incident, AWS began investigating the issue, as indicated by a tweet from Jeff Barr, a prominent AWS evangelist. This suggests that AWS is aware of the potential for such problems and may be considering ways to address them.





T-MOBILE AND VERIZON EMPLOYEES REPORT RECEIVING \$300 OFFERS FOR FACILITATING UNAUTHORIZED SIM SWAPS.

◆ **Bribery Offers to Telecom Employees:** T-Mobile and Verizon employees, including former staff, have reported receiving unsolicited messages offering \$300 for each SIM swap they facilitate. These messages were shared on Reddit, showcasing screenshots of the texts.

◆ **Method of Contact:** The attackers used various communication methods, including text messages and encrypted platforms like Telegram, to contact the employees. The messages often claimed to have obtained the employees' contact information from company directories.

◆ **Potential Insider Threats:** The situation raises concerns about insider threats within telecom companies, as the messages targeted current and former employees who might have access to the systems needed to execute SIM swaps.

◆ **Company Responses:** Both T-Mobile and Verizon are aware of these incidents. T-Mobile has stated that there was no system breach involved and that they are investigating the messages. Verizon's response is currently not detailed in the reports.

◆ **Impact of SIM Swapping:** SIM swapping can lead to significant security breaches, allowing attackers to bypass two-factor authentication, access personal and financial information, and potentially lead to financial fraud and identity theft.

◆ **Preventive Measures and Recommendations:** It is recommended that telecom companies enhance their internal security measures and employee verification processes to prevent such incidents. Employees are advised to report any suspicious activities and not engage with such offers.



MORE THAN 100 ARRESTED IN SPAIN IN \$900,000 WHATSAPP SCHEME

◆ Spanish police have arrested 34 individuals suspected of conducting various online scams, seizing firearms, a katana sword, a baseball bat, and €80,000 in the process.

◆ The alleged cybercriminals are accused of conducting scams via email, phone, and text, including "son in distress" scams and manipulation of delivery notes from technology companies.

◆ They are believed to have netted about €3 million and had access to a database with stolen information on four million people.

◆ The operation is part of a larger effort by Spanish law enforcement to crack down on cybercrime and scams.

◆ In a separate operation, Spanish police arrested 55 people involved in a wide-ranging cybercrime operation that involved phishing scams, SIM swapping, and more.

◆ This group, which called itself the "Black Panthers" and was based in Barcelona, operated in four separate cells that stole about €250,000 from nearly 100 people through a variety of scams that involved the takeover of bank accounts.

◆ Impersonation scams reported to the Federal Trade Commission cost victims about \$1.1 billion in 2023, more than three times what consumers reported in 2020.

◆ Of those reported cases in 2023, about 40 percent started online in one way or another, while a more traditional method — the scam phone call — accounted for 32 percent.

◆ Cybercriminals are targeting college students with fake job offers in the bioscience and health industries with the hope of extracting fees out of victims.

◆ Researchers at Proofpoint uncovered the campaign, which targeted university students in North America in May and June — graduation season — using job-themed scam emails.

◆ Deepfakes are adding an insidious edge to some sextortion schemes, according to a new alert from the FBI's Internet Crime Complaint Center (IC3).

◆ Some extortionists have resorted to using technology to create sexually explicit images or videos from otherwise benign content posted online.

◆ Hackers are targeting Asian bank accounts using stolen facial recognition data to bypass security measures.

◆ Spanish police arrested a 19-year-old suspected of carrying out a range of high-profile cyberattacks, calling him a "serious threat to national security"



IRANIAN STATE-BACKED CYBER SPIES

◆ **Impersonation Tactics:** APT42 has been impersonating well-known news outlets and think tanks, such as The Washington Post, The Economist, and The Jerusalem Post, to target journalists, researchers, and activists in Western countries and the Middle East. This campaign, which began in 2021 and is still ongoing, involves creating fake website links to harvest login credentials from victims.

◆ **Minimal Footprint:** The methods deployed by APT42 are designed to leave a minimal footprint, making the detection and mitigation of their activities more challenging for network defenders. This stealthiness is achieved through the use of typosquatting and social engineering techniques.

◆ **Typosquatting and Social Engineering:** APT42 often uses typosquatting, acquiring web domains that look real but contain small errors or alterations, to create malicious links. These links redirect recipients to fake Google login pages. An example provided is "washingtonpost[.]press," where a "q" replaces the "g" in "Washington".

◆ **Targeting Specific Individuals:** In 2023, APT42 reportedly impersonated a senior fellow with the U.K. think tank the Royal United Services Institute (RUSI) while attempting to spread malware to a nuclear security expert at a U.S.-based think tank focused on foreign affairs.

◆ **Cloud Environment Attacks:** Between 2022 and 2023, APT42 was observed exfiltrating documents and sensitive information from victims' public cloud infrastructure, such as the Microsoft 365 environment. These attacks targeted legal services companies and nonprofits in the U.S. and the U.K.

◆ **Overlap with Other Operations:** APT42's activities overlap with other Iran-linked operations labeled TA453, Charming Kitten, and Mint Sandstorm. This indicates a broader pattern of cyber espionage activities linked to Iranian state interests



ALLEGED CHINA-BASED HACKERS USING 'CUTTLEFISH' MALWARE PLATFORM TO TARGET TURKEY

◆ **Malware Identification and Activity:** The malware, identified as Cuttlefish, has been active since at least July 27, 2023, with the latest campaign running from October 2023 to April 2024. It is designed to infiltrate routers and other networking hardware to steal information quietly.

◆ **Geographical Focus and Victims:** The campaign has predominantly affected Turkey, with 99% of the infections occurring within the country. The remaining victims include global satellite phone providers and potentially a U.S.-based data center.

◆ **Connection to Chinese Operations:** Researchers at Black Lotus Labs suggest a link between Cuttlefish and the Chinese government due to significant overlaps with another malware called HiatusRat, which has been used in operations that align with Chinese interests.

◆ **Method of Operation:** Cuttlefish operates by capturing data from users and devices behind the targeted network's edge, allowing hackers to monitor all traffic through the compromised devices. It targets enterprise-grade small office/home office (SOHO) routers.

◆ **Data Theft:** The malware has been configured to steal keys for cloud-based services such as Alicloud, AWS, Digital Ocean, CloudFlare, and BitBucket. This enables the attackers to access data from cloud resources, which are typically less protected than traditional network perimeters.

◆ **Detection Challenges:** The nature of the attack, occurring over a trusted internal network, makes it particularly difficult to detect. Many security tools focus on external threats, thereby potentially overlooking such internally originated activities.

◆ **Broader Implications:** It highlights the evolving threat landscape where passive eavesdropping and data hijacking techniques are becoming more sophisticated. The specific targeting of cloud-based authentication material is a growing concern that requires enhanced security measures.



INVESTIGATION UNCOVERS SUBSTANTIAL SPYWARE EXPORTS TO INDONESIA

Spyware Capabilities:

◆ Spyware operations can be categorized into national in-house operations and commercial spyware sold for profit to government and private clients.

◆ Commercial spyware provides governments with advanced surveillance tools, enabling them to acquire capabilities they would otherwise struggle to obtain.

◆ The global spyware and digital forensics industry is booming, with at least 65 governments, both authoritarian and democratic, having contracted with commercial spyware vendors as of 2020.

◆ Spyware can be used to acquire sensitive data such as customers' full names, phone numbers, addresses, proprietary documentation, account numbers, card numbers, transaction histories, contracts, and passwords.

Acquisition Details:

◆ Chinese, Russian, and North Korean state-sponsored threat actors are behind most of the observed campaigns targeting various industries in Indonesia.

◆ In May 2023, the LockBit Ransomware group successfully compromised Bank Syariah Indonesia (BSI), a subsidiary of the state-owned enterprise Bank Mandiri, resulting in the acquisition of 1.5 terabytes of data.

◆ The global inventory of commercial spyware has seen a transition from older suppliers like FinFisher and Hacking Team to newer entrants such as NSO Group, Cytrox, and Candiru.

◆ The demand for spyware technology remains high, with government clients and private companies driving the market.

Investigation Progress:

◆ The European Parliament has set up a committee of inquiry to investigate the use of Pegasus and equivalent surveillance spyware.

◆ The investigation revealed that at least 70 governments worldwide have been targeted by commercial spyware, with over 180 journalists identified as targets.

◆ The investigation also found that there is a lot of surveillance industry activity in Cyprus involving the same actors that emerge in the spyware scandal.

◆ The investigation into the intrusion of Indonesian government networks by Mustang Panda, a Chinese threat actor, is ongoing, with authorities taking steps to identify and clean the infected systems. However, as of the last update, hosts inside Indonesian government networks were still communicating with the Mustang Panda malware servers.

OIL & GAS INDUSTRY UNDER CYBER-ATTACKS & GAMIFICATION



LNG systems are vulnerable to cyber-attacks due to intrinsic system risks, which include remotely managed third-party systems and vulnerable onboard technologies such as Programmable Logic Controllers (PLCs), Global Positioning System (GPS), and Automatic Identification System (AIS). These vulnerabilities could lead to overflowing fuel tanks, accidental release of LNG, and other risks that make LNG inaccessible or cause serious impacts when returned to its gaseous state.

In mid-February 2022, hackers gained access to computers belonging to current and former employees at nearly two dozen major natural gas suppliers and exporters, including Chevron Corp., Cheniere Energy Inc. and Kinder Morgan Inc. These attacks targeted companies involved with the production of liquefied natural gas (LNG) and were the first stage in an effort to infiltrate an increasingly critical sector of the energy industry.

Additionally, the FBI has warned the energy sector of a likely increase in targeting by Chinese and Russian hackers due to changes in the global energy supply chain. The alert cites factors such as increased US exports of LNG and ongoing Western pressure on Russia's energy supply but does not mention any specific attacks on LNG tankers.

Chevron Corp., Cheniere Energy Inc., and Kinder Morgan Inc. are all headquartered in the United States. Chevron's global headquarters are located in San Ramon, California, Cheniere Energy's headquarters are in Houston, Texas, and Kinder Morgan's headquarters are in Houston, Texas.

And now "We can't even build our own LNG tankers here in the United States"

In a delightful twist of irony, it turns out that not a single shipyard in the United States is capable of building LNG tankers, as admitted by US Navy Secretary Carlos Del Toro in his testimony before Congress on Wednesday. "We've lost this art here in the United States. We can't even build our own LNG tankers here, in the United States," Del Toro told the US House Armed Services Committee. According to shipbuilding records, the last time a US shipyard produced an LNG tanker was in 1980.

This revelation is a perfect example of the gamification of consciousness, where people focus on developing certain technologies to a certain level, then become complacent and neglect continuous improvement, research, and development. After all, why bother, since we've already achieved what we need? We've been trained by computer games, where once something is invented, it doesn't need to be reinvented. We level up our technology, bask in the glory, and then move on.

But then reality comes knocking, with its annoying habit of not following the rules of a game. Technologies can be forgotten and lost, progress can regress, and skilled workers can disperse and forget their skills. And if there's a 40-year gap between when a technology was last used and when it's decided to be revived, the principle of two dead generations comes into play. This principle states that 20-year-old engineers can be taught by 40-year-olds, but not by 60-year-olds. Even if someone who worked on technology in the 1980s is willing to teach, they may struggle to connect with the younger generation.

Cue the tears and cries of disbelief. "But I played on the computer, and it wasn't like this! It's too hard and confusing. Let's just pretend it's not true. After all, if the US could build a tanker or fly to the moon once, it must still be able to do so now. I believe it, and it's comforting and easy to believe it."



ARCHITECTURE OF NES CONSOLES

It seems you've traded the thrilling world of social interactions for the captivating realm of game console research. Let's dive into the depths of your newfound obsession called the Super Nintendo Entertainment System (SNES)? Fabien Sanglard, our hero, has meticulously dissected the SNES, offering us a trilogy of articles that could very well replace any human interaction.

First off, we have the exposé on SNES cartridges, those magical plastic blocks that, surprise, held more than just the dreams of 90s kids. They were technological marvels with their own hardware, including the oh-so-essential CIC copy protection chip.

Then, the author takes us on a historical journey through the evolution of the SNES motherboard. Twelve versions over twelve years, each one reducing the number of chips and components.

And let's not forget the heartwarming tale of the SNES's clock generators. These little timekeepers made sure everything ran like clockwork (pun absolutely intended). Because what's a gaming console without its precise timing to keep those tool-assisted speedruns accurate? It's not like gamers have anything better to do, like, say, going outside.

So, there you have it, a trilogy of articles that could very well serve as a substitute for human interaction. Who needs friends when you have the intricate details of the SNES to keep you warm at night? Thank you, Fabien Sanglard, for giving us the perfect excuse to avoid social obligations in favor of gaming console research.

SNES Cartridges:

The SNES cartridges were unique in that they could include additional hardware such as the CIC copy protection chip, SRAM, and enhancement processors like the "Super Accelerator 1" (SA-1). These processors significantly boosted the console's capabilities, allowing for advanced graphics and gameplay features. It highlights the evolutionary steps Nintendo took with the SNES motherboard to enhance the system's efficiency and cost-effectiveness over time.

Key Features

- ❖ The SNES motherboard underwent significant changes throughout its production, primarily aimed at reducing the complexity and cost of the system.
- ❖ The motherboard started with a high number of chips and components which were gradually reduced in later versions.

Chip Reduction

❖ One of the major advancements in the SNES motherboard design was the introduction of the 1-CHIP version. This version consolidated the CPU and the two PPUs (Picture Processing Units) into a single ASIC (Application-Specific Integrated Circuit), reducing the total number of chips on the motherboard to nine.

- ❖ This reduction not only simplified the design but also potentially improved the system's reliability and performance.

Motherboard Versions

- ❖ Over its 12-year lifespan, Nintendo released twelve different versions of the SNES motherboard.

◆ These versions include various models like SHVC-CPU-01, SNS-CPU-GPM-01, and SNS-CPU-1CHIP-01 among others, each corresponding to different production years and design tweaks.

◆ The versions are categorized into four major generations: Classic, APU, 1-CHIP, and Junior, with the 1-CHIP and Junior versions representing the most significant redesigns.

◆ The Super Nintendo Jr (also known as Mini) is noted as the final form of the SNES, maintaining the reduced chip count and featuring a more integrated design where the motherboard no longer has parts dedicated to specific subsystems.

Evolution of the SNES Motherboard:

Over its 12-year lifespan, Nintendo released twelve versions of the SNES motherboard, each reducing the number of chips and components. The most notable advancement was the 1-CHIP version, which integrated the CPU and two PPUs into a single ASIC, simplifying the design and potentially enhancing performance. It sheds light on the technical marvels and challenges of the SNES cartridge system, highlighting how Nintendo leveraged additional hardware within cartridges to push the boundaries of what was possible in video gaming during the era

Enhancement Processors

◆ SNES cartridges were notable for their ability to include more than just game instructions and assets. They could also house additional hardware components such as the CIC copy protection chip, SRAM, and enhancement processors.

◆ These enhancement processors, such as the "Super Accelerator 1" (SA-1) chip, significantly boosted the SNES's capabilities. The SA-1 chip, found in 34 cartridges, was a 65C816 CPU running at 10.74 MHz—four times faster than the SNES's main CPU. It also included 2KiB of SRAM and an integrated CIC.

Copy-Protection Mechanism

◆ The SNES utilized a copy-protection mechanism involving two CIC chips that communicated in lockstep—one in the console and the other in the cartridge. If the console's CIC detected an unauthorized game, it would reset every processor in the system.

◆ Some unsanctioned games, like "Super 3D Noah's Ark," bypassed this protection by requiring an official cartridge to be plugged on top of them, using the official game's CIC to authenticate.

Game Enhancements

◆ The inclusion of enhancement processors allowed for significant improvements in game performance and graphics. For example, the SA-1 chip enabled the SNES to animate and detect collisions on all 128 sprites available in the PPU, transform sprites on the fly (rotate/scale), and write them back into the PPU VRAM.

◆ Another enhancement chip, the Super-GFX, excelled at rendering pixels and rasterizing polygons, usually rendering into a framebuffer located on the cartridge. This content was then transferred to the VRAM during VSYNC.

Regional Compatibility and Circumvention

◆ The article also touches on the physical and electronic measures Nintendo used to enforce regional compatibility, such as the different shapes of cartridges and the CIC lockout system. However, it mentions that these measures were not foolproof and could be circumvented.

Community and Development Insights

◆ Discussions on platforms like Hacker News reflect on the impact and potential of these cartridges, comparing them to other Nintendo innovations and discussing the technical challenges and solutions provided by the SNES's design

Clock Generators in the SNES:

The SNES utilized two main clock generators to manage the timing for its various components. These clocks were crucial for the operation of the CPU, PPU, and APU. The system also included enhancement chips in some cartridges, which used these clocks for additional processing power, exemplified by the SuperFX chip used in games like StarFox. This detailed examination of the SNES's clock system reveals the intricate design and engineering that supported the console's complex graphics and audio capabilities, allowing for advanced gaming experiences during its era.

Clock Generators

◆ The SNES motherboard features two primary clock generators located in the X2 and X1 slots.

◆ The X2 slot houses a 24.576 MHz ceramic resonator, which is blue in color. This resonator is crucial for the operation of the Audio Processing Unit (APU), setting the pace for audio processing on the SNES.

◆ The X1 slot contains a 21.300 MHz oscillator, labeled D21L3, which is yellow. This oscillator is strategically placed near the CPU and the Picture Processing Unit (PPU), thereby setting their operational pace.

Clock Distribution and Enhancement Chips

◆ The SNES utilizes these master clocks in conjunction with dividers to generate additional clocks needed by various components. For instance, the Ricoh 5A22 CPU operates at 1/6th the frequency of the master clock, resulting in a frequency of 3.579545 MHz.

◆ The system includes a total of fifteen different clocks, highlighting the complex timing management within the SNES.

◆ The SYS-CLK line, which runs at 21.47727 MHz, is routed to the cartridge port. This setup is not typically necessary for the basic operation of the cartridges, which contain ROM with game data and instructions. However, this clock signal is crucial for cartridges that contain their own enhancement processors, like the SuperFX chip used in games such as StarFox.

◆ These enhancement chips can utilize the SYS-CLK for additional processing power, with some chips like the MARIO version of the SuperFX processor using an internal divider to adjust the clock frequency to suit specific processing needs.

Impact on Game Performance

- ❖ The precision of these clock generators is vital for the deterministic execution of game code, which is particularly important for applications like tool-assisted speedruns (TAS). Over time, the accuracy of ceramic resonators can degrade, leading to performance inconsistencies



ARCHITECTURE OF CONSOLES: A PRACTICAL ANALYSIS

Rodrigo Copetti's series of books, "Architecture of Consoles: A Practical Analysis," dives deep into the fascinating world of video game consoles, uncovering the secrets behind their mind-boggling technology. But let's be honest, who needs a social life when you can spend your time dissecting the inner workings of these magical boxes, right?

In this series, the author takes us on a wild ride through the evolution of consoles, proving that they're more than just a bunch of numbers and fancy jargon. From the Nintendo 3DS to the Xbox and PlayStation series, these books show that consoles are like snowflakes — each one is unique and special in its own way.

So, if you're ready to trade your social life for a deep dive into the mesmerizing world of console architecture, Copetti's books are just the ticket. They're a treasure trove of technical knowledge, perfect for anyone who's ever wondered what makes these magical boxes tick.

These books are part of a series on console architecture, and it is structured similarly to his previous work on the PS3's architecture. This allows readers who are familiar with the PS3's architecture to compare the two consoles side-by-side. Books on console architecture, including "PlayStation 3 Architecture", are targeted towards individuals with a basic knowledge of computing who are interested in the evolution and internal workings of video game consoles. His writings are not developer manuals but rather in-depth introductions to how each system works internally. He tries to adapt his content for wider audiences, so even those without a deep understanding of computing can still find value in his work. His books are appreciated by both technical and non-technical readers for their in-depth yet accessible explanations of complex console architectures. Therefore, his target audience can be considered quite broad, encompassing anyone from casual readers with an interest in technology to professionals in the gaming industry, computer engineers, and enthusiasts of console gaming and hardware.

Some other books by this author

- ❖ NES Architecture: More than a 6502 machine
- ❖ Game Boy Architecture
- ❖ Super Nintendo Architecture
- ❖ PlayStation Architecture
- ❖ Nintendo 64 Architecture
- ❖ GameCube Architecture
- ❖ Wii Architecture
- ❖ Nintendo DS Architecture
- ❖ Master System Architecture

Xbox Original

If you are not familiar with Xbox original, it's suggested to start with reading Xbox Arch before Xbox 360. "Xbox Architecture" The book provides an in-depth look at the console's architecture, focusing on its unique features and the technological innovations that set it apart from its competitors. The book begins by discussing the historical context of the Xbox's development, noting that Microsoft aimed to create a system that would be appreciated by developers and welcomed by users due to its familiarities and online services.

❖ **One of the main topics covered in the book is the Xbox's CPU.** The console uses a slightly customized version of the Intel Pentium III, a popular off-the-shelf CPU for computers at the time, running at 733 MHz. The book explores the implications of this choice and how it contributes to the overall architecture of the Xbox.

❖ **The book also delves into the Graphics of the Xbox.** It uses a custom implementation of Direct3D 8.0, which was extended to include Xbox-specific features. This allowed PC developers to port their games to the Xbox with minimal changes

❖ **The Development Ecosystem of the Xbox is another key topic covered in the book.** Game development on the Xbox is complex, with various libraries and frameworks interacting with the console's hardware. The book provides a detailed analysis of this ecosystem, helping readers understand the intricacies of game development on the Xbox

❖ **The Network Service of the Xbox is also discussed.** The Xbox included an Ethernet connection and a centralized online infrastructure called Xbox Live, which were innovative features at the time. The book explores how these features contribute to the overall architecture of the Xbox

❖ **Finally, the book also covers the Security aspects of the Xbox, including its anti-piracy system.** It explains how this system works and how it fits into the console's overall architecture

Xbox Original Architecture quick facts

- ❖ The original Xbox used a familiar system for developers and online services for users
- ❖ The Xbox CPU is based on Intel's Pentium III with the P6 microarchitecture
- ❖ The console has 64 MiB of DDR SDRAM, which is shared across all components
- ❖ The Xbox GPU is manufactured by Nvidia and is called the NV2A
- ❖ The original Xbox controller, called The Duke, was replaced with a new revision called Controller S due to criticism

Xbox 360

The book “Xbox 360 Architecture: A Supercomputer for the Rest of Us” provides an in-depth analysis of the Xbox 360’s architecture, discussing its design, capabilities, and the technological innovations it introduced and, explaining how the console works internally. It is a valuable resource for anyone interested in the evolution of gaming console technology. The book is part of the “Architecture of Consoles: A Practical Analysis” series, which looks at the evolution of video game consoles and their unique ways of working.

The book begins with a brief history of the Xbox 360, which was released a year before its main competitor, the PlayStation 3. It discusses the business aspect of the Xbox 360’s CPU and the sequence of events that led to its development.

The book then delves into the technical aspects of the Xbox 360’s architecture. It discusses the console’s CPU, which was a significant departure from the single-core CPU used in the original Xbox. The Xbox 360’s CPU, known as Xenon, was a triple-core processor designed by IBM. Each core was capable of handling two threads simultaneously, allowing up to six threads to be processed at once.

The book also discusses the Xbox 360’s GPU, known as Xenos, which was designed and manufactured by ATI. The GPU was based on a new architecture and could deliver 240 GFLOPS of performance. The Xenos GPU introduced the concept of a unified shader pipeline, which combined two different dedicated pipelines for increased performance.

The book further discusses the Xbox 360’s main memory, which was a significant increase over the original Xbox’s 64 MB. This allowed for more complex games and applications to be run on the console.

The book also covers the Xbox 360’s operating system, development ecosystem, and network service. It discusses how the console’s architecture was designed to be flexible and easy to program for, with a balanced hardware architecture that could adapt to different game genres and developer needs.

The main topics covered in the book include:

- ❖ **CPU:** The book delves into the details of the Xbox’s CPU, discussing its unique features and how it compares to the CPUs of other consoles. It also provides a historical context, explaining how the CPU’s design was influenced by the technological trends and challenges of the time
- ❖ **Graphics:** The book provides a detailed analysis of the Xbox’s graphics capabilities, including its use of a semi-customised version of Direct3D 9 and how this influenced future revisions of Direct3D
- ❖ **Security:** The book discusses the Xbox’s anti-piracy system, explaining how it works and how it contributes to the console’s overall architecture
- ❖ **Development Ecosystem:** The book explores the complexities of game development on the Xbox, discussing the various libraries and frameworks used and how they interact with the console’s hardware
- ❖ **Network Service:** The book also covers the Xbox’s online capabilities, discussing its Ethernet connection and the Xbox Live online infrastructure

Xbox 360 Architecture quick facts

- ❖ The Xbox 360 was released a year before its main competitor, the PS3
- ❖ The Xbox 360’s CPU, called Xenon, is a multi-core processor developed by IBM
- ❖ The console uses a semi-customized version of Direct3D 9 for its GPU, called Xenos
- ❖ The Xbox 360 has a unified memory architecture with 512 MB of GDDR3 RAM

PS2

“PlayStation 2 Architecture” provides an in-depth analysis of the PlayStation 2 console’s internal workings. Despite not being the most powerful console of its generation, the PlayStation 2 achieved a level of popularity that was unthinkable for other companies. The book explains that the PlayStation 2’s success was due to its Emotion Engine, a powerful package designed by Sony that ran at ~294.91 MHz. This chipset contained multiple components, including the main CPU and other components designed to speed up certain tasks. The book also discusses the PlayStation 2’s operating system, which relied on the Image Processing Unit (IPU) for DVD playback and compressed High-resolution textures. The PlayStation 2’s development ecosystem is also covered, with Sony providing the hardware and software to assist game development

PS2 Architecture quick facts

- ❖ The PlayStation 2 (PS2) was not the most powerful console of its generation but achieved immense popularity
- ❖ The Emotion Engine (EE) is the heart of the PS2, running at ~294.91 MHz and containing multiple components, including the main CPU
- ❖ The main core is a MIPS R5900-compatible CPU with various enhancements
- ❖ The PS2 uses Vector Processing Units (VPUs) to enhance its processing capabilities
- ❖ The console has backward compatibility with the original PlayStation through the use of an I/O Processor (IOP)
- ❖ The PS2 introduced the DualShock 2 controller, which featured two analog sticks and two vibration motors
- ❖ The operating system of the PS2 is stored on a 4 MB ROM chip

PS3

“PlayStation 3 Architecture” offers a comprehensive analysis of the PlayStation 3 console’s internal structure. The book explains that the PlayStation 3’s underlying hardware architecture continues the teachings of the Emotion Engine, focusing on vector processing to achieve power, even at the cost of complexity. The PlayStation 3’s CPU, the Cell Broadband Engine, is a product of a crisis of innovation and had to keep up as trends for multimedia services evolved. The book also discusses the PlayStation 3’s main memory and the Synergistic Processor Element (SPE), which are accelerators included within the PS3’s Cell. The PlayStation 3 also contains a GPU chip manufactured by Nvidia, called Reality Synthesizer or ‘RSX’, which runs at 500 MHz and is designed to offload part of the graphics pipeline

PS3 Architecture quick facts

- ❖ The PS3 focuses on vector processing to achieve power, even at the cost of complexity
- ❖ The Cell Broadband Engine is the main processor of the PS3, developed jointly by Sony, IBM, and Toshiba
- ❖ The PS3's CPU is massively complex and features a Power Processing Element (PPE) and multiple Synergistic Processor Elements (SPEs)
- ❖ The PS3 uses a GPU chip called Reality Synthesizer (RSX) manufactured by Nvidia

There are several notable differences in architectures are discussed in the books

Xbox 360 and Xbox Original

- ❖ **CPU:** The original Xbox relied on popular off-the-shelf stock (Intel's Pentium III) with slight customizations. This was a single-core CPU extended with vectorized instructions and a sophisticated cache design. On the other hand, the Xbox 360 introduced a new type of CPU that was unlike anything seen on the store shelves. This was a multi-core processor developed by IBM, reflecting an obsessive need for innovation characteristic of the 7th generation of consoles
- ❖ **GPU:** The original Xbox's GPU was based on the NV20 architecture, with some modifications to work in a unified memory architecture (UMA) environment. The Xbox 360, however, used a semi-customized version of Direct3D 9 for its GPU, called Xenos
- ❖ **Memory:** The original Xbox included a total of 64 MiB of DDR SDRAM, which was shared across all components of the system. The Xbox 360, on the other hand, had a unified memory architecture with 512 MB of GDDR3 RAM
- ❖ **Development Ecosystem:** The original Xbox was designed with familiarities appreciated by developers and online services welcomed by users. The Xbox 360, however, was designed with an emphasis on the emerging 'multi-core' processor and unorthodox symbiosis between components, which enabled engineers to tackle unsolvable challenges with cost-effective solutions
- ❖ **Release Timing:** The Xbox 360 was released a year before its main competitor, the PlayStation 3, and was already claiming technological superiority against the yet-to-be-seen PlayStation 3

PS2 and PS3:

- ❖ **CPU:** The PS2's Emotion Engine was designed by Toshiba, using MIPS technology, and focused on achieving acceptable 3D performance at a reduced cost. In contrast, the PS3's CPU, the Cell Broadband Engine, was developed through a collaboration between Sony, IBM, and Toshiba, and is a highly complex and innovative processor that intersects complex needs and unusual solutions
- ❖ **GPU:** The PS2's GPU, the Graphics Synthesizer, was a fixed-functionality GPU designed for 3D performance. The PS3's GPU, the Reality Synthesizer (RSX), was manufactured by Nvidia and was designed to offload part of the graphics pipeline, offering better parallel processing capabilities
- ❖ **Memory:** The PS2 had 32 MB of RDRAM, while the PS3 had a more advanced memory system, with 256 MB of XDR DRAM for the CPU and 256 MB of GDDR3 RAM for the GPU.
- ❖ **Development Ecosystem:** The PS2's development ecosystem was based on MIPS technology and focused on achieving acceptable 3D performance at a reduced cost. The PS3's development ecosystem was more complex, involving collaboration between Sony, IBM, and Toshiba, and focused on creating a powerful and innovative system
- ❖ **Backward Compatibility:** The PS2 was backward compatible with PS1 games through the inclusion of the original PS1 CPU and additional hardware components. The PS3 also offered backward compatibility with PS2 games, but this was achieved through software emulation in later revisions of the console

PS2 and Xbox Original:

- ❖ **CPU:** The PS2's Emotion Engine was designed by Toshiba, using MIPS technology, and focused on achieving acceptable 3D performance at a reduced cost. In contrast, the Xbox Original's CPU was based on Intel's Pentium III, which was a popular off-the-shelf stock with slight customizations
- ❖ **GPU:** The PS2's GPU, the Graphics Synthesizer, was a fixed-functionality GPU designed for 3D performance. The Xbox Original's GPU was based on the NV20 architecture, with some modifications to work in a unified memory architecture (UMA) environment
- ❖ **Memory:** The PS2 had 32 MB of RDRAM, while the Xbox Original included a total of 64 MiB of DDR SDRAM, which was shared across all components of the system
- ❖ **Development Ecosystem:** The PS2's development ecosystem was based on MIPS technology and focused on achieving acceptable 3D performance at a reduced cost. The Xbox Original was designed with familiarities appreciated by developers and online services welcomed by users

PS3 and Xbox 360:

- ❖ **CPU:** The PS3's CPU, the Cell Broadband Engine, is a highly complex and innovative processor that intersects complex needs and unusual solutions. It was developed through a collaboration between Sony, IBM, and Toshiba. On the other hand, the Xbox 360's CPU, Xenon, was a new type of CPU that was unlike anything seen on the store shelves. It reflects an obsessive need for innovation, a peculiar trait of that era
- ❖ **GPU:** The PS3's GPU, the Reality Synthesizer or 'RSX', was manufactured by Nvidia and was designed to offload part of the graphics pipeline. The Xbox 360's GPU, Xenos, was a semi-customised version of Direct3D 9 that makes room for the extra functions of Xenos
- ❖ **Memory:** The PS3's memory was distributed across different memory chips, and while it didn't implement a UMA architecture, it could still distribute graphics data across different memory chips if programmers decide to do so.
- ❖ **Development Ecosystem:** The PS3's development ecosystem was based on the Cell Broadband Engine, a joint project between Sony, IBM, Toshiba, and Nvidia. The Xbox 360's development ecosystem was based on the Xenon CPU and the semi-customized version of Direct3D 9

Read more: [Boosty](#) | [Sponsr](#) | [TG](#)



SNARKY SECURITY

CONTENTS



MEDICAL SECURITY



Let's all take a moment to appreciate the marvels of integrating Internet of Things (IoT) devices into healthcare. What could possibly go wrong with connecting every conceivable medical device to the internet? Pacemakers, MRI machines, smart infusion pumps - it's like every device is screaming, "Hack me, please!"

As we dive into the abyss of cybersecurity threats, let's not forget the sheer brilliance of having your heart's pacing dependent on something as stable and secure as the internet. And who could overlook the excitement of having your medical data floating around in the cloud, just a breach away from becoming public knowledge? But wait, there's more! Compliance with HIPAA and adherence to best practices will magically ward off all cyber threats. Because hackers totally play by the rules and are definitely deterred by a healthcare organization's best intentions.

The ripple effects of a cyber-attack on medical technology affect not just healthcare providers but also dragging down insurance companies, pharmaceuticals, and even emergency services into the mire. Hospitals in chaos, treatments delayed, and patient safety compromised - it's the perfect storm. But let's not forget the unsung heroes: cybersecurity firms, rubbing their hands in glee as the demand for their services skyrockets.

Welcome to the future of healthcare, where your medical device might just be part of the next big data breach headline. Sleep tight!



Another blockchain solution to solve all our healthcare woes. Because, you know, what the healthcare industry has been desperately missing is more buzzwords like "dual-blockchain architecture" and "attribute-based encryption." Who wouldn't sleep better knowing their sensitive medical data is bouncing around on not one, but two blockchains? It's like double the security blanket, or double the headache, depending on how you look at it. Let's not forget the pièce de résistance: AI integration. Because nothing says "trustworthy and secure" like throwing artificial intelligence into the mix.

And then there's the real-time monitoring feature because constant surveillance is exactly what we all need for peace of mind. Nothing screams "privacy" like having every heartbeat and blood pressure reading recorded on an immutable ledger. The system promises "decentralization," the magical word that apparently solves unauthorized data tampering. Because as we all know, decentralization has made cryptocurrencies such as Bitcoin completely immune to fraud and theft...

In all seriousness, patent CN111913833A does aim to tackle genuine issues in the healthcare sector, such as data breaches and the lack of standardized protocols for secure data exchange. However, one can't help but approach it with a healthy dose of skepticism. After all, if history has taught us anything, it's that technology is only as good as its implementation and the humans behind it. So, here's to hoping that this blockchain-based transaction system for the medical Internet of Things is more than just another buzzword bingo winner.



PATENT US11483343B2

Ah, behold the marvel that is US11483343B2, a patent that boldly claims to revolutionize the fight against the digital age's oldest trick: phishing. Because, of course, what we've all been missing is yet another "advanced" system promising to save us from the nefarious links lurking in our inboxes. This patent, with its grandiose title "Phishing Detection System and Method of Use," introduces a supposedly novel architecture designed to sniff out phishing attempts by scanning messages for suspicious URLs. Groundbreaking, isn't it?

And so, we arrive at the pièce de résistance: a multi-stage phishing detection system that not only scans messages but also resolves URLs, extracts webpage features, and employs machine learning to distinguish friend from foe. A solution so advanced, it almost makes one wonder how we ever managed to survive the internet without it. While it boldly strides into the battlefield of cybersecurity, one can't help but ponder the performance and accuracy challenges that lie ahead in the ever-evolving phishing landscape.

PATENT US11496512B2

Let's dive into the thrilling world of patent of Lookout, Inc., a masterpiece ingeniously titled "Detecting Real time Phishing from a Phished Client or at a Security Server." Because, you know, the world was desperately waiting for another patent to save us from the clutches of phishing attacks.

In a world teeming with cyber security solutions, our valiant inventors have emerged with a groundbreaking method: inserting an encoded tracking value (ETV) into webpages. This revolutionary technique promises to shield us from the ever-so-slight inconvenience of phishing attacks by tracking our every move online. How comforting!





DATABRICKS AI SECURITY FRAMEWORK (DASF)

The Databricks AI Security Framework (DASF), oh what a treasure trove of wisdom it is, bestows upon us the grand illusion of control in the wild west of AI systems. It's a veritable checklist of 53 security risks that could totally happen, but you know, only if you're unlucky or something.

❖ **Security Risks Identification:** Here, we'll pretend to be shocked at the discovery of vulnerabilities in AI systems. It's not like we ever thought these systems were bulletproof, right?

❖ **Control Measures:** This is where we get to play hero by implementing those 53 magical steps that promise to keep the AI boogeyman at bay.

❖ **Deployment Models:** Explore the various ways AI can be unleashed upon the world, because why not make things more complicated?

❖ **Integration with Existing Security Frameworks:** Reinventing the wheel is so last millennium, we'll see how DASF plays nice with other frameworks.

❖ **Practical Implementation:** This is where we roll up our sleeves and get to work, applying the framework with the same enthusiasm as a kid doing chores.

And why, you ask, is this analysis a godsend for security professionals and other specialists? Well, it's not like they have anything better to do than read through another set of guidelines, right? Plus, it's always fun to align with regulatory requirements.

In all seriousness, this analysis will be as beneficial as a screen door on a submarine for those looking to safeguard their AI assets. By following the DASF, organizations can pretend to have a handle on the future, secure in the knowledge that they've done the bare minimum to protect their AI systems from the big, bad world out there.



PATENT US11611582B2

The patent US11611582B2 has bestowed upon us a computer-implemented method that uses a pre-defined statistical model to detect phishing threats. Because, you know, phishing is such a novel concept that we've never thought to guard against it before.

This method, a dazzling spectacle of machine learning wizardry, dynamically analyzes network requests in real-time. It's not just any analysis, though—it's proactive! That means it actually tries to stop phishing attacks before they happen, unlike those other lazy methods that just sit around waiting for disaster to strike.

When a network request graciously makes its way to our system, it must first reveal its secrets—things like the fully qualified domain name, the domain's age (because older domains clearly have more wisdom), the domain registrar, IP address, and even its geographic location. Because obviously, geographic location is crucial. Everyone knows that phishing attacks from scenic locations are less suspicious.

These juicy details are then fed to the ever-hungry, pre-trained statistical model, which, in its infinite wisdom, calculates a probability score. This score, a beacon of numerical judgment, tells us the likelihood that this humble network request is ..., a.k.a. a phishing threat.

And should this score dare exceed the sanctity of our pre-defined threshold—an arbitrary line in the cyber sand—an alert is generated. Because nothing says "I'm on top of things" like a good old-fashioned alert.

This statistical model isn't some static relic; it's a living, learning creature. It's trained on datasets teeming with known phishing and non-phishing examples and is periodically updated with fresh data to keep up with the ever-evolving fashion trends of phishing attacks.

Truly, we are blessed to have such an innovative tool at our disposal, tirelessly defending our digital realms from the ceaseless onslaught of phishing attempts. What would we do without it? Probably just use common sense, but where's the fun in that?



PATENT US9071600B2

The patent US9071600B2 is a delightful example of innovation, where it introduces a method to prevent phishing and online fraud by establishing a VPN tunnel between a user computer and a server. This patent ensures that the user's data is as secure as a squirrel's nut in winter. It's a marvel how it uses such a complex technology like a VPN, which is as old as the internet itself, to create a secure communication channel. This method is not just about securing data but also about authenticating entities and separating internal networks from external threats, which is surely something the world has never seen before.

The patent details various operations such as the use of hyperlinks, webpages, and servers to create a fortress of digital security. It's almost as if the patent has rediscovered the wheel in terms of online security, providing a shield against the nefarious acts of cyber villains.

In essence, US9071600B2 is not just a patent; it's a beacon of hope in the dark world of cyber threats, standing tall like a lighthouse guiding the lost ships in a stormy sea of data breaches and online frauds. Truly, a masterpiece of modern technology, wrapped in the cloak of VPNs and network security protocols!

Read more: [Boosty](#) | [Sponsr](#) | [TG](#)

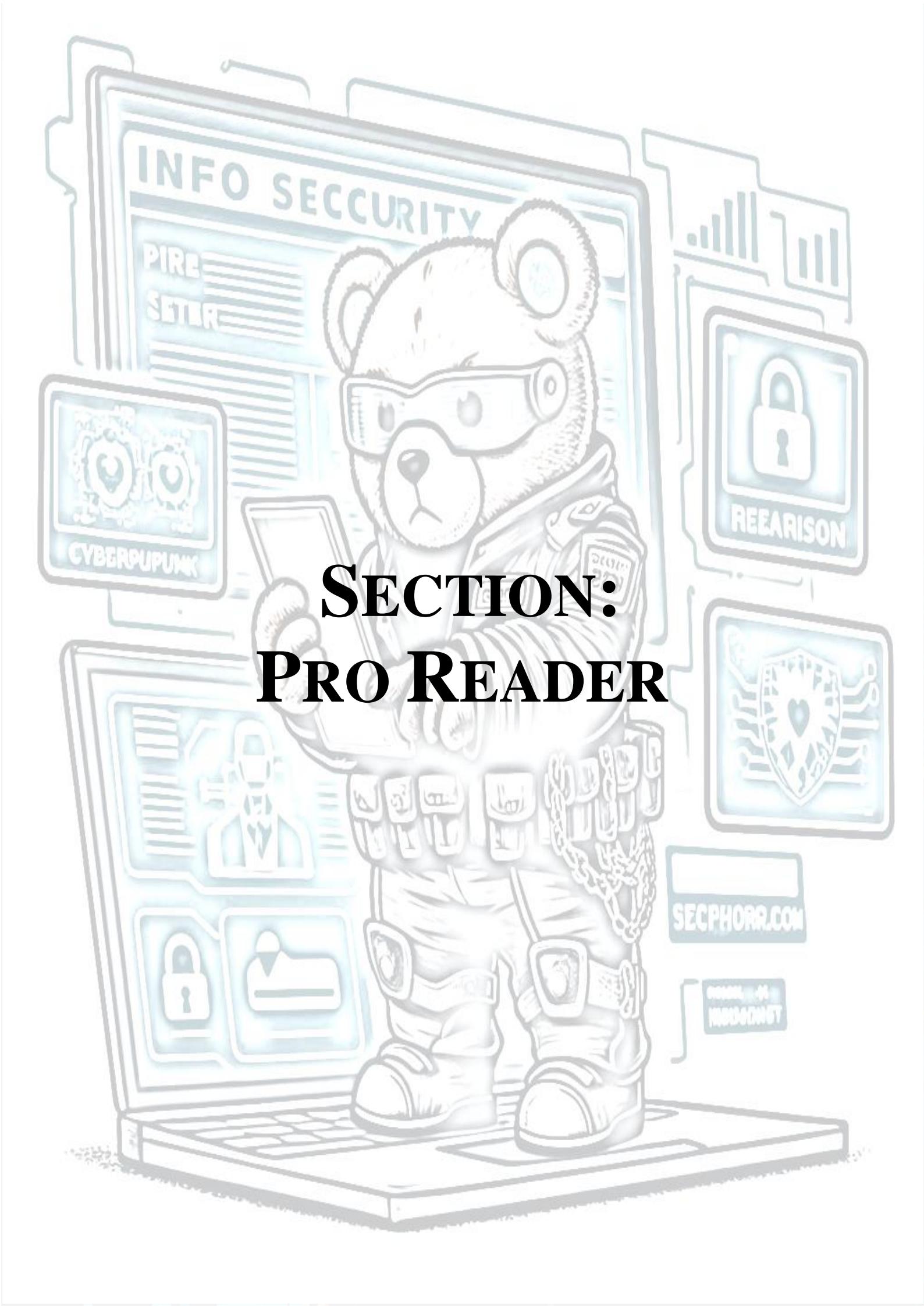


AIRCRAFT

Another thrilling read from the Department of the Army, hot off the presses in August 2023. "Counter-Unmanned Aircraft System (C-UAS)" – what we all need is a deeper dive into the riveting world of thwarting drones. This document, a sequel to its 2017 predecessor, promises to be the blockbuster of military literature, guiding soldiers in the art of playing with enemy drones.

It kicks off with a promise to enlighten military forces on how to give those pesky unmanned aircraft systems (UASs) a really bad day. Covering everything from the ABCs of threat UASs to the XYZs of knocking them out of the sky, it's essentially a how-to guide for ruining a drone's mission – and possibly its day.

The document is a must-read for anyone passionate about military strategy, drones, or just having a lot of time on their hands. It's packed with action, adventure, and appendices, making it the perfect addition to any security professional's bookshelf or as a makeshift doorstop.



SECTION: PRO READER

MEDICAL SECURITY





Abstract – This document highlights the cyber threats to medical technology and communication technology protocols and outlines the potential risks and vulnerabilities in these systems. It is designed to help healthcare organizations and medical professionals understand the importance of securing their technology systems to protect patient data and ensure the continuity of care.

A. Introduction

The integration of Internet of Things (IoT) devices in the healthcare and public health sectors has brought about significant advancements in patient care and operational efficiency. However, these benefits come with a set of cybersecurity challenges and threats that need to be addressed to protect sensitive health information and ensure the continuity of healthcare services. Here's a comprehensive overview of the cybersecurity threats in these sectors, focusing on devices like pacemakers, smart infusion pumps, MRI machines, and the broader implications for medical technology and communication protocols.

The security of digital technologies in the healthcare and public health sector is paramount for protecting patient safety, privacy, and the integrity of medical services. Healthcare organizations must adopt a comprehensive approach to data security, network security, and device security, implementing encryption, secure communication protocols, and robust network and device security measures. Compliance with HIPAA regulations and adherence to best practices and standards, such as those provided by CISA, HHS, and DICOM, are essential for mitigating cyber threats and ensuring the secure use of digital technologies in healthcare.

B. Industries

Cyber-attacks on medical technology can affect a wide range of industries beyond the immediate healthcare sector. The ripple effects of a cyber-attack on medical technology can extend far beyond the immediate healthcare sector, impacting a

wide array of industries and services that are interconnected with healthcare delivery and operations.

- **Healthcare Providers:** Hospitals, clinics, and private practices rely on medical technology for patient care. Cyber-attacks can disrupt clinical operations, delay treatments, and compromise patient safety.
- **Healthcare Technology Companies:** Firms that develop and maintain medical software and devices can suffer from intellectual property theft, loss of customer trust, and financial losses due to cyber-attacks.
- **Insurance Companies:** Insurers may face claims related to cyber-attacks on medical technology, including costs associated with data breaches, system restoration, and liability claims.
- **Pharmaceuticals and Biotech:** These industries rely on medical data for research and development. Cyber-attacks can lead to the loss of proprietary research data and disrupt the supply chain for critical medications.
- **Healthcare IT Services:** Companies providing IT support and services to healthcare organizations can be indirectly affected by cyber-attacks on their clients, leading to reputational damage and financial losses.
- **Government and Regulatory Bodies:** Government health agencies and regulatory bodies may need to respond to cyber-attacks on medical technology, affecting public health and potentially leading to regulatory changes.
- **Emergency Services:** Cyber-attacks that disrupt medical technology can lead to delays in emergency response and patient transfers, affecting ambulance services and emergency medical care.
- **Legal and Compliance Services:** Law firms and compliance consultants may see an increase in demand for their services as healthcare organizations navigate the legal ramifications of cyber-attacks.
- **Cybersecurity Firms:** These attacks can lead to increased demand for cybersecurity services, as healthcare organizations seek to bolster their defenses against future incidents.
- **Patients and the Public:** Ultimately, the public is affected as patients may experience compromised care, privacy breaches, and a loss of confidence in the healthcare system.

C. General Vulnerabilities and Threats

The healthcare and public health sector is increasingly reliant on digital technologies for managing patient information, medical procedures, and communication. This digital transformation, while beneficial, introduces significant security risks, including data breaches, unauthorized access, and cyberattacks, which can compromise patient safety, privacy, and the integrity of medical services.

Common cyber threats to medical technology and communication technology protocols include disruption, degradation, and destruction of devices, data poisoning, theft of personal and proprietary data, and unauthorized access to medical software. These threats are exacerbated by the expansion of the interoperable IT/OT environment in healthcare, the use of artificial intelligence (AI) and machine learning (ML)-enabled medical devices, and the increasing reliance on wireless connectivity, including 5G.

Medical devices, such as pacemakers, smart infusion pumps, and MRI machines, may be vulnerable to cyber incidents due to lack of data encryption protocols, poor network segmentation, and unpatched vulnerabilities. Additionally, medical software, such as DICOM and PACS, may lack proper input validation, transmit data in cleartext, and use poor cryptographic algorithms, making them susceptible to unauthorized access and data modification.

1) Smart Infusion Pumps:

These devices connect to hospital internal networks via Wi-Fi or Ethernet and transmit status, alerts, and alarms to central monitoring/control stations, as well as transfer data to Electronic Health Records (EHR).

2) MRI Machines:

MRI machines may be connected to the hospital's internal network, and scans can be encoded and sent to Picture Archiving and Communication System (PACS) software via Digital Imaging and Communications in Medicine (DICOM). PACS images may be stored locally and made available on web based EHR, potentially allowing unauthorized access to clinicians on network devices, including computers.

3) Pacemakers:

Pacemakers and other cardiac implantable electronic devices (CIEDs) have evolved to include wireless connectivity for monitoring and programming. This connectivity, while beneficial for patient care, introduces vulnerabilities. Cyberattacks could potentially lead to device malfunction or unauthorized access to patient data, posing significant risks to patient health.

4) IoT Devices:

Many IoT devices in healthcare lack robust security controls, making them susceptible to unauthorized access and data breaches. This includes issues with data encryption, cleartext data transmission, and insecure storage of passwords.

5) Third-Party Vendors:

Devices and software provided by third-party vendors can introduce vulnerabilities into healthcare networks, offering a backdoor for cyberattacks.

6) Medical Software:

Software like DICOM and PACS may lack proper input validation and use insecure communication protocols, increasing the risk of unauthorized access and data manipulation.

7) Radio Frequency (RF) Interference:

RF interference can disrupt device communication, leading to data loss or misinterpretation, which can have direct implications on patient care.

8) 5G Connectivity:

The adoption of 5G technology in healthcare introduces new vulnerabilities through expanded attack surfaces and potential supply chain risks.

D. Addressing risks

Addressing these risks requires a comprehensive approach to data security, network security, and device security.

1) Data Security

Data security in healthcare involves protecting sensitive patient information from unauthorized access, disclosure, and theft. The Health Insurance Portability and Accountability Act (HIPAA) sets the standard for protecting patient data, requiring encryption of electronic Protected Health Information (ePHI), unique user identification, and audit trails to monitor access and usage of PHI. Encryption is a critical technology for securing data during transfer, use, and storage, ensuring that data is unreadable to unauthorized individuals. Additionally, the adoption of secure communication protocols, such as those outlined by DICOM for medical data transfer, is essential for maintaining the confidentiality and integrity of patient information.

2) Network Security

Network security in the healthcare sector involves protecting the infrastructure that supports the transmission and storage of medical data. This includes securing wireless networks, implementing firewalls, and using virtual private networks (VPNs) to encrypt data in transit. The Cybersecurity and Infrastructure Security Agency (CISA) provides resources and best practices for strengthening network defenses and mitigating cyber threats. Healthcare organizations must also ensure that their network security measures comply with HIPAA regulations and other relevant standards.

3) Device Security

Device security focuses on protecting medical devices and mobile devices used in healthcare settings from cyber threats. This includes implementing strong authentication mechanisms, encrypting data stored on devices, and regularly updating device software to address security vulnerabilities. The increasing use of Internet of Medical Things (IoMT) devices introduces additional security challenges, requiring healthcare organizations to adopt comprehensive security measures to protect these devices from hacking and unauthorized access.

E. Attack Consequences

The consequences of a Cyber-attack on medical technology can be severe and wide-ranging, affecting patients, healthcare organizations, and medical device manufacturers.

- **Compromised patient safety:** Cyber-attacks on medical devices, such as pacemakers, smart infusion pumps, or MRI machines, can lead to disruption, degradation, or destruction of these devices, potentially endangering patient health and even lives.
- **Loss of sensitive data:** Hackers may steal or expose sensitive patient data, including personal information, treatment records, and financial statements, leading to privacy breaches and potential identity theft.
- **Financial and legal penalties:** Healthcare organizations may face significant fines, legal consequences, and sanctions for failing to secure patient data properly and comply with regulations like HIPAA.
- **Reputational damage:** Cyber-attacks can erode patient trust and damage the reputation of healthcare organizations and medical device manufacturers, which can be difficult to recover from.

- **Operational disruptions:** Cyber incidents can cause prolonged IT or production failures, paralyzing critical healthcare services and threatening the existence of affected organizations.
- **Hindered innovation:** The persistent threat of Cyber-attacks may limit the adoption of new technologies and slow down innovation in the healthcare sector

1) Smart Infusion Pumps

The consequences of a Cyber-attack on smart infusion pumps can be severe and potentially life-threatening. Smart infusion pumps are network-connected devices that deliver medications and fluids to patients, and they are commonly used in hospitals and clinics. According to a study by Palo Alto Networks' Unit 42 threat research service, 75% of infusion pumps have cybersecurity flaws, putting them at increased risk of being compromised by hackers.

These cybersecurity flaws can lead to various consequences, including:

- **Unauthorized access:** Hackers can gain unauthorized access to infusion pumps, potentially allowing them to change how the pump delivers intravenous medications. This can result in patients receiving incorrect dosages, which can be harmful or even fatal.
- **Interception of unencrypted communications:** Some infusion pumps transmit unencrypted communications, which can be intercepted by hackers. This can lead to the exposure of sensitive patient data, such as medical records and personal information.
- **Exploitation of known vulnerabilities:** Infusion pumps may have known security gaps, such as leaving usernames and passwords unchanged from the device's default factory settings. These vulnerabilities can be easily exploited by hackers, potentially putting patients at risk or exposing private data.
- **Disruption of services:** disrupt healthcare services, leading to software outages, loss of access to health records, and inability to provide appropriate care. In extreme cases, healthcare facilities may be forced to divert patients to other medical centers or cancel surgeries.

2) MRI Machines

The consequences of a Cyber-attack on MRI machines are multifaceted and can significantly impact patient safety, data integrity, and healthcare operations.

- **Patient Safety Risks:** Cyber-attacks can lead to the manipulation of MRI images, potentially resulting in incorrect diagnoses. For instance, attackers could alter images to either remove a tumor or erroneously add one, leading to misdiagnosis and inappropriate treatment, which could be fatal.
- **Disruption of Healthcare Services:** MRI machines are crucial for diagnosing and monitoring various conditions. A Cyber-attack could disable these machines, causing delays in diagnosis and treatment. In critical situations, even small delays can have severe consequences for patient health.

- **Ransomware Attacks:** MRI machines, like other medical devices, are vulnerable to ransomware attacks. Such attacks could block access to the machines or encrypt the images, demanding a ransom to restore access. This not only disrupts healthcare services but also puts patient data at risk.
- **Exposure of Sensitive Data:** MRI machines are connected to hospital networks, making them potential entry points for attackers to access and steal sensitive patient data, including personal and health information. This breach of privacy can have legal and financial implications for healthcare providers.
- **Operational and Financial Impact:** Recovering from a Cyber-attack on MRI machines can be costly and time-consuming. Healthcare providers may need to replace or repair compromised devices, and face potential legal penalties and loss of trust from patients.
- **Regulatory Challenges:** Strict regulations make it difficult to conduct basic updates on medical PCs connected to MRI machines, complicating efforts to protect against Cyber-attacks. The slow development process of medical imaging devices also leaves them vulnerable to evolving cyber threats

3) Pacemakers

The consequences of a Cyber-attack on pacemakers can be severe and potentially life-threatening. Cybersecurity vulnerabilities in pacemakers were first exposed by hackers in 2011, and since then, various security flaws have been discovered. In 2017, the US Food and Drug Administration (FDA) recalled an implantable pacemaker due to concerns that it could be hacked.

Potential consequences of a on pacemakers include:

- **Direct Threat to Patient Life:** can lead to life-threatening situations. Attackers could potentially take control of the device, altering pacing functions or delivering inappropriate electrical shocks, which could result in severe health complications or even death.
- **Battery Drainage:** Certain types of attacks, such as those involving the continuous sending of commands to the pacemaker, could lead to rapid battery depletion. This would necessitate an early surgical intervention to replace the device, posing additional health risks to the patient.
- **Unauthorized Access to Personal and Medical Data:** Pacemakers can store and transmit data regarding patient health and device performance. Cyber-attacks could compromise the confidentiality of this data, leading to privacy breaches and potential misuse of personal information.
- **Loss of Confidence in Medical Devices:** Widespread knowledge of vulnerabilities and successful attacks could erode public trust in pacemakers and other medical devices. This loss of confidence could deter patients from opting for potentially life-saving treatments

4) Medical IoTs

Cyber-attacks on IoT medical devices can have severe consequences for patient care, including loss of life. The primary target for cyber-attackers are Internet of Things (IoT) and Internet of Medical Things (IoMT) devices, which were the root cause for 21% of all ransomware attacks in the healthcare industry. The top-10 bedside devices that pose the greatest security risks include infusion pumps, VoIP devices, ultrasound machines, patient monitors, and medicine dispensers.

- **Patient Safety Risks:** can directly threaten patient lives by compromising the functionality of medical IoT devices such as pacemakers, insulin pumps, and ventilators. For example, attackers could alter device settings or functionality, leading to inappropriate treatment or device failure.
- **Data Breaches:** IoT medical devices often collect and transmit sensitive patient data. Cyber-attacks can lead to unauthorized access to this data, resulting in privacy violations, identity theft, and potential misuse of personal health information.
- **Operational Disruptions:** can disrupt healthcare operations by disabling medical devices, leading to delays in diagnosis, treatment, and care delivery. This can have cascading effects on patient flow and hospital capacity.
- **Financial Costs:** The aftermath of a can impose significant financial burdens on healthcare organizations, including costs associated with device replacement or repair, data breach response, increased insurance premiums, and potential legal liabilities.
- **Loss of Trust:** can erode trust between patients and healthcare providers. Patients may become hesitant to use certain medical devices or share their data, fearing privacy breaches and questioning the reliability of their care.
- **Regulatory and Legal Implications:** Healthcare organizations may face regulatory penalties for failing to protect patient data and ensure the security of medical devices. Legal actions could also arise from affected patients or regulatory bodies.
- **National Security Threats:** In the context of defense and military operations, compromised IoT devices could reveal sensitive information, posing national security risks. Third-Party Vendors

5) Third-party vendors

Cyber-attacks on third-party vendors in the medical sector can have severe consequences for both the healthcare organizations and the patients they serve. These attacks pose one of the biggest challenges on the healthcare cyber-risk landscape, with hospitals and health systems at increasing risk of cyberattacks on third parties such as business associates, medical device providers, and supply chain vendors. These consequences include:

- **Data Breach:** Third-party vendors often have access to sensitive data. If a third-party vendor is hacked, this data could be compromised, leading to unauthorized access to patient information and financial data.

- **Malware Infections:** If a third-party vendor's system is infected with malware, it could spread to your organization's system through the vendor.
- **Ransomware Attacks:** Many ransomware attacks occur through third-party vendors. If these vendors lack robust security and cyber defense measures, they can become an entry point for ransomware attacks.
- **Distributed Denial of Services (DDoS) Attacks:** Your organization could be targeted by DDoS attacks through third-party vendor systems.
- **Compliance Failures:** Third-party vendors may not always comply with the same regulations as the organizations they work with. This could lead to compliance failures for the organizations.
- **Reputation Damage:** If a third-party vendor is hacked, it could damage the reputation of the organizations they work with.
- **Impact on Medical Devices:** Cyber-attacks on third-party vendors can potentially affect medical devices such as CT and MRI machines, which are commonly connected to hospital networks. Vulnerabilities in outdated firmware can be exploited by cyber-attackers, disrupting digital patient records and potentially jeopardizing patients' health

6) Medical Software

The consequences of a cyber-attack on medical software are significant and multifaceted, impacting not only the healthcare organizations but also the patients they serve. The consequences of a cyber-attack on medical software extend beyond immediate financial losses, posing serious risks to patient safety, data integrity, and the overall effectiveness of healthcare delivery. It underscores the importance of prioritizing cybersecurity measures to protect sensitive health information and ensure the continuity and quality of care

- **Data Breaches:** can lead to unauthorized access to sensitive patient data, including personal and financial information, medical records, and treatment histories. This compromises patient privacy and can result in identity theft and financial fraud.
- **Financial and Legal Penalties:** Healthcare organizations may face substantial financial losses due to fines and legal penalties for failing to protect patient data adequately. The costs associated with responding to a breach, such as notification expenses and credit monitoring services for affected individuals
- **Patient Safety Concerns:** can disrupt healthcare services and compromise patient safety. For example, tampering with medical records or diagnostic software could lead to incorrect diagnoses, inappropriate treatments, or delays in care.
- **Damage to Patient Trust and Reputation:** erode trust between patients and healthcare providers. Patients may lose confidence in an organization's ability to protect their data and provide safe care, damaging the organization's reputation and potentially leading to a loss of business.

- **Loss of Productivity:** can disrupt healthcare operations, leading to delays in procedures and tests, longer patient stays, and overall reduced efficiency. This can strain healthcare resources and negatively impact patient care.
- **Increased Mortality Rates:** In some cases, cyber-attacks have been linked to increased patient mortality rates. Delays in procedures, tests, and the provision of care due to cyber incidents can have dire consequences for patient outcomes.
- **Compromised Value-Based Models:** can undermine the efforts of healthcare organizations to deliver value-based care by compromising the quality and integrity of data, which is crucial for making informed decisions about patient care.
- **Limited Innovation:** Persistent and large-scale cyber-attacks can stifle innovation within the healthcare sector. Concerns about cybersecurity may deter organizations from adopting new technologies that could improve patient care and operational efficiency.

7) Radio Frequency (RF) Interference medical

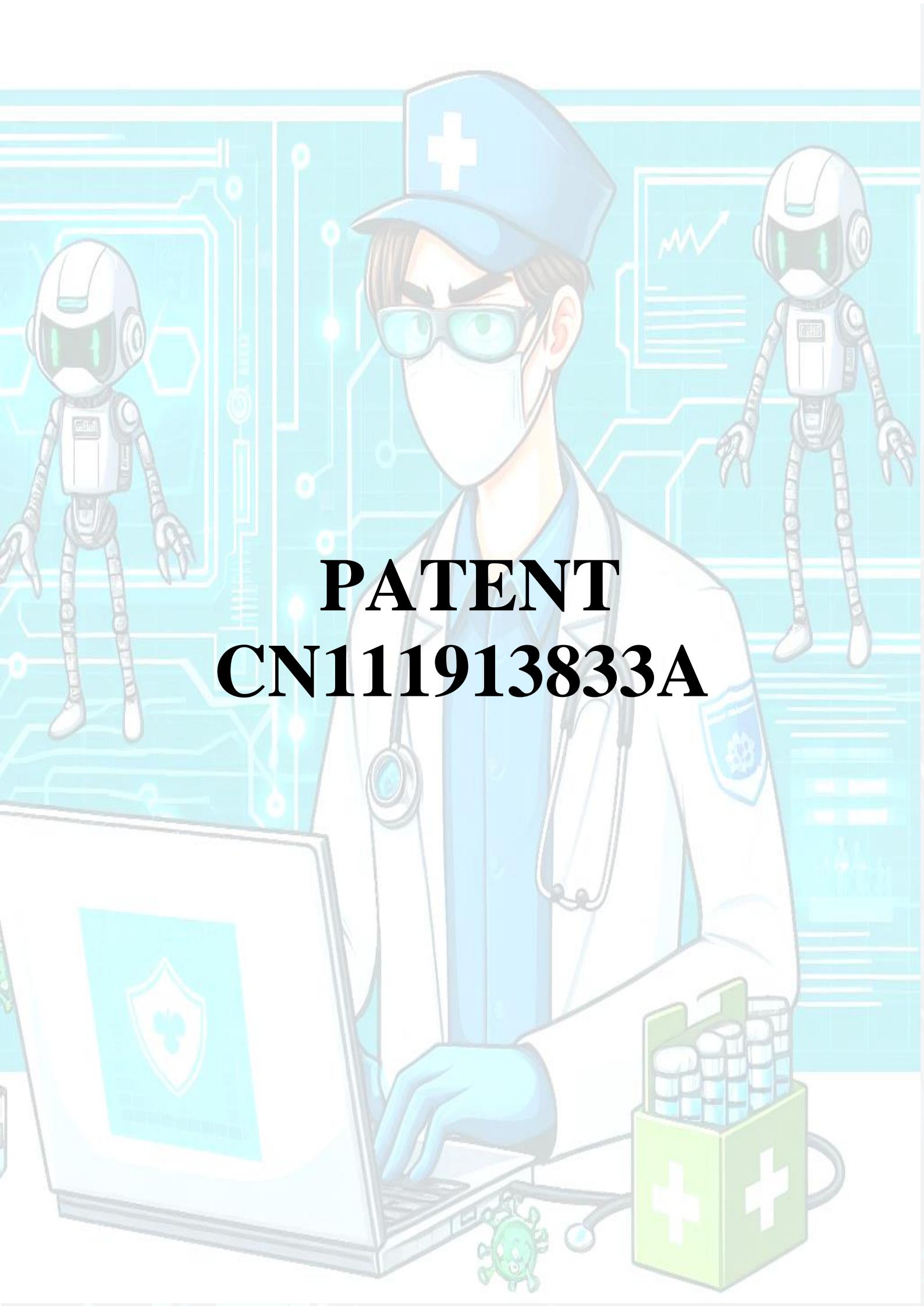
The consequences on Radio Frequency (RF) Interference in the medical field can be severe, as it can compromise the functionality and security of medical devices that rely on RF communication.

- **Interference with Device Functionality:** can disrupt the normal operation of medical devices, potentially leading to incorrect readings or malfunctions. This can have serious consequences for patient care, especially in critical situations where accurate measurements and device performance are essential.
- **Data Breaches:** RF interference can potentially be exploited to gain unauthorized access to sensitive patient data transmitted through RF communication channels. This can lead to data breaches, exposing personal and medical information, and potentially compromising patient privacy.
- **Device Tampering:** could potentially manipulate RF signals to send unauthorized commands to medical devices, such as pacemakers or insulin pumps, potentially causing harm to patients. This can include altering device settings, administering incorrect dosages, or even shutting down devices entirely.
- **Denial of Service:** can cause devices to become unresponsive or malfunction, leading to a denial of service. This can disrupt patient care and potentially put patients at risk, especially in situations where immediate medical attention is required.
- **Loss of Trust:** Successful attacks on RF interference can erode public trust in medical devices and the healthcare system, potentially leading to a reluctance to use such devices or seek medical care.

8) 5G Connectivity

The consequences on 5G connectivity in the medical field can be substantial, given the critical role of 5G in enhancing communication and data transfer within healthcare systems:

- **Increased Attack Surfaces:** The expansion of 5G networks increases the number of potential entry points for cyber-attackers, making it more challenging to secure the network against unauthorized access and data breaches.
- **Vulnerabilities in IoT Devices:** medical devices are part of the Internet of Medical Things (IoMT) and rely on 5G for connectivity. These devices may have inherent security weaknesses that can be exploited, leading to compromised patient data and device functionality.
- **GPRS Tunneling Protocol Risks:** The use of GPRS tunneling protocols in 5G networks can introduce security vulnerabilities, potentially allowing attackers to intercept and manipulate transmitted data.
- **Legacy Network Connections:** 5G networks connected to legacy systems may inherit existing vulnerabilities, providing cyber-attackers with opportunities to exploit these weaknesses and gain access to sensitive medical data and systems.
- **Increased Bandwidth Challenges:** The higher bandwidth of 5G networks can strain current security monitoring capabilities, making it more difficult to detect and respond to threats in real-time.
- **Network Function Virtualization:** The reliance on software and virtualization in 5G networks introduces new security challenges, as each virtual component needs to be monitored and secured to prevent potential breaches.
- **IMSI Encryption Weaknesses:** Weaknesses in IMSI encryption can lead to vulnerabilities in subscriber identity confidentiality, potentially allowing man-in-the-middle attacks and unauthorized tracking of devices.
- **Botnet and DDoS Attacks:** The increased number of connected devices in a 5G network can be leveraged by attackers to create botnets or launch distributed denial-of-service (DDoS) attacks, which can disrupt medical services and data availability.
- **Disruption of Critical Healthcare Services:** Cyber-attacks on 5G networks can disrupt the communication between medical devices and healthcare providers, leading to delays in critical care and potentially endangering patient lives.
- **Regulatory and Compliance Implications:** Healthcare organizations may face regulatory scrutiny and penalties if they fail to protect patient data and ensure the security of their 5G-enabled medical devices and services



PATENT

CN111913833A



Abstract – This document presents a comprehensive analysis of the Medical Internet of Things (IoMT) transaction system based on blockchain technology, specifically focusing on the Chinese patent CN111913833A. The analysis delves into various aspects of the system, including its architecture, security features, the enhancement of data security and privacy, interoperability among different healthcare systems, and the facilitation of secure and transparent transactions and potential applications within the healthcare sector.

A qualitative summary of the document is provided, ensuring that the essence of the patent is captured succinctly for the benefit of security professionals and specialists across various industries. The analysis is particularly beneficial for cybersecurity experts, DevOps engineers, healthcare IT professionals, medical device manufacturers, and forensic analysts in understanding the implications of combining blockchain technology with IoMT. It offers insights into how this integration can address common challenges in the healthcare industry, such as data breaches, unauthorized access, and the lack of a standardized protocol for secure data exchange.

A. Introduction

The patent CN111913833A proposes a blockchain-based transaction system specifically designed for the medical Internet of Things (IoT). This system aims to address the challenges of data security, privacy, and interoperability in healthcare. The proposed solution enhances security and privacy for patient data using dual blockchains, attribute-based authentication, and AI integration. It shares commonalities with other blockchain-based medical IoT systems but may have unique features in its architecture.

The main idea of the patent is to ensure the privacy and security of medical data while facilitating the sharing and exchange of this data among various stakeholders in the healthcare ecosystem.

It presents several key points and takeaways:

- **Dual-Blockchain Architecture:** The system incorporates two blockchains: a public blockchain (Blockchain) for the publication of user data and a private blockchain (Blockchain) for storing healthcare data securely.
- **Attribute-Based Encryption:** Access to medical data is controlled through attribute-based encryption, which allows only authorized users with specific attributes to access or modify the data.
- **Privacy and Security:** The system is designed to enhance the privacy and security of medical data, which is critical in the healthcare industry.
- **Interoperability:** By using blockchain technology, the system facilitates secure data sharing between different entities in the healthcare ecosystem, promoting interoperability.
- **Smart Contracts:** The system utilizes smart contracts to automate and enforce rules for data access and transactions, reducing the need for intermediaries and increasing efficiency.
- **AI Integration:** The patent suggests the potential integration of artificial intelligence with the blockchain to improve medical services, such as disease prediction models.
- **Real-Time Monitoring:** The proposed system may enable real-time monitoring of patient conditions through IoT devices, providing timely and accurate health data.
- **Decentralization:** The decentralized nature of blockchain provides a robust solution against single points of failure and unauthorized data tampering.

B. Industries

The patent has the potential to improve the way medical data is managed and shared across various sectors within the healthcare industry. Its emphasis on security, privacy, and interoperability aligns with the critical needs of these industries, promising to improve efficiency, reduce costs, and enhance patient outcomes. Based on the patent's content it infers the relevance to several industries:

1) Healthcare:

The healthcare industry stands to benefit significantly from this patent including hospitals, clinics, and other medical facilities that require secure management and sharing of patient data. The dual-blockchain system proposed in the patent could enhance the security and privacy of medical data, which is critical for patient trust and regulatory compliance. By using blockchain, healthcare providers can ensure that medical records are immutable and traceable, which is essential for maintaining the integrity of patient data.

2) Medical Devices:

Manufacturers and distributors of medical IoT devices, such as wearable health monitors and connected medical equipment, are directly involved in the ecosystem that the patent addresses. The system would manage the data these devices generate, ensuring that it is securely stored and shared only with

authorized parties. This could improve device monitoring, patient care, and the overall reliability of medical devices.

3) Health Information Technology:

Companies that specialize in health IT solutions, electronic health records (EHR), and medical data management systems would be interested in the blockchain-based system for its potential to enhance data security and interoperability. The patent could provide a new model for health information exchanges, making electronic medical records more secure and easily shareable between different healthcare systems.

4) Pharmaceuticals:

The pharmaceutical industry could use the system for secure data sharing in clinical trials and drug development processes. Blockchain's ability to provide a transparent and immutable record of transactions could help in tracking drug provenance, ensuring the authenticity of medications, and streamlining the supply chain.

5) Insurance:

Health insurance companies might use the system to securely access patient data for claims processing and fraud prevention. The immutable nature of blockchain records could help insurers verify the accuracy of claims and reduce fraudulent activities.

6) Research and Development:

Research institutions that require access to medical data for studies could benefit from the secure and controlled data sharing capabilities of the system. Blockchain could facilitate collaboration between researchers by providing a secure platform for exchanging data while maintaining patient privacy.

7) Regulatory Bodies:

Government health agencies and regulatory bodies might be interested in the system for monitoring compliance with health data privacy regulations such as HIPAA. Blockchain's inherent features could help ensure that healthcare providers and other stakeholders are adhering to the necessary standards.

8) Cybersecurity:

Companies specializing in cybersecurity solutions for the healthcare industry would find relevance in the patent, as it addresses the security of medical data transactions. The proposed blockchain system could offer new ways to protect against data breaches and cyber threats.

C. The proposed solution

The key components of the proposed solution are the dual-blockchain architecture, attribute-based encryption for data access control, a consensus algorithm optimized for transaction throughput, patient data access control, and various functions for remote diagnosis, data sharing, and transactions in the medical IoT context:

Dual-Blockchain Architecture:

- a public blockchain for publishing user data and
- a private blockchain for storing healthcare data securely.

Attribute-Based Encryption (ABE):

- Access to medical data is controlled through attribute-based encryption, which allows only authorized users with specific attributes to access or modify the data.
- This ensures the privacy and security of sensitive medical information.

Transaction throughput:

- To optimize transaction throughput in this scenario, the patent proposes a consensus algorithm based on transaction volume proof.
- This is designed to address the issue of low transaction throughput in existing public blockchain-based medical data solutions.

Patient Data Access Control:

- The system ensures that patients have management and control permissions over their health data.
- This addresses the issue of neglecting patient data access control in current consortium blockchain-based medical data solutions.

Remote Diagnosis, Data Sharing, and Data Transaction Functions:

- The system provides functions such as remote diagnosis, data sharing, and data transactions.
- These features enable various applications and services in the medical IoT ecosystem.

1) Dual-Blockchain Architecture

The proposed solution utilizes a dual-blockchain architecture consisting of a public blockchain for publishing user data and a private blockchain for securely storing healthcare data. This dual-blockchain approach aims to address the challenges of data security, privacy, and interoperability in the medical IoT ecosystem.

The key features of the dual-blockchain architecture revolve around combining the benefits of public and private blockchains, enabling secure data sharing, enhancing trust and data integrity, and potentially improving efficiency and performance in the context of a medical IoT transaction system.

Combination of public and private blockchains:

- The public blockchain is permissionless blockchain that allows anyone to join and participate in publishing and verifying user data transparently.
- The private blockchain is permissioned blockchain with restricted access for securely storing sensitive healthcare data.

Differentiated roles and access control:

- The public blockchain enables users to have control over their data and ensures transparency in data publication.
- The private blockchain provides a secure, private environment for storing and sharing healthcare data among authorized participants only.

Balancing transparency, security, and privacy:

- The dual-blockchain approach aims to leverage the strengths of both public and private blockchains.
- It seeks to strike a balance between the transparency and decentralization of public blockchains and the enhanced privacy and efficiency of private blockchains.

Addressing limitations of single blockchain types:

- Public blockchains alone may face challenges in scalability and privacy.
- Private blockchains alone may sacrifice some level of decentralization and transparency.
- The combination of both types mitigates their individual weaknesses.

Enabling secure data sharing and collaboration:

- The architecture facilitates secure sharing of healthcare data among authorized entities on the private blockchain.
- It promotes collaboration between healthcare stakeholders while maintaining patient privacy.

Enhancing trust and data integrity:

- The immutability and transparency of the public blockchain help establish trust in the overall system.
- The private blockchain ensures the integrity and confidentiality of sensitive healthcare data.

Potential for improved efficiency and performance:

- The restricted participation in the private blockchain can lead to faster transaction processing and consensus compared to public blockchains.
- The dual-blockchain structure allows for optimizing the system based on the specific requirements of each blockchain component.

2) Attribute-Based Encryption (ABE)

ABE is a generalization of public-key encryption that allows for more expressive access control policies. In traditional public-key encryption, a message is encrypted for a specific receiver using their public key. In contrast, ABE encrypts data based on attributes or policies, enabling access control based on the attributes possessed by users.

There are two main types of ABE:

- **Key-Policy ABE (KP-ABE):** In KP-ABE, each user's private key is associated with an access policy or structure that specifies which ciphertexts the key can decrypt. The ciphertexts are labeled with sets of attributes.
- **Ciphertext-Policy ABE (CP-ABE):** In CP-ABE, the access policy is embedded in the ciphertext, and each user's private key is associated with a set of attributes. A user can decrypt a ciphertext only if their attributes satisfy the access policy.

Key Features of ABE

- **Fine-Grained Access Control:** ABE enables fine-grained access control over encrypted data by allowing access policies to be defined based on attributes. This is particularly useful in healthcare, where different stakeholders (e.g., doctors, nurses, researchers) may need different levels of access to patient data.
- **Collusion Resistance:** ABE schemes are designed to be resistant to collusion attacks. Even if multiple users collude and combine their attributes, they should not be able to decrypt a ciphertext unless at least one of them individually satisfies the access policy.
- **Expressiveness:** ABE allows for expressive access policies, which can be represented as boolean formulas or tree structures. This enables complex access control requirements to be enforced.
- **Attribute Revocation:** Some ABE schemes support attribute revocation, allowing a user's attributes to be revoked without affecting other users who share the same attributes. This is important in dynamic environments like healthcare, where user roles and permissions may change over time.
- **Policy Update:** Certain ABE constructions allow for policy updates, enabling the access policies associated with ciphertexts to be modified without re-encrypting the data. This provides flexibility in managing access control as requirements evolve.
- **Traceability:** Some ABE schemes incorporate traceability, allowing the identity of a misbehaving user who leaked their decryption key to be traced. This helps in maintaining accountability and preventing unauthorized data sharing.

ABE in Healthcare

ABE has significant potential in securing healthcare data, particularly in cloud-based e-health systems. By using ABE, patient data can be encrypted with fine-grained access policies, ensuring that only authorized users (e.g., healthcare providers with specific roles or attributes) can decrypt and access the data. This helps in protecting patient privacy and meeting regulatory requirements like HIPAA.

Moreover, features like attribute revocation and policy update are crucial in healthcare, as user roles and data access requirements may change frequently. Traceability is also important for preventing data leakage and ensuring compliance.

3) Consensus Algorithm Based on Transaction Volume Proof

In blockchain systems, consensus algorithms are used to achieve agreement among participating nodes on the state of the ledger. They ensure that all nodes have a consistent view of the blockchain and prevent double-spending or other malicious activities. However, traditional consensus algorithms like Proof-of-Work (PoW) and Proof-of-Stake (PoS) often face scalability challenges, resulting in low transaction throughput.

The Consensus Algorithm Based on Transaction Volume Proof proposed in the patent aims to optimize transaction throughput specifically for the medical IoT scenario:

- **Transaction Volume as a Metric:** The algorithm likely uses the volume or number of transactions processed by a node as a metric for determining its eligibility to create new blocks. Nodes that process a higher volume of transactions may be given priority or more weight in the consensus process.
- **Encouraging Active Participation:** By basing the consensus on transaction volume, the algorithm incentivizes nodes to actively participate in the network and process transactions. Nodes that contribute more to the network's throughput are rewarded with a higher chance of creating new blocks and earning rewards.
- **Optimizing Throughput:** By prioritizing nodes with higher transaction volumes, the algorithm aims to optimize the overall throughput of the network. Nodes that can process transactions efficiently are given more opportunities to add new blocks, thereby increasing the transaction processing capacity of the blockchain.
- **Addressing Scalability:** The algorithm is designed to address the scalability limitations of existing public blockchain-based medical data solutions. By focusing on transaction volume as a key metric, it aims to improve the network's ability to handle a large number of transactions, which is crucial in the medical IoT context.

Key Features of the Consensus Algorithm

- **Throughput Optimization:** The primary goal of the algorithm is to optimize transaction throughput, enabling the blockchain network to process a higher volume of transactions efficiently.
- **Scalability:** By addressing the low transaction throughput issue, the algorithm aims to enhance the scalability of the blockchain system, making it suitable for handling the large-scale data generated in medical IoT scenarios.
- **Incentivizing Active Participation:** The algorithm rewards nodes that actively participate in the network and process a high volume of transactions. This encourages nodes to contribute to the network's throughput and maintain a healthy ecosystem.
- **Customization for Medical IoT:** The algorithm is specifically designed for the medical IoT transaction system, taking into account the unique requirements and challenges of this domain, such as the need for high-speed processing of large volumes of medical data.
- **Integration with Dual-Blockchain Architecture:** The Consensus Algorithm Based on Transaction Volume Proof is likely integrated with the dual-blockchain architecture proposed in the patent, optimizing the performance of the public Blockchain and private Blockchain components.

4) Patient Data Access Control

Patient data access control is a critical component of the proposed medical Internet of Things (IoT) transaction system based on blockchain. The system aims to ensure that patients have management and control permissions over their health data, addressing the issue of neglecting patient data access

control in current consortium blockchain-based medical data solutions.

It puts patients in control of their sensitive health information, uses attribute-based encryption and smart contracts to enable fine-grained and automated access policies, provides auditable and transparent records of access, allows for dynamic permission changes, and integrates with the broader IoT ecosystem. This comprehensive approach to access control enhances the security and privacy of patient data while enabling authorized data sharing for improved medical care and research.

The key features of the patient data access control mechanism in this system are:

Patient-centric control:

- The system is designed to give patients the primary control and management permissions over their own health data.
- This patient-centric approach ensures that the rights and interests of patients regarding their sensitive medical information are protected.
- Patients can decide who has access to their data and under what circumstances.

Attribute-based access control:

- Access to medical data is controlled through attribute-based encryption (ABE).
- ABE allows only authorized users with specific attributes to access or modify the data.
- The attributes could relate to the user's role (e.g. doctor, nurse, researcher), specialty, location, or other relevant factors.
- This fine-grained access control ensures that sensitive data is only accessible to those who have a legitimate need and authorization.

Smart contract-based automation:

- The access control policies and permissions are likely encoded into smart contracts on the blockchain.
- Smart contracts allow the automatic execution and enforcement of the access rules without manual intervention.
- This automation streamlines the access control process and reduces the risk of unauthorized access due to human error or manipulation.

Auditable and transparent:

- All access attempts and data transactions are recorded immutably on the blockchain.
- This creates an auditable trail of who accessed what data and when.
- The transparency and traceability enabled by blockchain helps ensure compliance with data protection regulations and deters unauthorized access attempts.

Dynamic and revocable access:

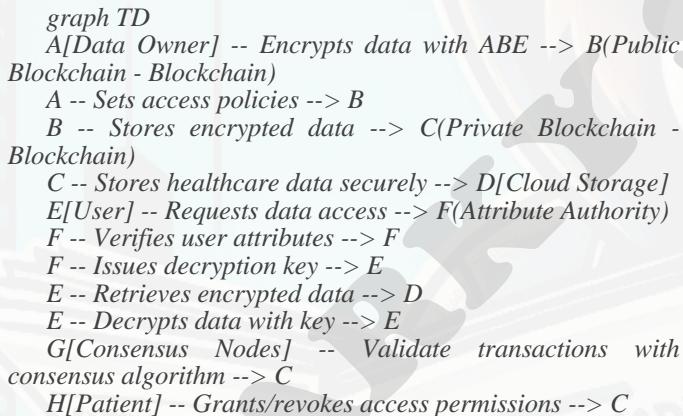
- Patient access permissions can be granted, modified or revoked dynamically as needed.
- For example, a patient may grant temporary access to a specialist for a specific treatment, and then revoke that access once the treatment is complete.
- This flexibility allows access control to adapt to the dynamic needs of medical care while maintaining security.

Integration with medical IoT ecosystem:

- The access control system is integrated with the broader medical IoT transaction system proposed in the patent.
- This enables secure and controlled access to data generated by various medical IoT devices and wearables.
- Authorized healthcare providers can access this IoT data for remote monitoring, diagnosis, and treatment of patients.

D. Process Flow

The proposed solution leverages a dual-blockchain architecture, with a public Blockchain for data publication and a private Blockchain for secure data storage. ABE is used for fine-grained access control, while the consensus algorithm ensures efficient transaction validation. Patients retain control over their data through access control mechanisms. The system aims to provide a secure, efficient, and patient-centric approach to managing and sharing medical data in an IoT environment.



Data Encryption and Access Policy Setting:

- The data owner (e.g., patient or healthcare provider) encrypts the medical data using Attribute-Based Encryption (ABE).
- The data owner defines the access policies specifying which attributes are required to decrypt the data.
- The encrypted data and access policies are published to the public blockchain (Blockchain).

Secure Data Storage:

- The encrypted healthcare data from the Blockchain is securely stored in the private blockchain (Blockchain).

- The Blockchain acts as a secure, access-controlled storage layer for the sensitive medical data.
- The encrypted data may also be stored in cloud storage for scalability and availability.

User Authentication and Key Issuance:

- A user (e.g., doctor, researcher) who wants to access the encrypted data sends a request to the Attribute Authority.
- The Attribute Authority verifies the user's attributes against the access policies.
- If the user possesses the required attributes, the Attribute Authority issues a decryption key to the user.

Data Access and Decryption:

- The authorized user retrieves the encrypted data from the Blockchain or cloud storage.
- Using the decryption key obtained from the Attribute Authority, the user decrypts the data.
- The user can now access the plaintext medical data as per the granted access permissions.

Transaction Validation and Consensus:

- Consensus nodes in the blockchain network validate the transactions using the Consensus Algorithm Based on Transaction Volume Proof.
- This consensus mechanism optimizes transaction throughput and ensures the integrity and security of the blockchain.

Patient Access Control:

- Patients have control over their medical data and can grant or revoke access permissions to specific users or entities.
- The access control policies are enforced through smart contracts on the Blockchain.

Additional Functions:

- The system supports remote diagnosis, allowing authorized healthcare providers to access patient data remotely for telemedicine purposes.
- Data sharing and transaction functions enable secure sharing of medical data among authorized parties, such as healthcare providers, researchers, or insurers.

E. Benefits, drawbacks and significance of proposed solution

The proposed medical IoT transaction system based on blockchain offers significant benefits in terms of enhanced security, privacy, patient control, and data sharing. However, it also faces limitations related to complexity, regulatory compliance, scalability, and dependence on blockchain technology.

Benefits:

- **Enhanced security and privacy:** The dual-blockchain architecture, with a public Blockchain for data publication and a private Blockchain for secure data

storage, along with attribute-based encryption (ABE) for fine-grained access control, significantly enhances the security and privacy of sensitive medical data.

- **Patient-centric control:** The system empowers patients with management and control permissions over their health data, ensuring their rights and interests are protected.
- **Improved data sharing and collaboration:** The secure, efficient data sharing enabled by the system promotes collaboration among healthcare stakeholders while maintaining patient privacy.
- **Increased trust and data integrity:** The immutability and transparency of blockchain transactions establish trust in the system and ensure data integrity.
- **Potential for improved efficiency:** The consensus algorithm based on transaction volume proof aims to optimize transaction throughput, addressing scalability issues in existing blockchain-based medical data solutions.

Limitations:

- **Complexity and adoption challenges:** The proposed system involves multiple components and technologies, which may pose challenges in terms of complexity, interoperability, and adoption by healthcare organizations.
- **Regulatory compliance:** Ensuring compliance with healthcare data privacy regulations and standards, such as HIPAA, could be challenging and may require additional measures.
- **Scalability and performance:** While the proposed consensus algorithm aims to improve transaction throughput, the scalability and performance of the system in handling large volumes of medical data in real-world scenarios need further validation.
- **Key management and access control:** Implementing secure and efficient key management for ABE and managing dynamic access control policies could be complex, especially in emergency situations.
- **Dependence on blockchain technology:** The system heavily relies on blockchain technology, which is still evolving and may face challenges related to energy consumption, interoperability, and legal recognition.

Significance:

- **Advancing secure medical data management:** The proposed solution addresses critical challenges in medical data security, privacy, and sharing, contributing to the development of more secure and patient-centric health information management systems.
- **Fostering innovation in healthcare:** By leveraging cutting-edge technologies like blockchain, ABE, and IoT, the patent encourages innovation in the healthcare domain, potentially leading to improved patient care, research, and overall efficiency.
- **Promoting patient empowerment:** The emphasis on patient control over their data aligns with the growing

trend of patient-centered healthcare and could inspire further innovations in this direction.

- **Encouraging collaboration and data sharing:** The secure data sharing capabilities of the system could facilitate unprecedented levels of collaboration among healthcare providers, researchers, and other stakeholders, accelerating medical advancements.
- **Contributing to the evolving landscape of blockchain in healthcare:** The patent adds to the growing body of research and innovation exploring the application of blockchain technology in the healthcare sector, helping shape its future direction and potential impact.

1) Dual-Blockchain Architecture

The Dual-Blockchain Architecture offers significant benefits in enhancing security, privacy, IoT integration, scalability, and patient data access control for medical data management. However, it also faces limitations related to complexity, regulatory compliance, and potential scalability issues. Despite these challenges, architecture represents a significant step forward in advancing secure medical data sharing, enabling collaboration, and empowering patients in the healthcare ecosystem.

a) Benefits:

Enhanced Security and Privacy:

- The dual-blockchain architecture, with a public Blockchain for data publication and a private Blockchain for secure data storage, significantly enhances the security and privacy of sensitive medical data.
- The Blockchain provides a secure, private environment for storing and sharing healthcare data among authorized participants only, ensuring confidentiality.
- Attribute-based encryption is used to control access to health data, ensuring that only entities meeting certain criteria can access it.

Integration with IoT Devices:

- The architecture facilitates secure sharing of healthcare data collected from various medical IoT devices and wearables.
- Authorized healthcare providers can access this IoT data for remote monitoring, diagnosis, and treatment of patients.
- Blockchain's decentralized nature enhances the integrity and security of data generated by IoT devices.

Scalability and Performance:

- The dual-blockchain structure allows for optimizing the system based on the specific requirements of each blockchain component.
- The restricted participation in the private Blockchain can lead to faster transaction processing and consensus compared to public blockchains.
- Parallelization techniques can be employed to increase the system's throughput and reduce network traffic.

Patient Data Access Control:

- Patients have control over their medical data and can grant or revoke access permissions to specific users or entities.
- The access control policies are enforced through smart contracts on the Blockchain.
- Fine-grained access control is enabled through attribute-based encryption, ensuring only authorized parties can access patient data.

b) Limitations:

Complexity and Adoption Challenges:

- The dual-blockchain architecture involves multiple components and technologies, which may pose challenges in terms of complexity, interoperability, and adoption by healthcare organizations.
- Integrating the system with existing healthcare infrastructure and ensuring compatibility could be complex.

Regulatory Compliance:

- Ensuring compliance with healthcare data privacy regulations and standards, such as HIPAA, could be challenging and may require additional measures.
- Navigating the legal and regulatory landscape across different jurisdictions may be complex.

Scalability and Performance Limitations:

- While the dual-blockchain architecture aims to improve scalability and performance, the system's ability to handle large volumes of medical data in real-world scenarios needs further validation.
- The consensus mechanism and data synchronization between the Blockchain and Blockchain may still face scalability challenges.

c) Significance:

Advancing Secure Medical Data Management:

- The dual-blockchain architecture addresses critical challenges in medical data security, privacy, and sharing.
- It contributes to the development of more secure and patient-centric health information management systems.

Enabling Secure Data Sharing and Collaboration:

- The architecture facilitates secure sharing of healthcare data among authorized entities, promoting collaboration between healthcare providers, researchers, and other stakeholders.
- It enables unprecedented levels of data sharing while maintaining patient privacy.

Empowering Patients:

- By giving patients control over their medical data access permissions, the system promotes patient empowerment and aligns with the trend of patient-centered healthcare.
- It allows patients to selectively share their data for improved care and research purposes.

2) Attribute-Based Encryption (ABE)

ABE offers significant benefits in enhancing security, privacy, and fine-grained access control for medical data, while enabling secure data sharing and patient empowerment. However, scalability, performance, and regulatory compliance remain key challenges to be addressed.

a) Benefits:

Enhanced Security and Privacy:

- ABE allows data to be encrypted in such a way that only users possessing specific attributes can decrypt and access the data, ensuring fine-grained access control
- It enables patients to store their health records in an encrypted form and cryptographically enforces patient or organizational access policies.
- ABE protects sensitive medical information from unauthorized access, enhancing privacy.

Integration with Blockchain and IoT:

- ABE can be effectively combined with blockchain technology to provide secure and decentralized access control in IoT environments, including healthcare.
- It allows for secure sharing of healthcare data collected from various medical IoT devices and wearables among authorized parties.
- The integration of ABE and blockchain ensures the integrity, confidentiality, and auditability of IoT data.

Fine-Grained Access Control:

- ABE enables fine-grained access control over encrypted data by allowing access policies to be defined based on attributes.
- It supports expressive access policies, which can be represented as boolean formulas or tree structures, enabling complex access control requirements to be enforced.
- Different stakeholders in healthcare, such as doctors, nurses, and researchers, can be granted different levels of access to patient data based on their attributes.

b) Limitations:

Scalability and Performance:

- ABE schemes can face scalability challenges, particularly when dealing with a large number of attributes or complex access policies.
- The computational overhead of encryption and decryption operations in ABE grows with the complexity of access policies and the number of attributes involved.

- Efficient key management and attribute revocation mechanisms are crucial for the practical deployment of ABE in large-scale systems.

Regulatory Compliance:

- Implementing ABE in healthcare systems must ensure compliance with data privacy regulations and standards, such as HIPAA, which can be challenging.
- Balancing the need for fine-grained access control with the requirements of emergency access to patient data in critical situations is a complex issue.

c) Significance:

Enabling Secure Data Sharing and Collaboration:

- ABE facilitates secure sharing of sensitive healthcare data among authorized parties, promoting collaboration between healthcare providers, researchers, and other stakeholders.
- It allows for granular access control, ensuring that different users can access only the specific data they are authorized to view.

Empowering Patients:

- By integrating ABE into healthcare systems, patients can have greater control over who can access their medical records and under what conditions.
- This patient-centric approach aligns with the growing trend of empowering patients to manage their own health data.

Advancing Privacy-Preserving Healthcare:

- ABE contributes to the development of privacy-preserving healthcare solutions, enabling secure storage and sharing of medical data in cloud environments.
- It addresses the critical challenges of data security and privacy in the era of digital health and IoT-enabled healthcare.

3) Consensus Algorithm Based on Transaction Volume Proof

The Consensus Algorithm Based on Transaction Volume Proof offers benefits in terms of optimizing transaction throughput, incentivizing active participation, and addressing scalability issues. However, it also has limitations related to potential centralization, vulnerability to attacks, and adoption challenges.

a) Benefits:

Optimized Transaction Throughput:

- The primary goal of the algorithm is to optimize transaction throughput, enabling the blockchain network to process a higher volume of transactions efficiently.
- By prioritizing nodes with higher transaction volumes, the algorithm aims to improve the network's overall throughput and capacity to handle a large number of transactions.

Incentivizing Active Participation:

- The algorithm rewards nodes that actively participate in the network and process a high volume of transactions.
- This encourages nodes to contribute to the network's throughput and maintain a healthy ecosystem.

Addressing Scalability Issues:

- The algorithm aims to address the low transaction throughput and scalability limitations of existing public blockchain-based medical data solutions.
- By focusing on transaction volume as a key metric, it seeks to enhance the network's ability to handle the large-scale data generated in medical IoT scenarios.

b) Limitations:

Potential Centralization:

- If a small number of nodes consistently process a significantly higher volume of transactions, they may gain disproportionate influence over the consensus process.
- This could lead to a degree of centralization, undermining the decentralized nature of the blockchain network.
- **Vulnerability to Attacks:**
- Nodes with high transaction volumes may become targets for attacks, as compromising them could allow an attacker to disrupt the consensus process.
- The algorithm may need additional security measures to mitigate the risk of such attacks.

Complexity and Adoption Challenges:

- Implementing and integrating the algorithm with existing systems may pose challenges in terms of complexity and adoption.
- The algorithm's effectiveness in real-world medical IoT scenarios needs further validation and testing.

c) Significance:

Advancing Scalable Blockchain Solutions:

- The algorithm contributes to the development of more scalable and efficient blockchain solutions for handling high transaction volumes.
- It addresses a critical challenge in applying blockchain technology to data-intensive domains like healthcare and IoT.

Promoting Blockchain Adoption in Healthcare:

- By optimizing transaction throughput, the algorithm can make blockchain more viable for managing and sharing large volumes of medical data.
- This can facilitate the adoption of blockchain technology in the healthcare industry, enabling secure and efficient data management and collaboration.

Encouraging Innovation in Consensus Algorithms:

- The algorithm represents an innovative approach to consensus, focusing on transaction volume as a key metric.
- It contributes to the ongoing research and development of new consensus algorithms tailored to specific use cases and requirements.

4) Patient Data Access Control

The patient data access control mechanism offers significant benefits in terms of enhanced security, privacy, fine-grained control, and patient empowerment.

a) Benefits:

Enhanced Security and Privacy:

- The system ensures that patients have management and control permissions over their health data, protecting their rights and interests.
- Fine-grained access control through attribute-based encryption (ABE) allows only authorized users with specific attributes to access or modify the data, ensuring the privacy and security of sensitive medical information.
- Access control policies are enforced through smart contracts on the blockchain, providing an automated and secure way to manage permissions.

Integration with Blockchain and IoT:

- The patient data access control mechanism is integrated with the broader blockchain-based medical IoT transaction system proposed in the patent.
- This integration enables secure and controlled access to data generated by various medical IoT devices and wearables.
- Blockchain's immutability and transparency features establish trust in the system and ensure data integrity.

Fine-Grained Access Control:

- The system employs attribute-based encryption (ABE) to enable fine-grained access control over encrypted data.
- Access policies can be defined based on various attributes such as user roles, locations, or other relevant factors, allowing for nuanced and flexible control over data access.
- Different stakeholders in healthcare, such as doctors, nurses, and researchers, can be granted different levels of access to patient data based on their attributes.

Patient Empowerment and Control:

- The system puts patients in control of their own health data, allowing them to grant, modify, or revoke access permissions to specific users or entities.
- This patient-centric approach aligns with the growing trend of empowering patients to manage their own health information.
- Patients can selectively share their data for improved care and research purposes while maintaining privacy.

b) Limitations:

Complexity and Adoption Challenges:

- Implementing fine-grained access control and integrating it with blockchain and IoT systems may be complex, requiring significant technical expertise and resources.
- Adoption challenges may arise due to the need for healthcare organizations to adapt their existing systems and processes to incorporate the new access control mechanisms.

Scalability and Performance Concerns:

- As the volume of patient data and the number of users grow, the scalability and performance of the access control system may be tested.
- Efficient key management, attribute revocation, and policy updates become crucial to maintain the system's responsiveness and effectiveness.

Regulatory Compliance and Emergency Access:

- Ensuring compliance with various healthcare data privacy regulations, such as HIPAA, while implementing granular access control can be challenging.
- Balancing the need for strict access control with the requirement for emergency access to patient data in critical situations is a complex issue that needs to be carefully addressed.

c) Significance:

Advancing Patient-Centric Healthcare:

- The patient data access control mechanism proposed in the patent promotes a patient-centric approach to healthcare data management.
- It empowers patients to have greater control over their personal health information, aligning with the shift towards patient-centered care models.

Enabling Secure Data Sharing and Collaboration:

- The fine-grained access control system facilitates secure sharing of patient data among authorized healthcare stakeholders, fostering collaboration and improving care coordination.
- It enables researchers to access anonymized patient data for medical research while maintaining patient privacy.

Driving Innovation in Healthcare Security:

- The integration of blockchain, IoT, and attribute-based encryption for patient data access control represents an innovative approach to healthcare data security.
- It showcases the potential of leveraging emerging technologies to address the critical challenges of data privacy, security, and patient empowerment in the digital health era.

5) Remote Diagnosis, Data Sharing, and Data Transaction Functions

The remote diagnosis, data sharing, and data transaction functions offer significant benefits in terms of improving access to healthcare, enhancing data sharing and collaboration, and enabling efficient data transactions. However, there are limitations related to technical challenges, data security and privacy concerns, and adoption and integration issues that need to be addressed.

a) Benefits:

Improved Access to Healthcare:

- Remote diagnosis enables patients to receive medical consultations and diagnoses from the comfort of their homes, reducing the need for in-person visits.
- This is particularly beneficial for patients in rural areas, elderly patients, or those with mobility issues who may have difficulty accessing traditional healthcare facilities.
- Remote monitoring allows for continuous tracking of patient health data, enabling early detection and intervention of potential health issues.

Enhanced Data Sharing and Collaboration:

- The system facilitates secure sharing of healthcare data among authorized parties, such as healthcare providers, researchers, and insurers.
- Blockchain technology ensures the integrity, confidentiality, and auditability of shared data.
- Improved data sharing promotes collaboration and enables more informed decision-making in patient care.

Efficient Data Transactions:

- The system enables efficient and secure data transactions between various stakeholders in the healthcare ecosystem.
- Smart contracts can automate data access and sharing processes, reducing administrative overhead and improving efficiency.
- Secure transactions help maintain patient privacy while enabling authorized access for legitimate purposes.

b) Limitations:

Technical Challenges:

- Implementing remote diagnosis and monitoring may require specialized equipment and reliable internet connectivity, which can be a challenge in certain areas.
- Integrating IoT devices and ensuring interoperability with existing healthcare systems can be complex.
- Handling large volumes of data generated by IoT devices and ensuring real-time processing and analysis can be technically demanding.

Data Security and Privacy Concerns:

- Sharing sensitive healthcare data raises concerns about data security and patient privacy.
- Robust security measures, such as encryption and access control mechanisms, need to be implemented to prevent unauthorized access and data breaches.
- Compliance with data protection regulations adds complexity to the system design and implementation.

Adoption and Integration Challenges:

- Adopting remote diagnosis and monitoring technologies may require significant changes to existing healthcare workflows and processes.
- Healthcare providers may need training and support to effectively use the new technologies and interpret the data generated.
- Integrating the system with existing electronic health record (EHR) systems and ensuring seamless data exchange can be challenging.

c) Significance:

Transforming Healthcare Delivery:

Remote diagnosis, data sharing, and data transaction functions have the potential to transform healthcare delivery by making it more accessible, efficient, and patient-centric.

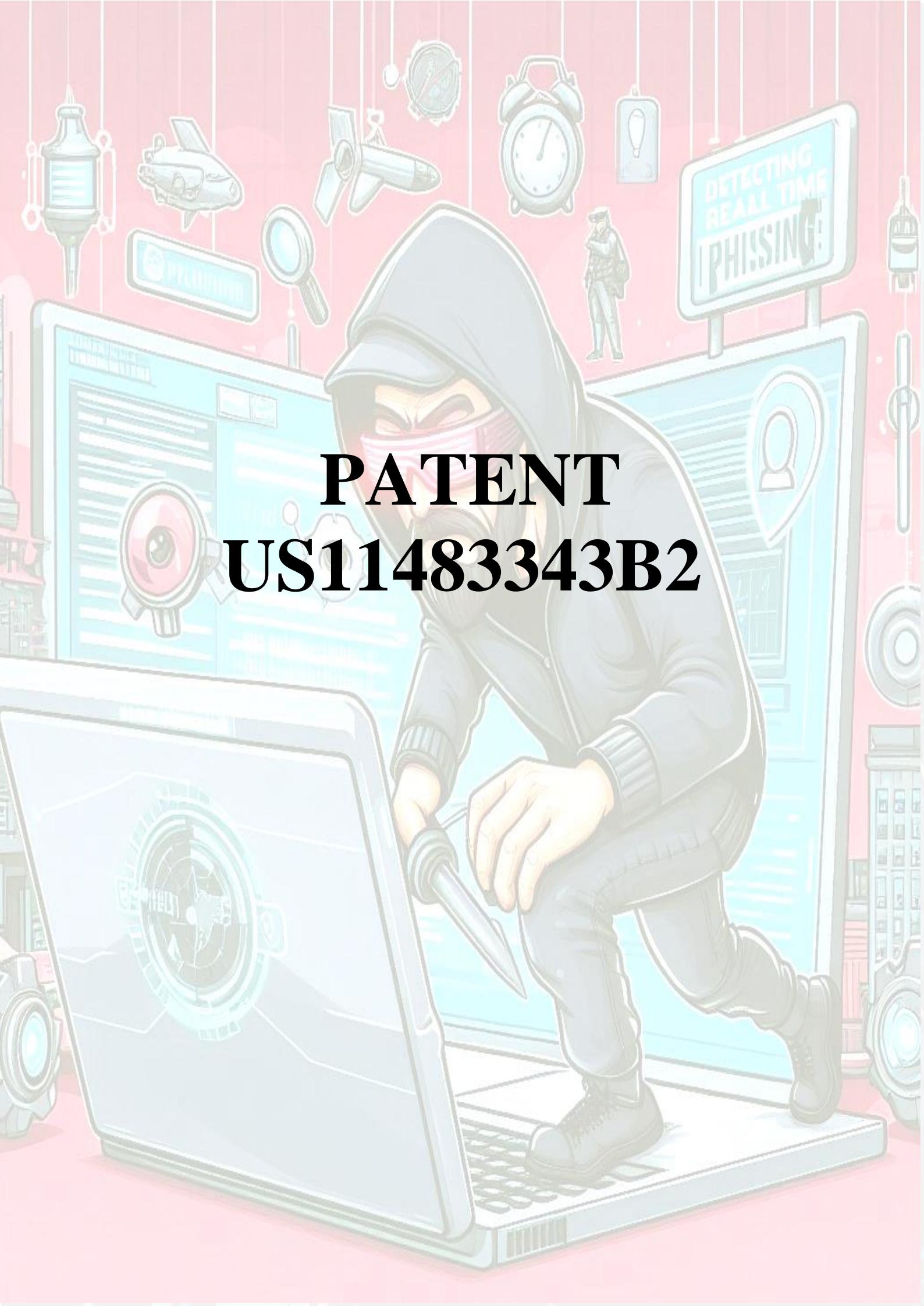
These technologies enable a shift towards proactive and preventive care, reducing the burden on healthcare facilities and improving patient outcomes.

Advancing Personalized Medicine:

- The continuous monitoring and analysis of patient data through remote monitoring enables the delivery of personalized and targeted interventions.
- Healthcare providers can tailor treatment plans based on individual patient needs and responses, leading to more effective and efficient care.

Enabling Data-Driven Healthcare:

- System generates a wealth of healthcare data that can be leveraged for research, analytics, and decision support.
- Analyzing aggregated and anonymized patient data can lead to insights into disease patterns, treatment effectiveness, and population health trends.
- Data-driven approaches can inform healthcare policies, resource allocation, and the development of new therapies and interventions.



PATENT

US11483343B2



Abstract – This document provides a comprehensive analysis of the patent US11483343B2, which pertains to a phishing detection system and method of use. The analysis will delve into various aspects of the patent, including its technological underpinnings, the novelty of the invention, its potential applications. A high-quality summary of the document is presented, highlighting the key elements that contribute to its significance in the field of cybersecurity.

The analysis is beneficial for security professionals, IT experts, and stakeholders in various industries, providing them with a distilled essence of the patent and its utility in enhancing cybersecurity measures. It serves as a valuable resource for understanding patented technology's contribution to the ongoing efforts to combat phishing and other cyber threats.

A. Introduction

The patent US11483343B2, titled "Phishing Detection System and Method of Use," focuses on an advanced system and methodology for identifying and mitigating phishing attacks. This patent proposes a specific architecture for a phishing detection system that scans messages for suspicious URLs and analyzes the corresponding webpages to identify phishing attempts.

B. Industries

The phishing detection system and method are applicable across a wide range of industries and sectors that rely on digital communications and are vulnerable to phishing attacks:

1) Technology Sector:

- Technology companies, especially those providing software, cloud services, social media platforms, and e-commerce, are prime targets for phishing attacks seeking user data and credentials.
- The technology sector would benefit from improved phishing detection to protect their platforms, customers, and reputation.

2) Financial Services:

- Financial institutions like banks, investment firms, insurance companies, and fintech startups handle sensitive financial data and transactions.
- Phishing attacks often impersonate financial services to steal account credentials, payment details, and commit fraud.
- The financial sector has a strong need for effective phishing detection to secure customer accounts and comply with regulations.

3) Healthcare:

- Healthcare organizations like hospitals, clinics, insurance providers, and pharmaceutical companies maintain personal health information and insurance/payment data.
- Phishing attacks may seek to steal patient data, commit insurance fraud, or disrupt operations.
- Protecting against phishing is critical for HIPAA compliance and patient trust in the healthcare sector.

4) Education:

- Educational institutions from schools to universities have moved many services online and hold student personal and financial data.
- Phishing attacks may target students, faculty, and staff to steal identities, academic records, or research data.
- Schools and universities need anti-phishing measures to safeguard educational data and intellectual property.

5) Government:

- Government agencies at the federal, state, and local levels are also targeted by phishers seeking sensitive data or to disrupt services.
- Improved phishing detection can help secure public sector systems and data.

C. The proposed solution

This patent proposes a multi-stage phishing detection system that scans messages, resolves embedded URLs, extracts webpage features, and applies machine learning to identify phishing attempts. While it offers more proactive and comprehensive coverage than traditional methods, it may face performance and accuracy challenges in the evolving landscape of phishing attacks. Nonetheless, it represents a significant step towards automated, real-time phishing detection and prevention.

The proposed phishing detection system and method identify phishing attempts in electronic messages and aims to proactively detect and block such malicious messages.

1) Key Components of the Proposed Solution:

Phishing Detector: The core component is a phishing detector module that analyzes messages for suspicious content. It consists of two main subcomponents:

- **Scan Engine:** Scans the message body and attachments to identify any URLs (web addresses) present. Extracts these URLs for further analysis.
- **Fetcher Component:** Takes the URLs found by the scan engine and resolves them to the actual webpages

they point to. Retrieves the HTML source code of these webpages.

Feature Extraction: The phishing detector then extracts two types of features from the retrieved webpages:

- **URL-based Features:** Analyzes the structure and components of the URL itself, such as length, special characters, IP address usage, etc. Suspicious patterns may indicate a phishing attempt.
- **Hyperlink-based Features:** Examines hyperlinks present in the webpage source code. Looks at target URLs, anchor text, and other link attributes for signs of deception.

Machine Learning Models:

- **Hybrid Feature Set:** The URL and hyperlink features are combined into a hybrid feature set representing each webpage. This provides a comprehensive characterization of the page's suspiciousness.
- **Machine Learning Models:** The hybrid feature sets are used to train machine learning classifiers to distinguish between phishing and legitimate webpages. Models are trained on large datasets of known phishing and benign examples.

2) Method of Use:

- **Message Scanning:** When a new message arrives, the phishing detector's scan engine identifies any URLs present in the content.
- **URL Resolution:** The fetcher component resolves the found URLs to their target webpages and retrieves the page source code.
- **Feature Extraction:** URL and hyperlink-based features are extracted from each webpage.
- **Classification:** The pre-trained machine learning models are applied to the extracted feature set. The models classify the webpage as phishing or legitimate.
- **Action:** If a webpage is deemed a phishing attempt, the original message can be quarantined or blocked. Alerts may be generated for administrators or the intended recipient.

D. Process Flow

The key process flow involves the scan engine extracting URLs from messages, the fetcher resolving those URLs to webpages, analyzing the URL and hyperlink features of those pages, and applying ML models to detect phishing attempts, leading to automatic deletion of phishing messages. This multi-stage analysis allows proactive, real-time filtering of phishing content based on the destination webpage characteristics, going beyond traditional URL or content-based filtering methods.

This process flow covers the end-to-end lifecycle of the proposed solution and focuses on the requested aspects:

1) Scan Engine and Fetcher:

- The scan engine scans incoming messages to identify and extract any URLs present in the message body or attachments.
- The fetcher component then resolves the extracted URLs to the actual webpages they point to and retrieves the HTML source code of those webpages.

2) URL Detection and Resolution:

- The scan engine is responsible for detecting URLs embedded in messages. It scans the message content and attachments to identify URL strings.
- Once URLs are detected, the fetcher component resolves them to their target webpages. This involves following redirects and retrieving the final webpage that the URL ultimately points to.
- The fetcher retrieves the full HTML source code of the resolved webpage for further analysis.

3) Webpage Analysis:

- The retrieved webpage HTML is analyzed to extract two types of features:
 - **URL-based features:** Analyzing the URL string itself for suspicious patterns like length, special characters, IP address usage, etc.
 - **Hyperlink-based features:** Examining the hyperlinks in the webpage source, looking at target URLs, anchor text, and link attributes.
- These URL and hyperlink features are combined into a hybrid feature set representing the webpage's suspiciousness.
- Pre-trained machine learning models are applied to this feature set to classify the webpage as phishing or legitimate.

4) Phishing Detection Criteria:

- The key phishing detection criteria are the URL and hyperlink features extracted from the resolved webpage.
- Suspicious URL patterns can include excessive length, random character strings, IP addresses, URL shorteners, etc.
- Hyperlink features like mismatched target URLs, suspicious anchor text, or links to known malicious sites can indicate phishing.
- The machine learning models are trained on datasets of known phishing and legitimate webpages to learn the distinguishing patterns.
- A webpage is classified as phishing if the model determines its URL and hyperlink features match learned patterns of malicious pages.

5) Message Deletion:

- If a webpage linked in a message is determined to be a phishing attempt, the original message can be quarantined or deleted automatically.

- This prevents the user from engaging with the malicious content and potentially compromising their information.
- Message deletion can happen as soon as the phishing determination is made, before the message reaches the user's inbox.
- Alternatively, suspicious messages could be flagged for review before deletion, in case of potential false positives.

E. Benefits, drawbacks and significance of proposed solution

1) Key benefits

The key benefits of this phishing detection system are its ability to automatically delete phishing messages, avoid reliance on potentially stale external blacklists, improve detection accuracy through machine learning, prevent phishing in real-time before messages reach inboxes, and integrate with existing email infrastructure for multi-layered defense. These capabilities represent a significant advancement over traditional phishing prevention methods.

a) Automated message deletion for phishing:

- If a webpage linked in a message is determined to be a phishing attempt, the original message can be automatically quarantined or deleted
- This prevents the user from engaging with the malicious content and potentially compromising their information
- Message deletion can happen as soon as the phishing determination is made, before the message reaches the user's inbox

b) Reduced reliance on external blacklists:

- The system avoids reliance on external blacklists or databases that may become stale
- It uses only URL and hyperlink-based features extracted from the webpage source code itself, without relying on third-party services
- This allows it to detect new and evolving phishing attempts that may not yet be included in blacklists

c) Improved phishing detection accuracy:

- Combining URL and hyperlink analysis provides more comprehensive coverage and accuracy compared to traditional methods
- Machine learning models are trained on large datasets of known phishing and benign examples to learn distinguishing patterns
- This enables adaptable, automated classification and reduces false positives compared to rule-based approaches

d) Real-time phishing prevention:

- The system proactively detects phishing by analyzing destination webpages, not just message content
- URLs are resolved and webpages analyzed in real-time as messages arrive

- This allows phishing attempts to be blocked before they reach the user's inbox, preventing engagement with malicious content

e) Integration with mail transfer agents or client software:

- The phishing detection system can be integrated into mail transfer agents (MTAs) or email client software
- Integration with MTAs allows scanning and blocking of phishing messages during the email delivery process
- Integration with email clients provides last-mile protection at the user's device level
- This enables a multi-layered defense, protecting at both the server and endpoint

2) Limitations

While the proposed system offers improvements over traditional methods, it still faces challenges in terms of computational efficiency, adaptability to new threats, accuracy trade-offs, dependency on external factors, language coverage, and user behavior. Addressing these limitations will be key to providing robust, real-time phishing protection in the face of ever-evolving attacks.

a) Computational cost and scalability:

- Resolving URLs and analyzing webpages at scale can be computationally expensive
- The system needs to handle a high volume of messages and URLs, which may impact performance and scalability
- Possible delays in message delivery due to the scanning process could affect user experience

b) Constant arms race with attackers:

- Phishers constantly adapt their techniques to evade detection, leading to an ongoing arms race
- The system may struggle to keep up with new phishing patterns and zero-day attacks
- Attackers may find ways to obscure phishing content or mimic benign pages to bypass detection

c) Handling false positives and negatives:

- The system may generate false positives, incorrectly flagging legitimate messages as phishing
- False negatives, where phishing attempts go undetected, are also a risk
- Balancing accuracy and minimizing false positives/negatives is challenging and impacts user trust

d) Dependency on external data sources:

- The system relies on third-party data like WHOIS records, PageRank, etc. for webpage analysis
- Changes or disruptions to these external data sources could affect the system's accuracy and reliability

e) Language and internationalization:

- Phishing attempts in different languages or targeting specific regions may be harder to detect
- The system may need adaptation and training for multilingual and international coverage
- f) *User behavior and social engineering:*
 - No technical solution can completely prevent users from falling for well-crafted social engineering attempts
 - User curiosity, distraction, or lack of caution can lead to clicks on phishing links despite warnings
 - Continuous user education and awareness are still necessary to complement any technical detection system
- g) *Potential privacy concerns:*
 - Analyzing user messages and browsing activity for phishing detection may raise privacy questions
 - Balancing user privacy with effective threat detection needs to be considered
- h) *Staying ahead of evolving threats:*
 - As phishing tactics evolve, the detection system needs continuous updating and retraining
 - Adapting to new phishing patterns and attack vectors requires ongoing effort and resources

3) Significance

The key significance of this phishing detection system is its ability to improve detection accuracy through machine learning, prevent phishing in real-time before messages reach inboxes, automatically delete phishing messages, avoid reliance on stale blacklists, and integrate with existing email infrastructure for comprehensive, multi-layered protection. These capabilities represent a significant advancement over traditional phishing prevention methods in the ongoing battle against increasingly sophisticated phishing attacks.

a) Improved Phishing Detection Accuracy:

- Combining URL and hyperlink analysis provides more comprehensive coverage and accuracy compared to traditional methods

- Machine learning models are trained on large datasets of known phishing and benign examples to learn distinguishing patterns, enabling adaptable, automated classification and reducing false positives

b) Real-Time Phishing Prevention:

- The system proactively detects phishing by analyzing destination webpages, not just message content, in real-time as messages arrive
- This allows phishing attempts to be blocked before they reach user inboxes, preventing engagement with malicious content

c) Automated Message Deletion:

- If a webpage linked in a message is determined to be a phishing attempt, the original message can be automatically quarantined or deleted before reaching the user's inbox
- This prevents users from engaging with the malicious content and potentially compromising their information

d) Reduced Reliance on External Blacklists:

- The system avoids reliance on potentially stale external blacklists by using only URL and hyperlink features extracted from the webpage source code itself
- This allows it to detect new and evolving phishing attempts that may not yet be included in blacklists

e) Integration with Email Infrastructure:

- The phishing detection system can be integrated into mail transfer agents or email client software for server-side scanning or last-mile endpoint protection
- This enables a multi-layered defense, protecting at both the email delivery and user device levels

DETECTING REALTIME PHISHING!

PATENT
US11496512B2



Abstract – This document provides an in-depth analysis of US11496512B2, a patent that outlines innovative techniques for detecting phishing websites. The analysis covers various aspects of the patent, including its technical foundation, implementation strategies, and potential impact on cybersecurity practices. By dissecting the methodology, this document aims to offer a comprehensive understanding of its contributions to enhancing online security.

This analysis provides a qualitative unpacking of US11496512B2, offering insights into its innovative approach to phishing detection. The document not only elucidates the technical underpinnings of the patent but also explores its practical applications, security benefits, and potential challenges. This examination is important for cybersecurity professionals, IT specialists, and stakeholders in various industries seeking to understand and implement advanced phishing detection techniques.

A. Introduction

US20220232015A1 is a patent titled "Detecting Realtime Phishing from a Phished Client or at a Security Server," issued on November 8, 2022. The inventors listed are Jeremy Boyd Richards and Brian James Buck, with the assignee being Lookout, Inc., based in San Francisco, CA. The patent describes a method involving receiving a request for a webpage from a client device at a server, generating and inserting an encoded tracking value into the webpage.

B. Main idea

The proposed solution is focused on improving security protocols to protect against phishing, which is a significant threat in the cybersecurity landscape. The use of an tracking value as described in the patent is a technical measure to track and verify web interactions to prevent unauthorized access or data breaches.

The key points are as follows:

Purpose: a method for detecting real-time phishing attacks, which can be applied when a client device has been phished or at a security server level.

Methodology: the method includes receiving a webpage request from a client device at a server, generating an encoded tracking value (ETV), and inserting this ETV into the webpage.

Application: the proposed solution is part of a broader system aimed at enhancing cybersecurity measures, specifically targeting the detection of phishing attempts in real-time.

Components of the process of functioning of the proposed solution as they occur:

Receiving a Request: A server receives a request for a webpage from a client device.

Generating and Inserting an Encoded Tracking Value (ETV): The server generates an ETV and inserts it into the webpage.

Additional Insertions: The server may perform additional insertions or modifications to the webpage as part of its operation.

C. Proposed solution

The proposed solution introduces a sophisticated method aimed at enhancing cybersecurity by detecting real-time phishing attempts. Below is a detailed exploration of the proposed method, focusing on its three main components: Receiving a Request, Generating and Inserting an Encoded Tracking Value (ETV), and Additional Insertions.

1) Receiving a Request

The initial step involves a server receiving a request for a webpage from a client device. This step is crucial as it establishes communication between the client and the server, setting the stage for the subsequent security measures to be applied. The request reception is the trigger point for the server to initiate the process of securing the webpage and monitoring for phishing activities.

In the context of cybersecurity, the initial request reception is a critical juncture. It is the moment when a server can establish the legitimacy of the interaction and apply appropriate security protocols. By starting the process with the reception of a request, the method ensures that every interaction is considered from a security perspective right from the outset.

This step is foundational to the entire method and involves a server receiving a request for a webpage from a client device.

a) Receiving a Request

Initiation of Communication: The process starts when a first computing device, which could be a user's mobile device or any other client device, initiates a request to access a service. This request is directed towards a server that hosts or controls the service or webpage in question.

Trigger for Security Measures: Upon receiving the request, the server is prompted to take action. This is the point at which security measures are considered and potentially applied. The server's response to this request is not just about

serving the requested webpage but also about ensuring the security of the transaction.

Identification of the Client Device: The server identifies the requesting client device. This identification is crucial for tailoring the security response to the context of the request. For instance, if the client device is known to be secure or has a history of interactions with the server, the security measures might differ compared to an unknown or suspicious device.

Potential for Real-Time Phishing Detection: The request reception is not only about delivering content but also about monitoring for signs of phishing. The server may analyze the request for anomalies or indicators of compromise that suggest a phishing attempt is underway.

Foundation for Encoded Tracking Value (ETV): The reception of the request sets the stage for the next steps in the method, particularly the generation and insertion of an Encoded Tracking Value (ETV). The ETV is a critical component that will be embedded in the webpage in response to the request, providing a means to track the webpage and verify its integrity.

2) Generating and Inserting an Encoded Tracking Value (ETV)

After receiving the webpage request, the server generates an Encoded Tracking Value (ETV) and inserts it into the webpage. The ETV is a unique identifier or marker that serves multiple purposes: **tracking, security and verification**.

This step represents a sophisticated approach to enhancing cybersecurity. By leveraging unique, secure identifiers embedded directly into webpages, this method provides a robust mechanism for real-time phishing detection, integrity verification, and overall enhancement of digital security protocols.

This component is a critical step in the proposed method for enhancing cybersecurity, specifically in the context of real-time phishing detection. This step follows the initial reception of a webpage request from a client device and is pivotal in establishing a mechanism for tracking, security, and verification.

a) Generating an Encoded Tracking Value (ETV)

Creation of the ETV: The server generates an Encoded Tracking Value (ETV) upon receiving a request for a webpage. The ETV is a unique identifier or code that is specifically crafted for the session or interaction. The generation of this value is a sophisticated process that ensures the ETV is secure and difficult to predict or replicate by malicious actors.

Security and Uniqueness: The ETV's design incorporates elements that enhance security, such as encryption or hashing, making it a robust tool against tampering and forgery. The uniqueness of each ETV is crucial for tracking individual webpage requests and responses, ensuring that each interaction can be independently verified.

b) Inserting the ETV into the Webpage

Embedding Process: Once generated, the ETV is inserted into the webpage that is to be served to the requesting client device. This insertion can be done in various ways, such as embedding the ETV within the webpage's code, inserting it as a hidden field, or incorporating it into the webpage's metadata.

Purpose of Insertion: The primary purpose of inserting the ETV into the webpage is to create a traceable link between the server's response and the client's request. This allows the server to verify the integrity and authenticity of the webpage when it is accessed or interacted with by the client device.

c) Role in Phishing Detection

Real-Time Detection: The ETV enables the server to detect phishing attempts in real-time. By verifying the presence and integrity of the ETV in subsequent interactions (such as form submissions or requests for additional resources), the server can identify discrepancies that may indicate a phishing attack.

Verification and Integrity Checking: The ETV acts as a cornerstone for verifying the webpage's integrity. Any alteration or absence of the ETV in expected interactions can trigger alerts or initiate protective measures, thereby preventing phishing attacks from succeeding.

d) Advantages

Enhanced Security: The generation and insertion of an ETV significantly enhance the security of web interactions by adding a layer of verification that is difficult for attackers to bypass.

Flexibility and Adaptability: The method allows for flexibility in how the ETV is generated and inserted, making it adaptable to different web technologies and security requirements.

Proactive Approach: By embedding security directly into the webpage served to the client, the method takes a proactive approach to security, rather than relying solely on reactive measures after an attack has been detected.

3) Additional Insertions

The method also includes the possibility of making additional insertions or modifications to the webpage. These could be further security measures, tracking codes, or any other modifications deemed necessary to enhance the webpage's security and integrity. The flexibility to add more layers of security measures ensures that the method can adapt to evolving cyber threats and phishing techniques.

This component is a crucial aspect of the proposed method for enhancing cybersecurity, particularly in the context of real-time phishing detection. This step builds upon the foundational steps of receiving a webpage request and generating and inserting an Encoded Tracking Value (ETV).

a) Concept of Additional Insertions

After the ETV is generated and inserted into the webpage, the method allows for further modifications or insertions into the webpage. These additional insertions can serve various purposes, enhancing the security, functionality, or user experience of the webpage. The nature of these insertions can vary widely, depending on the specific security requirements, the type of content being served, and the anticipated threats.

b) Types of Additional Insertions

Security Enhancements: Additional security measures, such as more sophisticated tracking codes, scripts for detecting unusual user behavior, or mechanisms for verifying user actions,

can be inserted. These enhancements aim to fortify the webpage against a broader array of cyber threats, including but not limited to phishing.

Content Personalization: Insertions can also include personalized content or features tailored to the user's profile or past interactions with the service. While not directly related to security, personalization can improve user engagement and, by extension, the effectiveness of any security prompts or warnings presented to the user.

User Experience Improvements: Additional scripts or elements that enhance the user experience, such as accessibility features, interactive elements, or dynamic content updates, can be included. Improving the user experience can indirectly contribute to security by making legitimate webpages more distinguishable from phishing attempts.

c) *Significance in Phishing Detection*

The inclusion of additional insertions is particularly relevant in the context of phishing detection for several reasons:

Layered Security Approach: By allowing for multiple layers of security measures, the method creates a more robust defense against phishing and other cyber threats. This layered approach makes it harder for attackers to mimic or bypass the security features of a legitimate webpage.

Adaptability to Emerging Threats: The flexibility to include additional insertions means that the method can be adapted over time to address new or evolving cyber threats. As phishing techniques become more sophisticated, new types of insertions can be developed and deployed to counteract them.

Enhanced Tracking and Analysis: Additional insertions can provide more data points for tracking user interactions and analyzing behavior. This data can be invaluable in identifying suspicious activity that may indicate a phishing attempt or other security threats.

D. *Significance of proposed solution*

The significance of proposed method of solution within the field of cybersecurity, particularly in combating phishing attacks, is multifaceted and profound. This method, which encompasses receiving a webpage request, generating and inserting an Encoded Tracking Value (ETV), and making additional insertions, represents a comprehensive approach to enhancing online security.

It extends beyond its technical merits, representing a shift towards more proactive, adaptive, and user-centric approaches to cybersecurity. By embedding security directly into the fabric of web interactions, the method offers a robust defense against phishing attacks, enhancing the safety and integrity of online spaces. As cyber threats continue to evolve, such innovative approaches will be critical in safeguarding digital assets and building trust in the digital ecosystem.

1) *Proactive Defense Against Phishing*

Phishing attacks have evolved to become highly sophisticated, often bypassing traditional security measures. The proposed method introduces a proactive defense mechanism that actively embeds security within the webpage itself through the use of ETVs and additional insertions. This approach not only

aims to detect phishing attempts as they occur but also to prevent them by making it significantly harder for attackers to replicate or tamper with legitimate webpages.

2) *Enhancing Webpage Integrity and Trust*

By generating and inserting an ETV into the webpage, the method ensures that the integrity of the webpage can be verified at any point in its interaction with the client. This process builds a layer of trust between the server and the client, reassuring users that the content they are interacting with is secure and has not been compromised. This is particularly important in an era where digital trust is paramount to the user experience.

3) *Adaptability to Emerging Threats*

The inclusion of "Additional Insertions" as part of the method allows for a flexible and adaptive security strategy. As cyber threats evolve, new security measures can be developed and seamlessly integrated into the webpage without requiring an overhaul of the existing security infrastructure. This adaptability ensures that the method remains effective against future phishing techniques and other cyber threats.

4) *Real-Time Detection and Response*

One of the standout features of the proposed method is its capability for real-time detection of phishing attempts. By monitoring the integrity of the ETV and the behavior of the webpage in real-time, the system can quickly identify potential phishing activities and respond accordingly. This immediate response capability is crucial for minimizing the impact of phishing attacks on users and organizations.

5) *Contribution to Cybersecurity Research and Practice*

The method contributes to the broader field of cybersecurity research and practice by providing a novel approach to phishing detection and prevention. It offers a practical solution that can be implemented by organizations to protect their online assets and users. Furthermore, the method serves as a foundation for future research and development in the area of web security, encouraging further innovations in the fight against cyber threats.

E. *Potential implications of proposed solution*

It represents a significant step forward in the fight against phishing and cyber threats. Its potential implications for future research are vast, spanning technical advancements in cybersecurity, improvements in user experience, cross-disciplinary applications, and influences on policy and regulation. By laying the groundwork for a more secure and trustworthy digital environment, this method sets the stage for a wide range of research opportunities aimed at further enhancing online security and user trust.

It offers a promising foundation for future research across a range of fields. By providing a novel approach to real-time phishing detection, it not only addresses a critical need in cybersecurity but also opens up new possibilities for advancing research methodologies, enhancing data integrity, fostering interdisciplinary studies, and contributing to better policy and practice in the digital age.

It also focuses on enhancing cybersecurity through real-time phishing detection via encoded tracking values (ETVs) and

additional insertions, holds significant potential implications for future research in several key areas:

1) Advancing Cybersecurity Measures

The method introduces a novel approach to detecting and mitigating phishing attacks in real-time, which could inspire further research into more sophisticated cybersecurity mechanisms. Future studies might explore the optimization of ETV generation and insertion techniques, the development of more advanced algorithms for real-time threat detection, and the integration of machine learning models to predict and prevent phishing attempts more effectively.

2) Enhancing Webpage Integrity Verification

The use of ETVs for verifying the integrity of webpages opens new avenues for research into ensuring the authenticity of digital content. This could lead to the development of new standards and protocols for web security, focusing on the dynamic verification of webpage elements to prevent tampering and unauthorized content modification.

3) Improving User Experience and Trust

The method's emphasis on maintaining the integrity of web interactions without compromising user experience could spur research into user-centric security solutions. Future studies might investigate how security measures like ETVs impact user behavior, trust in digital platforms, and the overall user experience. This research could lead to the design of more intuitive and less intrusive security mechanisms that enhance user engagement while ensuring robust protection against cyber threats.

4) Cross-Disciplinary Applications

The principles underlying the proposed method could have implications beyond cybersecurity, inspiring research in fields such as digital forensics, e-commerce, and online education. For instance, the method's approach to tracking and verifying webpage interactions could be adapted for use in digital forensic investigations, enhancing the ability to trace malicious activities and authenticate digital evidence.

5) Policy and Regulatory Implications

As the method provides a proactive approach to combating phishing, it could influence future policies and regulations related to online security and data protection. Research could explore the implications of widespread adoption of such methods on privacy laws, data protection standards, and regulatory requirements for online services. This could lead to recommendations for policymakers on how to incorporate advanced cybersecurity measures into regulatory frameworks.

F. Potential benefits for future research

It focuses on real-time phishing detection through the generation and insertion of Encoded Tracking Values (ETVs) and additional insertions, offers several potential benefits for future research across various domains. These benefits not only underscore the method's immediate application in enhancing cybersecurity but also highlight its broader implications for advancing research methodologies, improving data integrity, and fostering interdisciplinary studies.

It offers a promising foundation for future research across a range of fields. By providing a novel approach to real-time

phishing detection, it not only addresses a critical need in cybersecurity but also opens up new possibilities for advancing research methodologies, enhancing data integrity, fostering interdisciplinary studies, and contributing to better policy and practice in the digital age.

1) Advancing Cybersecurity Research

The method provides a novel approach to detecting and mitigating phishing attacks, which can serve as a foundation for further research in cybersecurity. It opens up new avenues for exploring how dynamic, real-time detection mechanisms can be developed and integrated into existing security frameworks. Researchers can build on this method to create more sophisticated algorithms and technologies that address the evolving landscape of cyber threats.

2) Enhancing Data Integrity and Trust

By ensuring the integrity of web interactions through ETVs, the proposed method can contribute to research on data integrity and trust in digital environments. This is particularly relevant in fields like e-commerce, online banking, and digital communications, where data authenticity and user trust are paramount. Future studies could explore how similar mechanisms can be applied to other types of digital transactions and interactions to prevent fraud and ensure data integrity.

3) Fostering Interdisciplinary Studies

The method's emphasis on real-time detection and the use of encoded tracking values has implications beyond cybersecurity, potentially benefiting interdisciplinary studies that combine technology with psychology, sociology, and law. For instance, researchers can investigate the psychological aspects of phishing attacks and user responses to security measures, or explore legal frameworks for protecting users and prosecuting attackers.

4) Improving Research Methodologies

The approach can also influence research methodologies, particularly in how data is collected, verified, and analyzed in real-time studies. This could lead to the development of new research tools and techniques that leverage encoded tracking or similar mechanisms to ensure the authenticity and reliability of data collected from online sources or through digital platforms.

5) Contributing to Policy and Practice

Finally, the proposed method has the potential to inform policy-making and best practices in cybersecurity. By demonstrating the effectiveness of real-time phishing detection, future research based on this method could provide evidence-based recommendations for developing stronger cybersecurity policies, regulations, and industry standards. This could help organizations, governments, and individuals better protect themselves against phishing and other cyber threats.

G. Potential limitations for future research

It highlights the importance of ongoing research and development in the field of cybersecurity. Future research will need to address these limitations by exploring the method's scalability, adaptability to evolving threats, user interaction models, analytical accuracy, privacy implications, and generalizability to different platforms and technologies. Acknowledging and addressing these limitations is crucial for

advancing the method's application and for contributing to the broader field of cybersecurity research.

While it offers a novel approach to real-time phishing detection, there are potential limitations that could impact its application in future research:

1) *Methodological Limitations*

Complexity of Implementation: The generation and insertion of ETVs may involve complex algorithms and require significant processing power, which could limit its scalability or applicability in resource-constrained environments.

Evolution of Phishing Tactics: Phishers continuously evolve their tactics to bypass security measures. The method may need to be regularly updated to keep pace with new phishing techniques, which could be a challenge for researchers and practitioners.

2) *Empirical Limitations*

User Behavior and Interaction: The effectiveness of the method may be influenced by user behavior. If users do not interact with the webpage as expected, the ETVs and additional insertions may not function as intended, potentially limiting the method's effectiveness.

False Positives/Negatives: The method could potentially produce false positives or negatives in detecting phishing attempts, which could impact user trust and the overall reliability of the system.

3) *Analytical Limitations*

Data Analysis and Interpretation: The method relies on the analysis of web interactions, which may be subject to interpretation errors. The accuracy of the phishing detection could be limited by the analytical tools and techniques used.

4) *Ethical and Privacy Concerns*

User Privacy: The tracking and analysis of user interactions could raise privacy concerns. Ensuring user consent and maintaining transparency about data usage are essential to address these concerns.

5) *Generalizability*

Applicability Across Different Platforms: The method may have been designed with certain types of webpages or services in mind. Its effectiveness across different platforms, devices, or browsers may be limited and require further research.

6) *Technological Advancements*

Adaptation to New Technologies: As web technologies evolve, the method may need to be adapted to remain effective. This could involve research into how the method can be applied to new web standards or technologies.

H. Conclusion

The proposed solution presents a method that significantly contributes to the field of cybersecurity by offering a proactive and dynamic approach to detecting and preventing phishing attacks in real-time. By focusing on the interaction between the client device and the server and utilizing an Encoded Tracking Value (ETV) along with the potential for additional security insertions, this method provides a robust framework for enhancing the security of web communications. This approach not only helps in identifying phishing attempts as they happen but also adds a layer of verification and integrity checking that is crucial in the current digital age, where phishing attacks are becoming increasingly sophisticated and harder to detect.

DATABRICKS AI SECURITY FRAMEWORK (DASF)



Abstract – This document provides an in-depth analysis of the DASF, exploring its structure, recommendations, and the practical applications it offers to organizations implementing AI solutions. This analysis not only serves as a quality examination but also highlights its significance and practical benefits for security experts and professionals across different sectors. By implementing the guidelines and controls recommended by the DASF, organizations can safeguard their AI assets against emerging threats and vulnerabilities.

A. Introduction

The Databricks AI Security Framework (DASF) is a comprehensive guide designed to address the evolving risks associated with the widespread integration of AI globally. The framework is created by the Databricks Security team and aims to provide actionable defensive control recommendations for AI systems, covering the entire AI lifecycle and facilitating collaboration between business, IT, data, AI, and security teams. The DASF is not limited to securing models or endpoints but adopts a holistic approach to mitigate cyber risks in AI systems, based on real-world evidence indicating that attackers employ simple tactics to compromise ML-driven systems.

The DASF identifies 55 technical security risks across 12 foundational components of a generic data-centric AI system, including raw data, data prep, datasets, data catalog governance, machine learning algorithms, evaluation, machine learning models, model management, model serving and inference, inference response, machine learning operations (MLOps), and data and AI platform security. Each risk is mapped to a set of mitigation controls that are ranked in prioritized order, starting with perimeter security to data security.

The Databricks Data Intelligence Platform is highlighted as a key component of the DASF, offering a unified foundation for all data and governance. The platform includes Mosaic AI, Databricks Unity Catalog, Databricks Platform Architecture, and Databricks Platform Security. Mosaic AI covers the end-to-end AI workflow, while Unity Catalog provides a unified

governance solution for data and AI assets. The platform architecture is a hybrid PaaS that is data-agnostic, and the platform security is based on trust, technology, and transparency principles.

The DASF is intended for security teams, ML practitioners, governance officers, and DevSecOps engineering teams. It provides a structured conversation on new threats and mitigations without requiring deep expertise crossover. The DASF also includes a detailed guide for understanding the security and compliance of specific ML systems, offering insights into how ML impacts system security, applying security engineering principles to ML, and providing a detailed guide for understanding the security and compliance of specific ML systems.

The DASF concludes with Databricks' final recommendations on how to manage and deploy AI models safely and securely, consistent with the core tenets of machine learning adoption: identify the ML business use case, determine the ML deployment model, select the most pertinent risks, enumerate threats for each risk, and choose which controls to implement. It also provides further reading to enhance knowledge of the AI field and the frameworks reviewed as part of the analysis.

DASF document serves as a guide for how organizations can effectively utilize the framework to enhance the security of their AI systems, promoting a collaborative and comprehensive approach to AI security across various teams and AI model types:

- **Collaborative Use:** The DASF is designed for collaborative use by data and AI teams along with their security counterparts. It emphasizes the importance of these teams working together throughout the AI lifecycle to ensure the security and compliance of AI systems.
- **Applicability Across Teams:** The concepts in the DASF are applicable to all teams, regardless of whether they use Databricks to build their AI solutions. This inclusivity ensures that the framework can be utilized by a broad audience to enhance AI security.
- **Guidance on AI Model Types:** The document suggests that organizations first identify what types of AI models are being built or used. It categorizes models broadly into predictive ML models, state-of-the-art open models, and external models, providing a framework for understanding the specific security considerations for each type.
- **Understanding AI System Components:** Organizations are encouraged to review the 12 foundational components of a generic data-centric AI system as outlined in the document.
- **Risk Identification and Mitigation:** The DASF guides organizations to identify relevant risks and determine applicable controls from a comprehensive list provided in the document. This structured approach helps in prioritizing security measures based on the specific needs of the organization.

- **Documentation and Features in Databricks Terminology:** While the document refers to documentation or features in Databricks terminology, it aims to be accessible to those who do not use Databricks. This approach helps in making the document useful for a wider audience while maintaining its practicality for Databricks users.

B. Audience

- **Security Teams:** This includes Chief Information Security Officers (CISOs), security leaders, DevSecOps, Site Reliability Engineers (SREs), and others responsible for the security of systems. They can use the DASF to understand how machine learning (ML) will impact system security and to grasp some of the basic mechanisms of ML.
- **ML Practitioners and Engineers:** This group comprises data engineers, data architects, ML engineers, and data scientists. The DASF helps them understand how security engineering and the "secure by design" mentality can be applied to ML.
- **Governance Officers:** These individuals are responsible for ensuring that data and AI practices within an organization comply with relevant laws, regulations, and policies. The DASF provides guidance on how ML impacts system security and compliance.
- **DevSecOps Engineering Teams:** These teams focus on integrating security into the development and operations processes. The DASF offers a structured way for these teams to have conversations about new threats and mitigations without requiring deep expertise crossover.

C. Benefits and Drawbacks

Databricks AI Security Framework (DASF) offers a comprehensive and actionable guide for organizations looking to understand and mitigate AI security risks. However, its complexity and Databricks-centric guidance may present challenges for some organizations.

1) Benefits

- **Holistic approach:** The DASF takes a holistic approach to AI security, addressing risks across the entire AI lifecycle and all components of a generic data-centric AI system. This comprehensive approach helps organizations identify and mitigate security risks more effectively.
- **Collaboration:** The framework is designed to facilitate collaboration between business, IT, data, AI, and security teams. This encourages a unified approach to AI security and helps bridge the gap between different disciplines.
- **Actionable recommendations:** The DASF provides actionable defensive control recommendations for each identified risk, which can be updated as new risks emerge and additional controls become available. This ensures that organizations can stay current with evolving AI security threats.

- **Applicability:** The DASF is applicable to organizations using various AI models, including predictive ML models, generative AI models, and external models. This broad applicability makes it a valuable resource for a wide range of organizations.
- **Integration with Databricks Data Intelligence Platform:** For organizations using the Databricks Data Intelligence Platform, the DASF offers specific guidance on leveraging the platform's AI risk mitigation controls. This helps organizations maximize the security benefits of the platform.

2) Drawbacks

- **Complexity:** The DASF covers a wide range of AI security risks and mitigation controls, which may be overwhelming for organizations new to AI security or with limited resources. Implementing the framework may require a significant investment of time and effort.
- **Databricks-centric guidance:** While the DASF offers valuable guidance for organizations using the Databricks Data Intelligence Platform, some of the recommendations may be less applicable or actionable for organizations using different AI platforms or tools.
- **Evolving landscape:** As the AI security landscape continues to evolve, organizations may need to continually update their security controls and practices to stay current.
- **Lack of specific examples:** The DASF provides a high-level overview of AI security risks and mitigation controls, but it may lack specific examples or case studies to illustrate how these risks and controls apply in real-world scenarios.
- **Focus on technical risks:** The DASF primarily focuses on technical security risks and mitigation controls. While this is an essential aspect of AI security, organizations should also consider non-technical risks, such as ethical, legal, and social implications of AI, which are not extensively covered in the DASF.

D. Framework Alignment

The Databricks AI Security Framework (DASF) is designed to complement and integrate with other security frameworks, such as NIST, HITRUST, ISO/IEC 27001 and 27002, and CIS Critical Security Controls. The DASF takes a holistic approach to mitigating AI security risks instead of focusing only on the security of models or model endpoints. This approach aligns with the principles of these frameworks, which provide a structured process for identifying, assessing, and mitigating cybersecurity risks.

E. Databricks AI Security Framework

The framework categorizes the AI system into 12 primary components, each associated with specific security risks identified through extensive analysis. This analysis includes predictive ML models, generative foundation models, and external models, informed by customer inquiries, security assessments, workshops with Chief Information Security Officers (CISOs), and surveys on AI risks. The identified risks

are then mapped to corresponding mitigation controls within the Databricks Data Intelligence Platform, with links to detailed product documentation for each risk.

The document outlines the AI system components, and their associated risks as follows:

- **Data Operations:** This stage encompasses the initial handling of raw data, including ingestion, transformation, and ensuring data security and governance. It is crucial for the development of reliable ML models and a secure DataOps infrastructure. A total of 19 specific risks are identified in this category, ranging from insufficient access controls to lack of end-to-end ML lifecycle management.
- **Model Operations:** This stage involves the creation of ML models, whether through building predictive models, acquiring models from marketplaces, or utilizing APIs like OpenAI. It requires a series of experiments and tracking mechanisms to compare various conditions and outcomes. There are 14 specific risks identified, including issues like lack of experiment reproducibility and model drift.
- **Model Deployment and Serving:** This stage focuses on securely deploying model images, serving models, and managing features such as automated scaling and rate limiting. It also includes the provision of high-availability services for structured data in RAG applications. A total of 15 specific risks are highlighted, including prompt injection and model inversion.
- **Operations and Platform:** This final stage includes platform vulnerability management, patching, model isolation, and ensuring authorized access to models with security built into the architecture. It also involves operational tooling for CI/CD to maintain secure MLOps across development, staging, and production environments. Seven specific risks are identified, such as lack of MLOps standards and vulnerability management.

F. Raw data

- **Importance of Raw Data:** Raw data is the foundation of AI systems, encompassing enterprise data, metadata, and operational data in various forms such as semi-structured or unstructured data, batch data, or streaming data.
- **Data Security:** Securing raw data is paramount for the integrity of machine learning algorithms and any technical deployment particulars. It presents unique challenges, and all data collections in an AI system are subject to standard data security challenges as well as new ones.
- **Risk Mitigation Controls:** The document outlines specific risks associated with raw data and provides detailed mitigation controls for each. These controls include effective access management, data classification, data quality enforcement, storage and encryption, data versioning, data lineage, data

trustworthiness, legal considerations, handling stale data, and data access logs.

- **Access Management:** Ensuring that only authorized individuals or groups can access specific datasets is fundamental to data security. This involves authentication, authorization, and finely tuned access controls.
- **Data Classification:** Classifying data is critical for governance, enabling organizations to sort and categorize data by sensitivity, importance, and criticality, which is essential for implementing appropriate security measures and governance policies.
- **Data Quality:** High data quality is crucial for reliable data-driven decisions and is a cornerstone of data governance. Organizations must rigorously evaluate key data attributes to ensure analytical accuracy and cost-effectiveness.
- **Storage and Encryption:** Encrypting data at rest and in transit is vital to protect against unauthorized access and to comply with industry-specific data security regulations.
- **Data Versioning and Lineage:** Versioning data and tracking change logs are important for rolling back or tracing back to the original data in case of corruption. Data lineage helps with compliance and audit-readiness by providing a clear understanding and traceability of data used for AI.
- **Trustworthiness and Legal Aspects:** Ensuring the trustworthiness of data and compliance with legal mandates such as GDPR and CCPA is essential. This includes the ability to "delete" specific data from machine learning systems and retrain models using clean and ownership-verified datasets.
- **Stale Data and Access Logs:** Addressing the risks of stale data and the lack of data access logs is important for maintaining the efficiency and security of business processes. Proper audit mechanisms are critical for data security and regulatory compliance.

G. Data Prep

- **Definition and Importance:** Data preparation is defined as the process of transforming raw input data into a format that machine learning algorithms can interpret. This stage is crucial as it directly impacts the security and explainability of an ML system.
- **Security Risks and Mitigations:** The section outlines various security risks associated with data preparation and provides detailed mitigation controls for each. These risks include preprocessing integrity, feature manipulation, raw data criteria, and adversarial partitions.
- **Preprocessing Integrity:** Ensuring the integrity of preprocessing involves numerical transformations, data aggregation, text or image data encoding, and new feature creation. Mitigation controls include setting up Single Sign-On (SSO) with Identity Provider (IdP) and Multi-

Factor Authentication (MFA), restricting access using IP access lists, and implementing private links to limit the source for inbound requests.

- **Feature Manipulation:** This risk involves the potential for attackers to manipulate how data is annotated into features, which can compromise the integrity and accuracy of the model. Controls include securing model features to prevent unauthorized updates and employing data-centric MLOps and LLMOps to promote models as code.
- **Raw Data Criteria:** Understanding the selection criteria for raw data is essential to prevent attackers from introducing malicious input that compromises system integrity. Controls include using access control lists and data-centric MLOps for unit and integration testing.
- **Adversarial Partitions:** This involves the risk of attackers influencing the partitioning of datasets used in training and evaluation, potentially controlling the ML system indirectly. Mitigation involves tracking and reproducing the training data used for ML model training and identifying ML models and runs derived from a particular dataset.
- **Comprehensive Mitigation Strategies:** The section emphasizes the importance of a comprehensive approach to securing the data preparation process, including the use of stringent security measures to safeguard against manipulations that can undermine the integrity and reliability of ML systems

H. Datasets

- **Significance of Datasets:** Datasets are crucial for training, validating, and testing machine learning models. They must be carefully managed to ensure the integrity and effectiveness of the AI systems.
- **Security Risks:** The section outlines various security risks associated with datasets, including data poisoning, ineffective storage and encryption, and label flipping. These risks can compromise the reliability and performance of machine learning models.
- **Data Poisoning:** This risk involves attackers manipulating training data to affect the model's output at the inference stage. Mitigation strategies include robust access controls, data quality checks, and monitoring data lineage to prevent unauthorized data manipulation.
- **Ineffective Storage and Encryption:** Proper data storage and encryption are critical to protect datasets from unauthorized access and breaches. The framework recommends encryption of data at rest and in transit, along with stringent access controls.
- **Label Flipping:** This specific type of data poisoning involves changing the labels in training data, which can mislead the model during training and degrade its performance. Encryption and secure access to datasets are recommended to mitigate this risk.

- **Mitigation Controls:** For each identified risk, the DASF provides detailed mitigation controls. These controls include the use of Single Sign-On (SSO) with Identity Providers (IdP), Multi-Factor Authentication (MFA), IP access lists, private links, and data encryption to enhance the security of datasets.
- **Comprehensive Risk Management:** The section emphasizes the importance of a comprehensive approach to managing dataset security, from the initial data collection to the deployment of machine learning models. This includes regular audits, updates to security protocols, and continuous monitoring of data integrity.

I. Data Catalog Governance

- **Comprehensive Governance Approach:** Data catalog and governance involve managing an organization's data assets throughout their lifecycle, which includes principles, practices, and tools for effective management.
- **Centralized Access Control:** Managing governance for data and AI assets enables centralized access control, auditing, lineage, data, and model discovery capabilities, which limits the risk of data or model duplication, improper use of classified data for training, loss of provenance, and model theft.
- **Data Privacy and Security:** When dealing with datasets that may contain sensitive information, it is crucial to ensure that personally identifiable information (PII) and other sensitive data are adequately secured to prevent breaches and leaks. This is particularly important in sectors with stringent regulatory requirements.
- **Audit Trails and Transparency:** Proper data catalog governance allows for audit trails and tracing the origin and transformations of data used to train AI models. This transparency encourages trust and accountability, reduces the risk of biases, and improves AI outcomes.
- **Regulatory Compliance:** Ensuring that sensitive information in datasets is adequately secured is essential for compliance with regulations such as GDPR and CCPA. This includes the ability to demonstrate data security and maintain audit trails.
- **Collaborative Dashboard:** For computer vision projects involving multiple stakeholders, having an easy-to-use labeling tool with a collaborative dashboard is essential to keep everyone on the same page in real-time and avoid mission creep.
- **Automated Data Pipelines:** For projects with large volumes of data, automating data pipelines by connecting datasets and models using APIs can streamline the process and make it faster to train ML models.
- **Quality Control Workflows:** It is important to have customizable and manageable quality control workflows to validate labels and annotations, reduce errors and bias, and fix bugs in datasets. Automated annotation tools can help in this process

J. Machine Learning Algorithms

- **Technical Core of ML Systems:** Machine learning algorithms are described as the technical core of any ML system, crucial for the functionality and security of the system.
- **Lesser Security Risk:** It is noted that attacks against machine learning algorithms generally present significantly less security risk compared to the data used for training, testing, and eventual operation.
- **Offline and Online Systems:** The section distinguishes between offline and online machine learning algorithms. Offline systems are trained on a fixed dataset and then used for predictions, while online systems continuously learn and adapt through iterative training with new data.
- **Security Advantages of Offline Systems:** Offline systems are said to have certain security advantages due to their fixed, static nature, which reduces the attack surface and minimizes exposure to data-borne vulnerabilities over time.
- **Vulnerabilities of Online Systems:** Online systems are constantly exposed to new data, which increases their susceptibility to poisoning attacks, adversarial inputs, and manipulation of learning processes.
- **Careful Selection of Algorithms:** The document emphasizes the importance of carefully considering the choice between offline and online learning algorithms based on the specific security requirements and operating environment of the ML system

K. Evaluation

- **Critical Role of Evaluation:** Evaluation is essential for assessing the effectiveness of machine learning systems in achieving their intended functionalities. It involves using dedicated datasets to systematically analyze the performance of a trained model on its specific task.
- **Evaluation Data Poisoning:** There is a risk of upstream attacks against data, where the data is tampered with before it is used for machine learning, significantly complicating the training and evaluation of ML models. These attacks can corrupt or alter the data in a way that skews the training process, leading to unreliable models.
- **Insufficient Evaluation Data:** Evaluation datasets can also be too small or too similar to the training data to be useful. Poor evaluation data can lead to biases, hallucinations, and toxic output. It is difficult to effectively evaluate large language models (LLMs), as these models rarely have an objective ground truth labeled.
- **Mitigation Controls:**
 - Implementing Single Sign-On (SSO) with Identity Provider (IdP) and Multi-Factor Authentication (MFA) to limit who can access your data and AI platform.

- Using IP access lists to restrict the IP addresses that can authenticate to Databricks.
- Encrypting data at rest and in transit.
- Monitoring data and AI system from a single pane of glass for changes and take action when changes occur.
- **Importance of Robust Evaluation:** Effective evaluation is crucial for ensuring the reliability and accuracy of machine learning models. It helps in identifying discrepancies or anomalies in the model's decision-making process and provides insights into the model's performance.

L. Machine Learning Models

- **Model Security:** Machine learning models are the core of AI systems, and their security is crucial to ensure the integrity and reliability of the system. The section discusses various risks associated with machine learning models and provides mitigation controls for each risk.
- **Backdoor Machine Learning/Trojaned Model:** This risk involves an attacker embedding a backdoor in the model during training, which can be exploited later to manipulate the model's behavior. Mitigation controls include monitoring model performance, using robust training data, and implementing access controls.
- **Model Asset Leak:** This risk involves the unauthorized disclosure of model assets, such as model architecture, weights, and training data. Mitigation controls include encryption, access control, and monitoring for unauthorized access.
- **ML Supply Chain Vulnerabilities:** This risk arises from vulnerabilities in the ML supply chain, such as third-party libraries and dependencies. Mitigation controls include regular vulnerability assessments, using trusted sources, and implementing secure development practices.
- **Source Code Control Attack:** This risk involves an attacker gaining unauthorized access to the source code repository and modifying the code to introduce vulnerabilities or backdoors. Mitigation controls include access control, code review, and monitoring for unauthorized access.
- **Model Attribution:** This risk involves the unauthorized use of a model without proper attribution to its original creators. Mitigation controls include using digital watermarking, maintaining proper documentation, and enforcing licensing agreements.
- **Model Theft:** This risk involves an attacker stealing a model by reverse-engineering its behavior or directly accessing its code. Mitigation controls include encryption, access control, and monitoring for unauthorized access.
- **Model Lifecycle without HITL:** This risk arises from the lack of human-in-the-loop (HITL) involvement in the model lifecycle, which can lead to biased or incorrect

predictions. Mitigation controls include regular model validation, human review, and continuous monitoring.

- **Model Inversion:** This risk involves an attacker inferring sensitive information about the training data by analyzing the model's behavior. Mitigation controls include using differential privacy, access control, and monitoring for unauthorized access.

M. Model Management

- **Model Management Overview:** Model management is the process of organizing, tracking, and maintaining machine learning models throughout their lifecycle, from development to deployment and retirement.
- **Security Risks:** The section outlines various security risks associated with model management, including model attribution, model theft, model lifecycle without human-in-the-loop (HITL), and model inversion.
- **Model Attribution:** This risk involves the unauthorized use of a model without proper attribution to its original creators. Mitigation controls include using digital watermarking, maintaining proper documentation, and enforcing licensing agreements.
- **Model Theft:** This risk involves an attacker stealing a model by reverse-engineering its behavior or directly accessing its code. Mitigation controls include encryption, access control, and monitoring for unauthorized access.
- **Model Lifecycle without HITL:** This risk arises from the lack of human-in-the-loop (HITL) involvement in the model lifecycle, which can lead to biased or incorrect predictions. Mitigation controls include regular model validation, human review, and continuous monitoring.
- **Model Inversion:** This risk involves an attacker inferring sensitive information about the training data by analyzing the model's behavior. Mitigation controls include using differential privacy, access control, and monitoring for unauthorized access.
- **Mitigation Controls:** For each identified risk, the DASF provides detailed mitigation controls. These controls include the use of Single Sign-On (SSO) with Identity Providers (IdP), Multi-Factor Authentication (MFA), IP access lists, private links, and data encryption to enhance the security of model management.
- **Comprehensive Risk Management:** The section emphasizes the importance of a comprehensive approach to managing model security, from the initial development to the deployment and retirement of machine learning models. This includes regular audits, updates to security protocols, and continuous monitoring of model integrity.

N. Model Serving and Inference Requests

- **Model Serving:** Model serving is the process of deploying a trained machine learning model in a production environment to generate predictions on new data.

- **Inference Requests:** Inference requests are the input data sent to the deployed model for generating predictions.
- **Security Risks:** The section outlines various security risks associated with model serving and inference requests, including prompt injection, model inversion, model breakout, looped input, inferring training data membership, discovering ML model ontology, denial of service (DoS), LLM hallucinations, input resource control, and accidental exposure of unauthorized data to models.
- **Prompt Injection:** This risk involves an attacker injecting malicious input into the model to manipulate its behavior or extract sensitive information.
- **Model Inversion:** This risk involves an attacker attempting to reconstruct the original training data or sensitive features by observing the model's output.
- **Model Breakout:** This risk involves an attacker exploiting vulnerabilities in the model serving environment to gain unauthorized access to the underlying system or data.
- **Looped Input:** This risk involves an attacker submitting repeated or looped input to the model to cause resource exhaustion or degrade the system's performance.
- **Inferring Training Data Membership:** This risk involves an attacker attempting to determine whether a specific data point was used in the model's training data.
- **Discovering ML Model Ontology:** This risk involves an attacker attempting to extract information about the model's internal structure or functionality.
- **Denial of Service (DoS):** This risk involves an attacker submitting a large volume of inference requests to overwhelm the model serving infrastructure and cause service disruption.
- **LLM Hallucinations:** This risk involves the model generating incorrect or misleading output due to the inherent uncertainty or limitations of the underlying algorithms.
- **Input Resource Control:** This risk involves an attacker manipulating the input data to consume excessive resources during the inference process.
- **Accidental Exposure of Unauthorized Data to Models:** This risk involves unintentionally exposing sensitive or unauthorized data to the model during the inference process.

O. Model Serving and Inference Response

- **Model Serving:** Model serving is the process of deploying a trained machine learning model in a production environment to generate predictions on new data.

- **Inference Response:** Inference response refers to the output generated by the deployed model in response to the input data sent for prediction.
- **Security Risks:** The section outlines various security risks associated with model serving and inference response, including lack of audit and monitoring, inference quality, output manipulation, discovering ML model ontology, discovering ML model family, and black-box attacks.
- **Lack of Audit and Monitoring Inference Quality:** This risk involves the absence of proper monitoring and auditing mechanisms to ensure the quality and accuracy of the model's predictions.
- **Output Manipulation:** This risk involves an attacker manipulating the model's output to cause incorrect or misleading predictions.
- **Discovering ML Model Ontology:** This risk involves an attacker attempting to extract information about the model's internal structure or functionality by analyzing the output.
- **Discovering ML Model Family:** This risk involves an attacker attempting to identify the specific type or family of the model used in the system by analyzing the output.
- **Black-Box Attacks:** This risk involves an attacker exploiting the model's vulnerabilities by treating it as a black box and manipulating the input data to generate desired outputs.
- **Mitigation Controls:** For each identified risk, the DASF provides detailed mitigation controls. These controls include the use of Single Sign-On (SSO) with Identity Providers (IdP), Multi-Factor Authentication (MFA), IP access lists, private links, and data encryption to enhance the security of model serving and inference response

P. Machine Learning Operations (MLOps)

- **MLOps Definition:** MLOps is the practice of combining Machine Learning (ML), DevOps, and Data Engineering to automate and standardize the process of deploying, maintaining, and updating ML models in production environments.
- **Security Risks:** The section outlines various security risks associated with MLOps, including lack of MLOps, repeatable enforced standards, and lack of compliance.
- **Lack of MLOps:** This risk involves the absence of a standardized and automated process for deploying, maintaining, and updating ML models, which can lead to inconsistencies, errors, and security vulnerabilities.
- **Repeatable Enforced Standards:** Enforcing repeatable standards is crucial for ensuring the security and reliability of ML models in production environments. This includes implementing version control, automated testing, and continuous integration and deployment (CI/CD) pipelines.

- **Lack of Compliance:** This risk involves the failure to comply with relevant regulations and industry standards, which can result in legal and financial consequences for the organization.
- **Mitigation Controls:** For each identified risk, the DASF provides detailed mitigation controls. These controls include the use of Single Sign-On (SSO) with Identity Providers (IdP), Multi-Factor Authentication (MFA), IP access lists, private links, and data encryption to enhance the security of MLOps

Q. Data and AI Platform Security

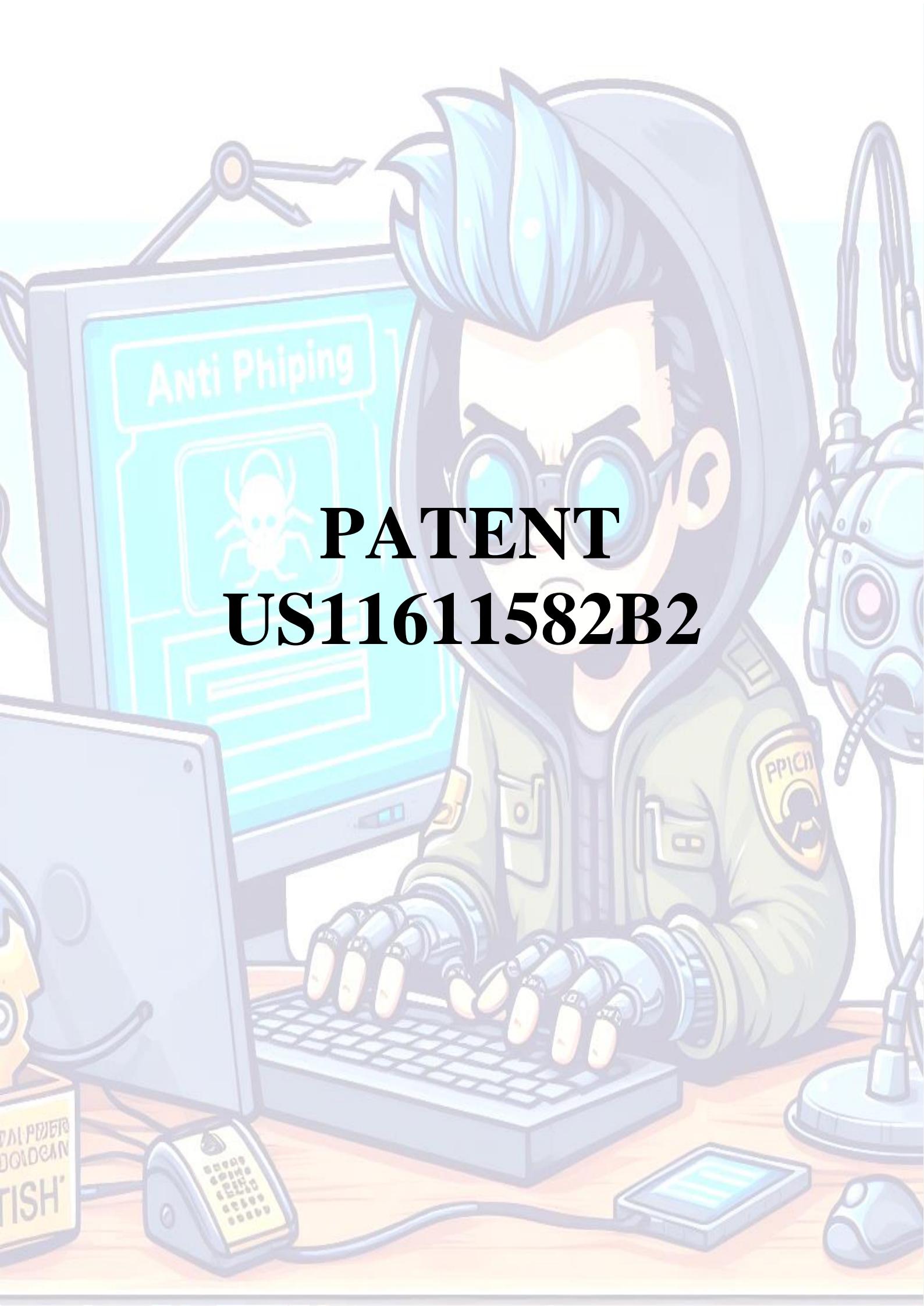
- **Inherent Risks and Rewards:** The choice of platform used for building and deploying AI models can have inherent risks and rewards. Real-world evidence suggests that attackers often use simple tactics to compromise ML-driven systems.
- **Lack of Incident Response:** AI/ML applications are mission-critical for businesses, and platform vendors must address security issues quickly and effectively. A combination of automated monitoring and manual analysis is recommended to address general and ML-specific threats (DASF 39 Platform security — Incident Response Team).
- **Unauthorized Privileged Access:** Malicious internal actors, such as employees or contractors, can pose a significant security threat. They might gain unauthorized access to private training data or ML models, leading to data breaches, leakage of sensitive information, business process abuses, and potential sabotage of ML systems. Implementing stringent internal security measures and monitoring protocols is crucial to mitigate insider risks (DASF 40 Platform security — Internal access).
- **Poor Security in the Software Development Lifecycle (SDLC):** Software platform security is an important part of any progressive security program. Hackers often exploit bugs in the platform where AI is built. The security of AI depends on the platform's security (DASF 41 Platform security — secure SDLC).
- **Lack of Compliance:** As AI applications become more prevalent, they are increasingly subject to scrutiny and regulations such as GDPR and CCPA. Utilizing a compliance-certified platform can be a significant advantage for organizations, as these platforms are specifically designed to meet regulatory standards and provide essential tools and resources to help organizations build and deploy AI applications that are compliant with these laws

R. Databricks Data Intelligence Platform

The Databricks Data Intelligence Platform is a comprehensive solution for AI and data management.

- **Mosaic AI:** This component of the platform covers the end-to-end AI workflow, from data preparation to model deployment and monitoring.

- **Databricks Unity Catalog:** This is a unified governance solution for data and AI assets. It provides data discovery, data lineage, and fine-grained access control.
 - **Databricks Platform Architecture:** The platform architecture is a hybrid PaaS that is data-agnostic, supporting a wide range of data types and sources.
 - **Databricks Platform Security:** The security of the platform is based on trust, technology, and transparency principles. It includes features like encryption, access control, and monitoring.
 - **AI Risk Mitigation Controls:** Databricks has identified 55 technical security risks across 12 foundational components of a generic data-centric AI system. For each risk, the platform provides a guide to the AI and ML mitigation control, its shared responsibility between Databricks and the organization, and the associated Databricks technical documentation.
- S. Databricks AI Risk Mitigation Controls*
- **Databricks AI Risk Mitigation Controls:** Databricks has identified 55 technical security risks across 12 foundational components of a generic data-centric AI system. For each risk, the DASF provides a guide to the AI and ML mitigation control, its shared responsibility between Databricks and the organization, and the associated Databricks technical documentation.
- **Shared Responsibility:** The responsibility for implementing the mitigation controls is shared between Databricks and the organization using the platform. Databricks provides the tools and resources needed to implement the controls, while the organization is responsible for configuring and managing them according to their specific needs.
 - **Comprehensive Approach:** The Databricks AI risk mitigation controls cover a wide range of security risks, from data security and access control to model deployment and monitoring. This comprehensive approach helps organizations reduce overall risk in their AI system development and deployment processes.
 - **Applicability:** The Databricks AI risk mitigation controls are applicable to all types of AI models, including predictive ML models, generative AI models, and external models. This ensures that organizations can implement the appropriate controls based on the specific AI models they are using.
 - **Effort Estimation:** Each control is tagged as "Out-of-the-box," "Configuration," or "Implementation," helping teams estimate the effort involved in implementing the control on the Databricks Data Intelligence Platform. This allows organizations to prioritize their security efforts and allocate resources effectively



PATENT

US11611582B2



Abstract – This document will provide a analysis of patent US11611582B2, which describes a computer-implemented method for detecting phishing threats. The analysis will cover various aspects of the patent, including its technical details, potential applications, and implications for cybersecurity professionals and other industry sectors.

Furthermore, it has a relevance to the evolving landscape of DevSecOps underscores its potential to contribute to more secure and efficient software development lifecycles as it offers a methodical approach to phishing detection that can be adopted by various tools and services to safeguard users and organizations from malicious online activities. Cybersecurity professionals should consider integrating such methods into their defensive strategies to stay ahead of emerging threats.

A. Introduction

The patent US20220232015A1 describes a method for dynamically detecting phishing threats using a pre-defined statistical model. This method is a machine learning based technique to dynamically analyze network requests in real-time and flag potential phishing attempts, in order to proactively protect users and systems from phishing attacks. The statistical model and feature set allow adapting to new phishing patterns.

B. Main idea

The main idea of the patent is to provide a scalable and automated approach to detect phishing attempts in real-time using machine learning, with the goal of proactively protecting users from falling victim to increasingly sophisticated phishing attacks. The dynamic analysis of web request attributes allows identifying new phishing sites that static lists may miss.

- The patent describes a computer-implemented method for dynamically detecting phishing threats using a pre-defined statistical model. The goal is to determine in real-time if a requested network resource is a potential phishing threat.

- When a request to access a network resource is received, a set of features associated with the request are extracted. These features may include the fully qualified domain name (FQDN), age of the domain, domain registrar, IP address, geographic location, etc.
- The extracted features are fed into a pre-trained statistical model which outputs a probability score indicating the likelihood that the requested resource is a phishing threat. If the score exceeds a pre-defined threshold, an alert is generated.
- The statistical model is trained using machine learning techniques on datasets containing known phishing and non-phishing examples. It can be periodically updated with new training data to adapt to evolving phishing patterns.

C. Industries

The specific implementation details and integration points will vary based on each industry's unique requirements and existing technology stack. However, the core capabilities of dynamic phishing detection using machine learning can be tailored to deliver significant security benefits in a wide range of sectors facing the growing threat of phishing attacks.

1) Telecommunications:

Telecom companies can integrate the phishing detection system into their network infrastructure to protect customers from phishing attacks delivered via SMS, MMS, or other messaging services.

The real-time detection capabilities can help block phishing links before they reach end-users, reducing the risk of account compromise and identity theft.

Telecom providers can offer phishing protection as a value-added service to differentiate themselves in the market and build customer trust.

2) Information Technology:

IT companies can deploy phishing detection solutions as part of their cybersecurity offerings to clients, helping protect against phishing attacks targeting employees and customers.

Managed Security Service Providers (MSSPs) can integrate the technology into their threat monitoring and incident response services to detect and block phishing attempts in real-time.

Software-as-a-Service (SaaS) providers can embed the phishing detection into their platforms to scan for suspicious URLs and attachments, enhancing the security of their applications.

3) Finance:

Financial institutions can use the phishing detection system to protect their customers from targeted phishing attacks aimed at stealing login credentials, credit card numbers, and other sensitive financial data.

The solution can be integrated into online banking platforms, mobile apps, and email systems to scan for and flag potential phishing attempts in real-time.

By proactively detecting and blocking phishing threats, financial firms can reduce fraud losses, maintain customer trust, and comply with regulatory requirements for data protection.

4) Healthcare:

Healthcare organizations can leverage the phishing detection technology to safeguard sensitive patient data and prevent phishing attacks that could compromise the confidentiality, integrity, and availability of healthcare systems.

The solution can be deployed to monitor email communications, patient portals, and other digital channels for signs of phishing attempts targeting healthcare staff or patients.

By detecting and blocking phishing threats, healthcare providers can mitigate the risk of data breaches, protect patient privacy, and ensure the continuity of critical healthcare services.

5) E-commerce:

Online retailers can integrate the phishing detection capabilities into their e-commerce platforms to protect customers from phishing attacks that could lead to account takeover, fraudulent transactions, and identity theft.

The real-time detection can help identify and block phishing attempts delivered via fake order confirmation emails, account verification requests, or customer support inquiries.

By proactively addressing phishing threats, e-commerce companies can maintain customer trust, reduce chargebacks and fraud losses, and safeguard their brand reputation.

D. The proposed solution

The key aspects are extracting relevant features from web requests, using a trained statistical model to score the requests, updating the model over time, and generating alerts when the score exceeds a threshold. This allows dynamic and adaptive detection of phishing threats. The key components of the method are:

Feature Extraction:

- When a request to access a network resource is received, a set of features associated with the request are extracted.
- These features may include the fully qualified domain name (FQDN), age of the domain, domain registrar, IP address, geographic location, etc.
- Feature extraction allows representing the key attributes of the web request that can indicate if it is a potential phishing attempt.

Statistical Model:

- The extracted features are fed into a pre-trained statistical model which outputs a probability score.
- The model is trained using machine learning techniques on datasets containing known phishing and non-phishing examples.
- Various ML models like logistic regression, decision trees, neural networks etc. can be used.
- The model learns the patterns and combinations of feature values that are indicative of phishing.

Model Training and Updating:

- The statistical model is initially trained on a labeled dataset before deployment.
- It can be periodically retrained with new training data to adapt to evolving phishing patterns.
- Updating the model allows it to recognize new phishing techniques and maintain accuracy over time.

Thresholding and Alert Generation:

- The output of the model is a probability score indicating the likelihood of the web request being a phishing attempt.
- If the score exceeds a pre-defined threshold, an alert is generated.
- The threshold can be adjusted to tune the sensitivity of the system based on desired false positive vs false negative rates.
- Protective actions can be taken like blocking the web request when an alert is triggered.

E. Process Flow

This process flow covers the end-to-end lifecycle of the proposed phishing detection system, from initial data collection and model development to real-time deployment, alert generation, and continuous improvement through model updates. The key stages are feature extraction, model training and evaluation, real-time scoring of live network requests, alert generation and response, and periodic model retraining to adapt to evolving phishing tactics.

Data Collection and Preprocessing:

- Collect a dataset of known phishing and legitimate network resource requests.
- Preprocess the raw request data to extract relevant features like URL, domain age, registrar, IP address, geographic location, etc.
- Label each request example as phishing or benign.

Feature Extraction:

- Define a set of discriminative features that can distinguish phishing attempts from legitimate requests based on domain knowledge and prior research.
- Implement feature extraction logic to parse the relevant attributes from the preprocessed request data.
- Transform the extracted feature values into a suitable format (e.g., numerical vectors) for input to the machine learning model.

Model Training:

- Select a machine learning algorithm for the phishing classification task (e.g., Random Forest, SVM, Neural Networks).
- Split the labeled dataset into training and testing subsets.

- Train the chosen model on the training set, learning the patterns that map the input features to the phishing/benign labels.
- Tune the model's hyperparameters using techniques like cross-validation to optimize performance.

Model Evaluation:

- Evaluate the trained model's performance on the held-out testing set.
- Calculate evaluation metrics such as accuracy, precision, recall, F1-score, etc.
- Analyze the model's performance to assess its effectiveness in detecting phishing attempts and identify areas for improvement.

Model Deployment:

- Integrate the trained phishing detection model into a live network monitoring system.
- Extract the same set of features from incoming network requests in real-time.
- Apply the model to each request's features to obtain a phishing probability score.
- Compare the score to a predefined threshold to classify the request as phishing or benign.

Alert Generation and Response:

- If a request's phishing score exceeds the threshold, generate an alert with relevant details like URL, source IP, risk score, etc.
- Deliver the alerts to security teams via appropriate channels like email, SMS, SIEM integration, etc.
- Trigger automated response actions based on alert severity, such as blocking the request or quarantining associated network traffic.
- Conduct manual investigation and remediation of high-priority alerts by security analysts.

Model Updating:

- Continuously collect new examples of phishing and benign requests in production.
- Periodically retrain the phishing detection model on an updated dataset to learn new attack patterns.
- Evaluate the retrained model's performance and deploy it to replace the existing model if it offers improved accuracy.
- Monitor the model's predictions over time to detect concept drift or performance degradation that may require further updates.

F. Feature Extraction

Feature extraction involves identifying and selecting relevant characteristics or attributes from the raw data of the

network resource request. The extracted features, such as FQDN, domain age, registrar, IP address and location, serve as inputs to the statistical model to dynamically assess phishing risk.

The goal is to transform the request data into a set of informative features that can be fed into the statistical model to determine if the request is potentially malicious.

- **Fully Qualified Domain Name (FQDN):** The complete domain name of the requested resource, which includes the hostname, subdomain (if present), second-level domain, and top-level domain (TLD). For example, "mail.example.com" is an FQDN where "mail" is the hostname, "example" is the second-level domain and ".com" is the TLD.
- **Age of the Domain:** This refers to how long ago the domain name was registered. Newly registered domains are more likely to be associated with phishing attempts. The domain age can be determined by checking the domain's initial registration date.
- **Domain Registrar:** The entity through which the domain name was registered. Certain registrars may be more commonly used by phishing sites.
- **IP Address:** The numerical label assigned to the server hosting the requested resource.
- **Geographic Location:** The physical location of the server based on its IP address. Requests originating from unexpected geographic regions could indicate higher phishing risk.

Extracting these specific sub-features allows representing the key elements of the request in a structured format that can be analyzed by the statistical model. The feature values are likely transformed and normalized to make them suitable for input to the machine learning algorithm.

It is suggested that additional sub-features could also be extracted depending on the specific implementation. The feature extraction process essentially converts the raw request data into a vector of relevant attributes that succinctly capture the information needed to assess the phishing risk.

By carefully engineering and selecting the features, the accuracy and efficiency of the downstream phishing detection model can be optimized. The extracted features aim to capture patterns and signals that distinguish legitimate requests from phishing attempts based on the domain, server, and request characteristics.

G. Statistical Model

The statistical model takes the extracted features of a network resource request as input and outputs a probability score indicating the likelihood that the requested resource is a phishing threat.

Model Type: it suggests using machine learning techniques to train the statistical model, specifically mentioning the Random Forest algorithm as one possible implementation. Random Forest is an ensemble learning method that constructs multiple decision trees and outputs the class that is the mode of

the classes output by the individual trees. It is known for its ability to generalize well to new data.

Model Inputs: The input to the model is the set of features extracted from the network resource request, such as the FQDN, domain age, registrar, IP address, geographic location, etc. These features are transformed and normalized into a suitable format (e.g. a feature vector) before being fed into the model.

Model Output: The output of the model is a probability score between 0 and 1, representing the estimated likelihood that the requested resource is a phishing attempt. If the score exceeds a predefined threshold (e.g. 0.8), the resource is classified as a potential phishing threat.²

Model Training: The statistical model is trained on a labeled dataset containing examples of known phishing and non-phishing (benign) network resources. During training, the model learns to recognize patterns and combinations of feature values that are indicative of phishing. The Random Forest algorithm adjusts the model parameters to minimize misclassification errors.

Model Evaluation: The performance of the trained model is evaluated using metrics like accuracy, precision, recall, F1-score, etc. on a separate test set. This helps assess how well the model generalizes to unseen data and guides model selection and hyperparameter tuning.

Model Updating: To adapt to evolving phishing tactics, the statistical model can be periodically retrained with new labeled data. This allows the model to learn new patterns and maintain its accuracy over time as the characteristics of phishing attempts change.

The statistical model is a machine learning classifier at the core of the dynamic phishing detection system. It is trained to predict the probability of a network resource being a phishing threat based on its extracted features. The model's architecture, training procedure, and updating strategy are designed to enable accurate, adaptive, and real-time identification of phishing attempts.

The use of a data-driven statistical approach allows the system to learn complex patterns from historical phishing data and generalize that knowledge to detect new, previously unseen phishing attempts. This provides a more dynamic and robust defense compared to static rule-based methods.

H. Model Training and Updating

Model training and updating refer to the processes of initially building the statistical model on a training dataset and subsequently refining it over time as new data becomes available. This is a crucial part of the machine learning pipeline that enables the phishing detection system to adapt and maintain accuracy in the face of evolving threats.

Initial Model Training:

- Before deployment, the statistical model (e.g., Random Forest classifier) is trained on a labeled dataset containing examples of known phishing and benign network resource requests.

- Each training example consists of the extracted features (FQDN, domain age, registrar, IP, location, etc.) and the corresponding label (phishing or benign).
- During training, the model learns to recognize patterns and combinations of feature values that distinguish phishing attempts from legitimate requests.
- The model's parameters are optimized to minimize prediction errors on the training data.

Periodic Model Updating:

- It emphasizes the importance of periodically retraining the model with new labeled data to adapt to evolving phishing tactics.
- As new types of phishing attacks emerge, the characteristics of phishing requests may change over time.
- Updating the model allows it to learn these new patterns while retaining knowledge of previously seen phishing indicators.
- The frequency of model updates can be adjusted based on the volume and velocity of new phishing data collected.

Continuous Learning:

- Some machine learning architectures, like online learning or incremental learning, are specifically designed to support continuous updating of the model as new data arrives.
- Instead of retraining on the entire cumulative dataset, these methods can incrementally adjust the model parameters based on mini-batches of new examples.
- Continuous learning helps alleviate the computational burden of repeated retraining and allows faster adaptation to new threats.

Data Management:

- Effective model updating requires careful management of the training data over time.
- The labeled dataset needs to be expanded with new phishing and benign examples while maintaining a balance between the classes.
- Techniques like active learning can be used to strategically select the most informative examples for labeling, optimizing the use of human annotation efforts.

Evaluation and Monitoring:

- After each update, the retrained model should be evaluated on a separate test set to assess its performance and ensure it hasn't degraded.
- Continuous monitoring of the model's predictions in production is also important to detect concept drift or errors that may necessitate further updates.

The model training and updating are essential for the long-term effectiveness of the phishing detection system. The initial training process builds the model's baseline knowledge, while periodic updates allow it to adapt to new phishing patterns over time. Techniques like continuous learning, active data selection, and performance monitoring help optimize the update process and maintain the model's accuracy in the face of evolving threats.

I. Thresholding and Alert Generation

Thresholding and alert generation refer to the process of deciding whether a given network resource request should be classified as a phishing attempt based on the probability score output by the statistical model, and raising an appropriate alert if the decision is positive. This is a critical step that translates the model's predictions into actionable security decisions and notifications.

Probability Score Threshold:

- The statistical model outputs a probability score between 0 and 1 for each network resource request, indicating the estimated likelihood of it being a phishing attempt.
- A predefined threshold value (e.g., 0.8) is used to make the final classification decision.
- If the score exceeds the threshold, the request is classified as a potential phishing threat. Otherwise, it is considered benign.

Threshold Selection:

- The choice of threshold value involves a trade-off between false positives (legitimate requests misclassified as phishing) and false negatives (phishing attempts misclassified as benign).
- A higher threshold reduces false positives but may miss some real phishing attempts. A lower threshold catches more phishing but also flags more benign requests.
- The optimal threshold can be determined based on the specific security requirements and the relative costs of false positives and false negatives in the deployment context.

Alert Generation:

- When a request's score exceeds the phishing threshold, an alert is generated to indicate a potential phishing threat.
- The alert may include relevant details about the request, such as the requested URL, source IP address, associated probability score, etc.
- Alerts can be delivered through various channels like console logs, email notifications, SMS messages, security incident and event management (SIEM) systems, etc.

Alert Validation and Filtering:

- To reduce false positives, generated alerts may go through additional validation steps before being escalated.
- This could involve comparing the alert details against allowlists of known benign resources, checking for alert flooding from the same source, or applying other heuristic filters.
- Manual review of a subset of alerts by security analysts can help tune the thresholds and validation rules over time.

Alert Response Actions:

- Depending on the severity and confidence of the phishing classification, different response actions can be triggered by the alerts.
- Lower severity alerts may simply be logged for later analysis, while higher severity ones may trigger immediate blocking of the resource request and quarantining of associated network traffic.
- Automated responses can be complemented by manual investigation and remediation actions based on the alert details.

The thresholding and alert generation bridge the gap between the probabilistic predictions of the phishing detection model and the deterministic security decisions and actions needed to protect users and systems. By selecting appropriate threshold values, generating informative alerts, and triggering proportional response actions, this component operationalizes the intelligence gathered by the model to provide effective anti-phishing defense.

J. Benefits, drawbacks and significance of proposed solution

This patent illustrates an important evolution from reactive, signature-based phishing detection to a more dynamic, adaptive approach powered by statistical modeling. While not a silver bullet, it represents a meaningful step towards stronger, more intelligent anti-phishing defenses.

This patent presents an automated, data-driven approach to detect phishing attempts in real-time by learning generalized patterns instead of using static rules. The dynamic nature allows adapting to evolving phishing techniques. Generating probabilistic risk scores enables prioritizing the most suspicious cases.

By describing a flexible machine learning pipeline with feature extraction, model training/updating, and alert generation, the patent provides a framework for building more effective anti-phishing systems. The proposed method could significantly improve an organization's ability to proactively identify and block phishing threats before they victimize users. However, it does require substantial data collection and engineering effort to implement and maintain.

The statistical model is trained on historical phishing and benign examples to learn patterns that distinguish the two classes. It can be periodically retrained on new data to adapt to evolving phishing tactics.

Key Benefits:

- Enables proactive, real-time detection of phishing attempts, including new attacks not seen before, by analyzing patterns in URL/domain attributes
- Provides a probability score allowing prioritization of the riskiest threats
- Adapts to changing phishing tactics over time through periodic retraining of the model
- Generates informative alerts with key request details for security teams to investigate
- Allows tuning detection sensitivity by adjusting the alert threshold

Drawbacks:

- Requires significant historical phishing and benign data for initial model training
- Needs ongoing labeled data collection to retrain and update the model over time
- May miss some novel phishing patterns not reflected in the training data
- Extracting an effective feature set requires careful engineering and domain expertise
- Could generate false positives that may need additional filtering/validation

1) Feature Extraction

Feature extraction is a crucial step that allows building effective ML models for phishing detection by representing request data in an informative format. However, it requires significant expertise and effort to develop and maintain a robust feature set. Combining manual feature engineering with automatic representation learning can help alleviate some of these drawbacks and create more powerful hybrid detection models.

a) Benefits:

- Enables representing the key characteristics of network resource requests in a structured format suitable for analysis by machine learning models. Extracting relevant features is crucial for building accurate phishing detection models.
- Allows capturing discriminative patterns that distinguish phishing attempts from legitimate requests. Carefully engineered features can provide strong signals for classification.
- Reduces the dimensionality of raw request data, making it more computationally efficient to process. Working with a compact set of informative features is faster than analyzing the full request content.
- Feature extraction by domain experts leverages their knowledge to create highly relevant features for the specific task of phishing detection. Manual feature

engineering guided by expertise can yield very effective feature sets.

- Extracted features can be combined with automatically learned features from deep learning to create powerful hybrid models. This allows getting the best of both manual feature engineering and representation learning.

b) Drawbacks:

- Requires significant domain expertise and manual effort to identify and implement effective features. Developing a good feature set for phishing detection is time-consuming and relies heavily on expert knowledge.
- Engineered features may not capture all relevant patterns, especially novel ones in evolving phishing attacks. There's a risk of missing important signals that experts haven't thought of.
- Feature extraction code needs to be regularly updated to handle changes in web technologies and phishing techniques. Maintaining the feature pipeline can be an ongoing engineering overhead.
- Extracted features may be specific to certain types of phishing attacks, limiting the model's ability to generalize to new attack variants. Overly specialized features can lead to brittle models.
- Relying solely on manually engineered features may result in lower performance compared to end-to-end deep learning on raw data. For some tasks, learned representations can outperform hand-crafted features.

2) Statistical Model

Statistical models, especially hybrid approaches combining engineered features and deep learning, offer powerful capabilities for dynamic and adaptive phishing detection. However, they also introduce challenges around data quality, feature engineering, computational complexity, and robustness to adversarial attacks. Effective deployment requires carefully addressing these limitations through continuous data collection, model updates, and expert oversight.

a) Benefits:

- Enables dynamic and adaptive detection of phishing threats by learning patterns from historical data. The statistical model can recognize complex combinations of features indicative of phishing, beyond simple rules.
- Outputs a probability score that quantifies the risk of a request being a phishing attempt. This provides more nuanced information than a binary classification, allowing fine-grained risk assessment and prioritization.
- Can be updated over time by retraining on new data to adapt to evolving phishing tactics. The model's predictive power can be maintained as attackers change their techniques.
- Suitable for real-time detection due to fast inference time once the model is trained. Allows integration into live monitoring and prevention systems.

- Hybrid models combining manual feature engineering and deep learning have shown improved accuracy over traditional ML models in phishing detection. Leverages the strengths of both human expertise and data-driven learning.

b) Drawbacks:

- Requires a large labeled dataset for initial training, which can be expensive and time-consuming to obtain. Phishing datasets must be continuously updated to include new attack patterns.
- Model performance depends heavily on the quality and representativeness of the training data. Biased or incomplete datasets can lead to skewed predictions and blind spots.
- Feature engineering still plays a crucial role in building effective ML models for phishing detection. Relevant features must be manually crafted, requiring significant domain expertise.
- Traditional ML models like Random Forest may plateau in performance and fail to detect novel phishing patterns not seen during training. Keeping models up-to-date is an ongoing challenge.
- Deep learning models can be computationally expensive to train and may require specialized hardware. Increased complexity also makes the models harder to interpret and debug.
- Risk of adversarial attacks where phishers deliberately craft messages to evade detection by the model. ML models can be brittle and vulnerable to manipulation.

3) Model Training and Updating

The model training and updating are essential for maintaining the effectiveness of the phishing detection system as new threats emerge. However, the process also introduces operational complexities around data collection, labeling, computational resources, and change management. Careful design of the retraining pipeline, data quality controls, and monitoring mechanisms is crucial to realizing the benefits while mitigating the drawbacks.

a) Benefits:

- Allows the phishing detection model to adapt to evolving threats by learning from new labeled examples over time. Periodic retraining helps the model recognize novel phishing patterns.
- Continuous learning techniques can incrementally update the model with new data, reducing the computational cost compared to full retraining. This enables more frequent and efficient model updates.
- Active learning strategies can optimize the selection of new examples for labeling, minimizing the manual annotation effort required. This helps manage the ongoing data curation process.
- Regular model evaluation on new test sets ensures that updates actually improve performance and don't

introduce regressions. Monitoring model behavior in production catches potential issues early.

- Updating the model with a diverse set of new phishing and benign examples improves its robustness and generalization to different attack variants. A broad training set helps the model handle a wide range of threats.

b) Drawbacks:

- Requires a continuous stream of new labeled phishing and benign examples to retrain the model, which can be challenging and expensive to obtain at scale. Labeling new training examples requires manual effort by domain experts and can be time-consuming. Developing efficient annotation workflows and interfaces is crucial.
- If the distribution of new training data differs significantly from the original data, the updated model may experience performance degradation or instability. Careful data quality control and monitoring are needed.
- Frequent model updates can be computationally expensive, especially for large deep learning models. Incremental learning techniques help but may still require significant resources.
- Updating the model changes its behavior, which can be disruptive to downstream systems and workflows relying on its predictions. Versioning and change management processes are important.
- There's a risk of the model overfitting to recent training examples and losing performance on older phishing patterns. Balancing the mix of old and new data during retraining is tricky.

4) Thresholding and Alert Generation

The thresholding and alert generation play a crucial role in operationalizing the phishing detection model by converting its probabilistic outputs into concrete security actions. However, this process also introduces challenges around threshold tuning, false positive management, and alert fatigue. Careful design and ongoing refinement of the thresholding logic, in tandem with the model's performance, are key to striking an effective balance between risk reduction and operational efficiency.

a) Benefits:

- Allows translating the probabilistic output of the statistical model into actionable security decisions. By comparing the model's phishing probability score to a predefined threshold, the system can automatically determine whether to flag a request as a potential threat.
- Provides a tunable parameter (the threshold) to balance the trade-off between false positives and false negatives. Adjusting the threshold allows administrators to control the sensitivity of the alerts based on their risk tolerance and operational constraints.
- Enables generating informative alerts with relevant details about the suspicious request, such as the URL, source IP, and associated risk score. This contextual

information helps security teams quickly triage and investigate potential phishing incidents.

- Supports flexible alert delivery channels, such as console logs, email, SMS, or integration with security information and event management (SIEM) systems. This allows phishing alerts to be seamlessly incorporated into existing security monitoring workflows.
- Allows implementing additional validation logic and filters to further reduce false positives. For example, alerts can be suppressed for whitelisted domains or IP ranges, or if the model's confidence score is below a certain level.

b) *Drawbacks:*

- Selecting an appropriate threshold value requires careful tuning and may involve trial and error. Setting the threshold too low can result in a high volume of false positives, while setting it too high may miss actual phishing attempts.
- The optimal threshold may need to be periodically adjusted as the characteristics of phishing attacks evolve over time. Maintaining an effective threshold requires ongoing monitoring and analysis of the system's performance and the changing threat landscape.
- Thresholding reduces the rich information provided by the model's probability score to a binary decision (alert or no alert). This can result in a loss of nuance and granularity in assessing the risk of borderline cases.
- Alerts generated by the system may still require manual review and investigation by security analysts. While thresholding helps prioritize the most suspicious cases, it doesn't eliminate the need for human judgment and intervention.
- The effectiveness of the alerts ultimately depends on the accuracy of the underlying statistical model. If the model's predictions are biased or miscalibrated, even a well-tuned threshold may produce suboptimal results.



PATENT US9071600B2



Abstract – This analysis provides a examination of patent US9071600B2, which pertains to phishing and online fraud prevention. The document will be scrutinized to explore various aspects including the technical field, the problem addressed by the invention, the proposed solution, and its principal uses.

The detailed analysis of patent US9071600B2 reveals its potential to significantly impact the field of cybersecurity and various industries reliant on secure online operations. The document offers a quality extract of the patent, underscoring its utility for security professionals and specialists seeking to enhance online safety and prevent fraudulent activities. For cybersecurity experts, understanding the mechanisms of such a system can aid in developing more robust security protocols to combat evolving online threats. For professionals in IT and DevOps, the patent's focus on VPNs and secure communication channels is particularly pertinent

A. Introduction

The patent US9071600B2 addresses the critical issue of online security, specifically focusing on phishing and fraud prevention techniques. It outlines a system that establishes a Virtual Private Network (VPN) tunnel between a user computer and a server to enhance security during online transactions. The invention's technical classification falls under network security, authentication of entities, and countermeasures against malicious traffic.

B. Main idea

The main idea of the patent's implications is to extend to industries that rely heavily on online transactions, such as finance and e-commerce. By providing a method to safeguard against phishing and fraud, the patent contributes to the overall trustworthiness of online services, which is essential for consumer confidence and the smooth functioning of digital marketplaces. It provides insights into the design and implementation of secure networks, which is a fundamental aspect of maintaining operational security in various organizational contexts. In the context of cybersecurity, the patent's relevance is paramount. It offers a method to protect

sensitive user information and prevent unauthorized access, which is crucial for maintaining the integrity of online systems.

C. Keypoints

- **Purpose:** The patent is focused on methods and systems to prevent phishing and fraudulent activities online
- **Classification:** The patent falls under several classifications related to network security, authentication of entities, and countermeasures against malicious traffic, indicating its relevance to cybersecurity
- **Innovation in Security:** The patent represents an innovative approach to enhancing online security by identifying and mitigating risks associated with unauthorized access and fraudulent transactions.
- **Technical Contributions:** The cited and citing patents demonstrate the technical contributions of US9071600B2 to the broader field of cybersecurity and its ongoing relevance to new security technologies.
- **Impact of Expiry:** The expiration of the patent opens opportunities for other individuals and companies to explore and potentially build upon the previously protected technology without the concern of infringement.
- **Research and Development:** The patent is part of a larger ecosystem of research and development in cybersecurity, with its references to prior art and subsequent citations indicating a collaborative progression of knowledge and technology in this domain.

D. Industries

The patent is highly relevant to industries that engage in online activities requiring secure authentication, data protection, and fraud prevention measures. These industries would benefit from the implementation of the patented systems and methods to enhance their cybersecurity posture and protect against phishing and online fraud.

1) Banking and Finance

Financial institutions manage vast amounts of sensitive financial data and conduct numerous online transactions daily. This sector is heavily reliant on secure online transactions and the protection of customer financial information. The patent's focus on preventing phishing and fraudulent activities is crucial for protecting customer accounts and maintaining trust in online banking systems. Implementing the patented methods can help banks detect and mitigate threats, ensuring the security of online transactions and safeguarding against the financial losses associated with fraud.

2) Technology and Software

Technology and software companies, including those specializing in cybersecurity solutions, stand to benefit significantly from the innovations. Companies in this sector develop and provide the platforms and software that enable online transactions and data storage. The security measures outlined in the patent are essential for maintaining the integrity

of these platforms and protecting against cyber threats. These companies can integrate the patent's methodologies into their security platforms, offering enhanced protection against phishing and fraud to their clients. The patent's relevance extends to developers of web browsers, email services, and other applications where user authentication and data integrity are critical. By adopting these security measures, technology firms can provide more robust defenses against increasingly sophisticated cyber threats.

3) E-commerce

Online retailers and service providers are prime targets for phishing and fraud. The e-commerce industry relies heavily on consumer trust and the secure handling of personal and payment information. Online retailers and service providers are frequent targets of phishing attacks aimed at stealing customer data. The preventive measures can be instrumental in securing e-commerce platforms, protecting customer transactions from fraudulent interference, and ensuring the confidentiality of personal information. By implementing these security protocols, e-commerce businesses can enhance their reputation for safety and reliability, encouraging continued consumer engagement.

4) Healthcare

With the increasing digitization of healthcare records and services, this industry requires robust security measures to protect patient information and ensure the privacy and integrity of medical data shared online. The healthcare organizations manage sensitive patient data, making them a critical area for the application of patent's security measures. The patent's technologies can help protect electronic health records (EHRs), patient portals, and other digital healthcare services from unauthorized access and fraud. Ensuring the privacy and integrity of medical information is not only a matter of regulatory compliance but also essential for patient trust and the effective delivery of care. The adoption of these security solutions can significantly contribute to the safeguarding of health data in an increasingly digital medical landscape.

5) Government and Public Sector

Government agencies and public sector organizations often handle sensitive information and provide services that require secure online interactions. The technologies and methods in the patent can help safeguard against fraudulent activities that target public sector websites and online services. The security challenges faced by these entities include protecting against unauthorized access to confidential data and ensuring the integrity of online services. The methods and systems can offer valuable solutions for enhancing the cybersecurity posture of government websites and digital services, protecting against phishing attempts, and preventing online fraud.

E. The proposed solution

The patent presents a multi-faceted approach to combating phishing and online fraud. By combining user authentication, website verification, secure communication, real-time monitoring, advanced threat detection algorithms, user education, and a feedback mechanism, the proposed solution offers a robust defense against the evolving threats in the digital landscape. These components work together to protect users and

organizations from the financial and reputational damage associated with online fraud and phishing attacks.

Key Components of the Proposed Solution

- **User Authentication:** A critical component of the solution involves verifying the identity of users attempting to access a service or perform a transaction. This process ensures that access is granted only to legitimate users, thereby reducing the risk of unauthorized access.
- **Website Verification:** The system includes mechanisms for verifying the authenticity of websites. This is crucial for preventing users from being directed to or interacting with fraudulent websites designed to mimic legitimate ones for the purpose of phishing.
- **Secure Communication Channels:** Establishing secure communication channels between users and services is another vital aspect. This includes the use of encryption and secure protocols to protect data in transit, preventing interception or manipulation by malicious actors.
- **Real-time Monitoring and Analysis:** The proposed solution incorporates real-time monitoring of user activities and transactions. By analyzing patterns and behaviors, the system can identify potential threats or fraudulent activities, enabling timely intervention.
- **Threat Detection Algorithms:** Advanced algorithms are employed to detect phishing attempts and fraudulent actions. These algorithms leverage various indicators and heuristics to identify suspicious activities, such as unusual login attempts or transactions that deviate from a user's typical behavior.
- **User Education and Awareness:** Part of the solution involves educating users about the risks of phishing and fraud. This may include alerts or warnings when a potential threat is detected, guiding users to take appropriate actions to protect their information.
- **Feedback Mechanism:** The system allows for feedback from users regarding potential threats or false positives. This feedback is used to continuously improve the accuracy and effectiveness of the threat detection algorithms.

1) User Authentication

The 'User Authentication' component encompasses various methods and systems for securely authenticating users to prevent unauthorized access and protect against phishing and online fraud. These techniques include inline authentication forms, stored authentication data, authentication of identification attributes, the 3-D Secure protocol, and multilayer access control security systems.

It refers to methods and systems that authenticate users in a secure manner to prevent unauthorized access and protect against phishing and online fraud:

- **Inline Authentication Form:** One approach to user authentication involves the use of an inline

authentication form. This form is presented to the user asynchronously and can be embedded within an iFrame on a merchant's checkout page after verifying that the components of the authentication system can support it. The inline authentication form is used if the system components can support it, and if not, a different authentication process is employed.

- **Stored Authentication Data:** Another method of user authentication involves the use of an authentication platform that can store authentication data received from an issuer access control server. The authentication platform can authenticate users and portable devices on behalf of the issuer access control server using the stored authentication data. This approach ensures that the issuer access control server can rely on the authentication platform to conduct authentication.
- **Authentication of Identification Attributes:** The patent also discusses systems and methods for authenticating various identification attributes of parties involved in a transaction. These attributes can include items such as the participant's name, address, social security number, date of birth, or any other identifying attributes. In some embodiments, all participants in a transaction may have their identification information authenticated.
- **Three-Dimensional (3-D) Secure Protocol:** The patent extends and enhances the 3-D Secure protocol and framework to provide the ability to authenticate the identification of parties involved in a transaction. This protocol ensures that the participants in a transaction are authenticated, providing an additional layer of security.
- **Multilayer Access Control Security System:** The patent also mentions a multilayer access control security system that can be used for user authentication. This system provides multiple layers of security to ensure that only authorized users can access protected resources.

2) Website Verification

The 'Website Verification' component of the proposed solution involves various methods for verifying the authenticity of websites and preventing users from interacting with fraudulent sites. These methods include using a shared secret, establishing a VPN tunnel, using pre-shared keys or private certificates for VPN tunnel authentication, and verifying user information associated with the website. By implementing these methods, the solution aims to mitigate phishing attacks and online fraud, ensuring the security of user data and transactions.

It is designed to verify the authenticity of websites and prevent users from interacting with fraudulent sites that helps in mitigating phishing attacks and online fraud:

- **Verifying the Authenticity of Websites:** One approach to website verification involves using a shared secret between the user's device and the website. This shared secret is used to authenticate the website and ensure that the user is interacting with the legitimate site.
- **Establishing a VPN Tunnel:** Another method involves establishing a VPN tunnel between the user's device and

a trusted server. The VPN tunnel ensures secure communication between the device and the server, preventing unauthorized access and protecting against phishing attacks. This method is discussed in the patent document, although it is not explicitly mentioned as a website verification method.

- **Site-to-Site VPN Tunnel Authentication:** This method involves using pre-shared keys or private certificates from AWS Private Certificate Authority to authenticate the VPN tunnel endpoints. This ensures that only authorized devices can establish a VPN connection and access the resources on the other end of the tunnel.
- **User Information Verification:** The patent US8037316B2, which is cited by US9071600B2, discusses a method and system for user information verification that could be adapted to verify the authenticity of websites by checking the user information associated with the website.

3) Secure Communication Channels

Secure communication channels are crucial for protecting data during transmission in various contexts, including cybersecurity. The concept is related to the protection of data during transmission:

- **End-to-End Encryption:** This method involves encrypting data at the source and decrypting it at the destination, ensuring that only the intended recipient can access the information. End-to-end encryption can be implemented using various cryptographic techniques, such as symmetric or asymmetric encryption.
- **Secure Sockets Layer (SSL) and Transport Layer Security (TLS):** These protocols provide secure communication over the internet by establishing a secure connection between two parties, such as a web browser and a web server. SSL and TLS use both symmetric and asymmetric encryption to verify identities and encrypt data exchanged between the parties.
- **Secure Shell (SSH):** SSH is a protocol that allows secure remote access to another operating system over a network. It uses public-key encryption to authenticate the user and the host, and then creates a secure channel that encrypts all the data exchanged between them.
- **Virtual Private Network (VPN):** A VPN creates a secure tunnel between two or more operating systems over a network, allowing for secure data transmission. VPNs can be used to protect data in transit, especially when using public networks.
- **Authentication Protocols:** Authentication protocols, such as CHAP, PAP, and EAP, are used to secure communication channels by verifying the identity of the parties involved in the communication.
- **Firewall Restrictions and Data Encryption:** To prevent unauthorized participation, eavesdropping, spying, data leakage, and communications interception, mitigating technologies such as firewall restrictions,

data encryption, and authentication security measures can be employed.

4) Real-time Monitoring and Analysis

Real-time monitoring and analysis is a crucial component in the context of patent, as it enables the system to detect and respond to potential threats in real-time. This component involves continuously monitoring user activities and transactions, analyzing patterns and behaviors, and identifying potential threats or fraudulent activities. By doing so, the system can take appropriate actions to mitigate the risks associated with phishing and online fraud.

5) Threat Detection Algorithms

The 'Threat Detection Algorithms' component is a crucial aspect of the proposed solution for phishing and online fraud prevention. This component employs advanced algorithms to identify suspicious activities, such as unusual login attempts or transactions that deviate from a user's typical behavior. By leveraging various indicators and heuristics, these algorithms can detect potential threats and fraudulent actions in real-time.

One key aspect of the threat detection algorithms is their ability to analyze patterns and behaviors in user activities and transactions. By establishing a baseline of normal user behavior, the algorithms can identify anomalies that may indicate a potential threat. For example, if a user typically logs in from a specific geographic location and suddenly attempts to access their account from a different country, the algorithm may flag this activity as suspicious and trigger an alert.

The threat detection algorithms can also monitor for specific indicators of phishing and fraud, such as the presence of known malicious URLs or the use of suspicious email content. By maintaining a database of known threats and continuously updating it with new information, the algorithms can quickly identify and respond to emerging threats.

Another important aspect of threat detection algorithms is their ability to adapt and learn over time. As new threats emerge and attackers change their tactics, the algorithms must be able to evolve to keep pace. By incorporating machine learning techniques, the algorithms can continuously improve their accuracy and effectiveness based on feedback and new data.

The patent also mentions the use of real-time monitoring and analysis in conjunction with threat detection algorithms. By continuously monitoring user activities and transactions, the system can detect potential threats as they occur and take immediate action to mitigate the risk. This real-time capability is essential for preventing unauthorized access and fraudulent activities before they can cause significant damage.

6) Feedback Mechanism

This component allows users to provide feedback regarding potential threats or false positives, which can be used to continuously improve the accuracy and effectiveness of the threat detection algorithms. When combined with other components such as threat detection algorithms and real-time monitoring, the feedback mechanism helps to create a more robust and adaptable security system that can keep pace with the ever-changing landscape of cyber threats. This feedback loop

ensures that the system remains up-to-date and effective in the face of evolving cyber threats.

Another important aspect of the feedback mechanism is that it provides a way for users to actively participate in the security process. By empowering users to report potential threats, the system can leverage the collective intelligence of its user base to identify and respond to new threats more quickly. This collaborative approach to security can be particularly effective in detecting targeted attacks or sophisticated phishing campaigns that may evade traditional security measures.

The feedback mechanism can also help to reduce false positives, which can be a significant problem in automated threat detection systems. False positives occur when the system incorrectly identifies a legitimate activity as a potential threat, which can lead to unnecessary alerts and disruptions for users. By allowing users to provide feedback on these false positives, the system can learn to distinguish between legitimate and malicious activities more accurately over time.

To be effective, the feedback mechanism must be easy to use and accessible to all users. This may involve providing clear instructions on how to report potential threats or false positives, as well as offering multiple channels for submitting feedback, such as email, web forms, or mobile apps. The system should also provide timely responses to user feedback, acknowledging receipt of the report and providing updates on any actions taken as a result.

F. Process Flow

The process flow of the proposed solution from patent involves several steps to ensure the security of user data and prevent unauthorized access and fraudulent activities.

- **Establishing a VPN Tunnel:** The user computer establishes a VPN tunnel between itself and a network. This secure connection ensures that data transmitted between the user and the network is encrypted and protected from unauthorized access.
- **Authentication:** The user is authenticated using various methods, such as user information verification or the 3-D Secure protocol. This step ensures that only authorized users can access the network and perform transactions.
- **Website Verification:** The authenticity of websites is verified to prevent users from interacting with fraudulent sites. This can be achieved using a shared secret between the user's device and the website or by establishing a VPN tunnel.
- **Secure Communication Channels:** Secure communication channels are established using techniques such as end-to-end encryption, SSL/TLS, or SSH. These channels ensure that data transmitted between parties is protected and cannot be intercepted or manipulated by malicious actors.
- **Real-time Monitoring and Analysis:** User activities and transactions are monitored in real-time, and advanced algorithms are used to detect potential threats or fraudulent activities. This allows for timely intervention and mitigation of risks.

- **Threat Detection Algorithms:** Advanced algorithms are employed to identify suspicious activities, such as unusual login attempts or transactions that deviate from a user's typical behavior. These algorithms use various indicators and heuristics to detect potential threats and prevent unauthorized access and fraudulent activities.
- **Feedback Mechanism:** Users can provide feedback regarding potential threats or false positives, which can be used to improve the accuracy and effectiveness of the threat detection algorithms. This feedback loop ensures that the system remains up-to-date and effective in the face of evolving cyber threats.

Steps 4-7 (Secure Communication Channels, Real-time Monitoring and Analysis, Threat Detection Algorithms, Feedback Mechanism) continue in a loop to provide continuous, adaptive protection against evolving phishing and fraud threats during the user's session.

G. Benefits, drawbacks and significance of proposed solution

This patent illustrates an important evolution from reactive, signature-based phishing detection to a more dynamic, adaptive approach powered by statistical modeling. While not a silver bullet, it represents a meaningful step towards stronger, more intelligent anti-phishing defenses.

The proposed solution from patent offers a comprehensive approach to securing online transactions and protecting users from unauthorized access and fraudulent activities. The solution includes several components, such as user authentication, website verification, secure communication channels, real-time monitoring and analysis, threat detection algorithms, and a feedback mechanism.

Benefits

- **Enhanced Security:** The proposed solution provides a multi-layered approach to security, ensuring that user data and transactions are protected from unauthorized access and fraudulent activities.
- **Real-time Threat Detection:** The real-time monitoring and analysis component enables the system to detect potential threats in real-time, allowing for timely intervention and mitigation of risks.
- **User Authentication:** The user authentication component ensures that only authorized users can access the network and perform transactions, preventing unauthorized access.
- **Website Verification:** The website verification component ensures that users interact with legitimate websites, preventing phishing attacks.
- **Secure Communication Channels:** The secure communication channels component ensures that data transmitted between parties is protected, preventing interception or manipulation by malicious actors.
- **Feedback Mechanism:** The feedback mechanism allows users to provide feedback on potential threats or false positives, enabling the system to continuously improve its accuracy and effectiveness.

Drawbacks

- **Complexity:** The proposed solution involves multiple components, which may require significant resources and expertise to implement and maintain.
- **False Positives:** The threat detection algorithms may occasionally flag legitimate activities as potential threats, leading to unnecessary alerts and disruptions for users.
- **Expense:** Maintaining the system's enforceability and paying maintenance fees for 20 years can be expensive, potentially limiting its accessibility for smaller businesses or individuals.

Significance

The proposed solution from patent is significant in the context of cybersecurity, as it addresses the growing threat of phishing and online fraud. The solution's multi-layered approach to security and real-time threat detection make it a valuable tool for protecting user data and transactions in the digital age. However, its complexity and expense may limit its adoption by smaller businesses or individuals.

1) User Authentication

This component aims to verify the identity of users before granting them access to protected resources and plays a vital role in ensuring the security and protection of sensitive data and systems. While there are limitations and challenges associated with user authentication, its benefits and significance in the context of cybersecurity make it a crucial aspect of any comprehensive security strategy.

Benefits

- **Increased Security:** User authentication helps secure systems, applications, and networks by identifying user identities and ensuring that only authorized users can access sensitive data.
- **Compliance with Regulations:** Many industries, such as finance and healthcare, must comply with data protection laws and regulations that mandate robust user authentication methods to protect confidential information.
- **Improved Accountability:** User authentication allows organizations to track and monitor user activity, providing an audit trail that can be used to investigate suspicious behavior or resolve disputes.
- **Protection Against Identity Theft:** By requiring users to prove their identity before accessing sensitive information, user authentication can help prevent identity theft.
- **Enhanced Trust:** User authentication can enhance the trust between users and organizations by providing a secure and reliable way of accessing information.

Limitations

- **Vulnerability to Phishing Attacks:** Password-based authentication, which is one type of user authentication,

is highly susceptible to phishing attacks, as many people use simple, easy-to-remember passwords.

- Complexity and User Experience: Some user authentication methods, such as multi-factor authentication, may be complex and difficult for users to manage, leading to potential frustration and reduced user experience.
- Potential for False Positives: User authentication systems may occasionally flag legitimate activities as potential threats, leading to unnecessary alerts and disruptions for users.

Significance

- **Cybersecurity Bastion:** User authentication is a critical component in the overall cybersecurity landscape, as it protects sensitive information and prevents unauthorized access to systems and data.
- **Adaptability:** User authentication methods can be adapted to various situations and environments, such as remote work or different industries with specific compliance requirements.
- **Integration with Other Security Measures:** User authentication can be integrated with other security measures, such as multi-factor authentication, to provide additional layers of protection and enhance overall security.

2) Website Verification

This component is significant in various industries, particularly those that rely heavily on online transactions and the exchange of sensitive information. This component aims to ensure that users are interacting with legitimate websites and not falling victim to phishing scams or other fraudulent activities.

Benefits

- **Enhanced Security:** By verifying the authenticity of websites, users are protected from unknowingly sharing sensitive information with malicious actors. This is particularly important in industries such as banking, e-commerce, and healthcare, where sensitive data is frequently exchanged.
- **Increased Trust:** Website verification can increase user trust in online services, as it provides assurance that they are interacting with a legitimate entity. This can lead to increased engagement and customer loyalty.
- **Reduced Fraud:** By preventing users from accessing fraudulent websites, the risk of financial losses due to online scams is significantly reduced. This benefits both individuals and businesses.

Limitations

- **Potential for False Positives:** Website verification systems may occasionally flag legitimate websites as potentially fraudulent. This can cause inconvenience for users and may lead to a loss of trust in the system.

- **Reliance on Technology:** The effectiveness of website verification is heavily dependent on the technology used. If the technology is outdated or not robust enough, it may fail to detect sophisticated phishing attempts.
- **Additional Costs:** Implementing and maintaining a website verification system can be costly, particularly for smaller businesses. This may deter some organizations from adopting this technology.

Significance

This component addresses a critical aspect of online security. With the increasing prevalence of phishing scams and online fraud, the need for effective website verification is more important than ever. This technology can provide an additional layer of security, helping to protect users and businesses from the potentially devastating consequences of online fraud.

3) Secure Communication Channels

This component plays a crucial role in ensuring the safe and reliable exchange of information between parties.

Benefits

- **Data Protection:** Secure communication channels help protect sensitive data from unauthorized access, interception, and manipulation. This is especially important in industries that handle confidential information, such as financial institutions, healthcare providers, and government agencies.
- **Compliance with Regulations:** Many industries are subject to strict data protection regulations, such as GDPR, HIPAA, and PCI-DSS. Secure communication channels help organizations comply with these regulations by ensuring that data is transmitted securely.
- **Trust and Reputation:** Implementing secure communication channels can enhance an organization's reputation and build trust with its customers and partners. This can lead to increased customer loyalty and improved business relationships.

Limitations

- **Complexity:** Implementing and maintaining secure communication channels can be complex and technically challenging. This may require specialized skills and resources, which can be costly for smaller organizations.
- **Performance Overhead:** Encrypting and decrypting data can introduce latency and reduce the overall performance of communication channels. This may be a concern for applications that require real-time or low-latency communication.
- **Compatibility Issues:** Secure communication channels may not be compatible with all devices, applications, or networks. This can limit their usability and effectiveness in certain situations.

Significance

The 'Secure Communication Channels' addresses a critical aspect of online security. With the increasing prevalence of cyber threats, the need for secure communication channels is more important than ever. This technology can provide an additional layer of security, helping to protect users and businesses from the potentially devastating consequences of data breaches and cyber-attacks.

4) Real-time Monitoring and Analysis

This component focuses on continuously monitoring and analyzing system activities, network traffic, and user behavior to detect and respond to potential threats and anomalies in real-time.

Benefits

- **Early Threat Detection:** Real-time monitoring and analysis enable organizations to detect potential threats and anomalies as they occur, allowing for a quicker response and minimizing the potential damage caused by cyber-attacks.
- **Improved Incident Response:** With real-time monitoring, security teams can respond to incidents more effectively, as they have immediate access to relevant data and insights. This can significantly reduce the time it takes to contain and mitigate security incidents.
- **Proactive Security:** Real-time monitoring and analysis allow organizations to shift from a reactive security posture to a proactive one. By continuously monitoring and analyzing system activities, organizations can identify and address potential vulnerabilities before they are exploited by attackers.

Limitations

- **Complexity:** Implementing and maintaining real-time monitoring and analysis systems can be complex and technically challenging. This may require specialized skills and resources, which can be costly for smaller organizations.
- **False Positives:** Real-time monitoring and analysis systems can sometimes generate false positives, which can lead to unnecessary alerts and increased workload for security teams. This can be mitigated by fine-tuning the system and using advanced analytics techniques.
- **Privacy Concerns:** Real-time monitoring and analysis may raise privacy concerns, as it involves collecting and analyzing sensitive data. Organizations must ensure that they comply with relevant data protection regulations and implement appropriate safeguards to protect user privacy.

Significance

The 'Real-time Monitoring and Analysis' component addresses a critical aspect of cyber security. With the increasing prevalence of cyber threats, the need for real-time monitoring and analysis is more important than ever. This technology can provide organizations with the visibility and insights they need to detect and respond to potential threats in real-time, helping to

protect their assets and maintain the trust of their customers and partners.

5) Threat Detection Algorithms

Benefits

- **Automated Threat Detection:** Threat detection algorithms can automatically analyze vast amounts of data to identify patterns and anomalies that might indicate a cyber threat. This automation allows for the rapid detection of potential threats, reducing the time it takes to respond to and mitigate them.
- **Adaptability to New Threats:** Machine learning algorithms can learn from past incidents and adapt to new threats, improving the speed and accuracy of threat detection. This adaptability enables threat detection algorithms to stay current with the ever-evolving landscape of cyber threats.
- **Improved Incident Response:** AI-powered cybersecurity systems can assist in automating incident response processes, allowing for faster and more efficient mitigation of cyber threats. This automation can help reduce the impact of a cyber-attack and minimize the damage caused.

Limitations

- **Complexity and Uncertainty:** Cybersecurity data can be vast, varied, and often difficult to interpret. This complexity can make it challenging for machine learning algorithms to process, analyze, and detect potential security threats accurately. Additionally, cybercriminals are continuously developing new tactics, techniques, and procedures to evade security measures, which adds more complexity to the data.
- **Limited Human Oversight:** While AI and machine learning algorithms can process and analyze data quickly, they may not always make accurate decisions independently. Human oversight is still necessary to ensure that the algorithms are working correctly and that false positives or negatives are minimized. However, the high volume of data involved in cybersecurity makes it difficult for humans to keep up with the speed and accuracy of AI.
- **Bias and Discrimination:** Artificial intelligence and machine learning algorithms can be prone to bias and discrimination, which can be a significant concern in cybersecurity. If the algorithms are trained on partial data or flawed assumptions, they may make incorrect decisions that can have serious consequences.

Significance

The significance of threat detection algorithms lies in their ability to enhance cybersecurity defenses by automating threat detection and incident response processes. As cyber threats continue to evolve and become more sophisticated, the need for advanced threat detection algorithms becomes increasingly important. These algorithms can help organizations stay ahead

of potential threats and respond to them more effectively, ultimately improving their overall cybersecurity posture.

6) Feedback Mechanism

This component focuses on collecting and analyzing user feedback to improve the overall performance and effectiveness of the system.

Benefits

- **Continuous Improvement:** Feedback mechanisms enable organizations to continuously improve their cyber security systems by identifying and addressing potential weaknesses and vulnerabilities. This ongoing improvement helps maintain the system's effectiveness in the face of evolving cyber threats.
- **User Engagement:** By involving users in the feedback process, organizations can increase user engagement and satisfaction. Users are more likely to trust and adopt a system that takes their feedback into account and makes necessary improvements.
- **Proactive Security:** Feedback mechanisms can help organizations shift from a reactive security posture to a proactive one. By collecting and analyzing user feedback, organizations can identify and address potential vulnerabilities before they are exploited by attackers.

Limitations

- **Complexity:** Implementing and maintaining effective feedback mechanisms can be complex and technically challenging. This may require specialized skills and resources, which can be costly for smaller organizations.
- **Feedback Overload:** If not managed properly, feedback mechanisms can lead to an overwhelming amount of data, making it difficult for organizations to identify and prioritize the most critical issues. This can be mitigated by using advanced analytics techniques and prioritization methods.
- **Privacy Concerns:** Feedback mechanisms may raise privacy concerns, as they involve collecting and analyzing sensitive data. Organizations must ensure that they comply with relevant data protection regulations and implement appropriate safeguards to protect user privacy.

Significance

The 'Feedback Mechanism' component is significant in the context of patent US9071600B2 as it addresses a critical aspect of cyber security. With the increasing prevalence of cyber threats, the need for effective feedback mechanisms is more important than ever. This technology can provide organizations with the insights they need to continuously improve their cyber security systems, helping to protect their assets and maintain the trust of their customers and partners.

AIRCRAFT





Abstract – This document provides a comprehensive analysis of the "Counter-Unmanned Aircraft System (CUAS)" published by the Headquarters, Department of the Army in August 2023. The analysis delves into various aspects, including its technological components, operational considerations, and the implications for security professionals and various industries.

The document provides a quality summary of the C-UAS, detailing the technological advancements, operational strategies, and market dynamics. It is instrumental for security professionals, offering insights into the development, testing, and implementation of C-UAS technologies. The analysis underscores the significance of C-UAS in enhancing national security, protecting critical infrastructure, and maintaining airspace safety. It also emphasizes the need for continuous innovation and collaboration among industry stakeholders to address the evolving threats posed by unmanned aircraft systems. Additionally, the document's insights are valuable for different industries, enabling them to develop robust defense mechanisms against UAS threats and to stay ahead in the competitive market.

A. Introduction

The document, titled "Counter-Unmanned Aircraft System (C-UAS)" was published in August 2023 by the Headquarters, Department of the Army and superseded the previous version of the same document dated 13 April 2017.

It provides guidelines and considerations for military forces to counteract enemy unmanned aircraft systems (UASs) and prevent them from accomplishing their mission. It covers a range of topics including the description of threat UASs, planning for them at brigade and below, defensive and offensive actions for soldiers and units to take, resources for additional training, and example counter-unmanned aircraft system equipment a unit.

The principal audience is brigade and below commanders and staff, junior leaders at the company, platoon, and squad level. It is applicable to all members of the Army profession: leaders, soldiers, and Army civilians, and applies to the Active Army, Army National Guard, and United States Army Reserve.

The purpose of this document is to establish how the Army prevents threat UASs from impacting Army operations. It

emphasizes that countering UASs is not a stand-alone effort or the sole responsibility of any warfighting function or branch. Rather, it is part of local security and counter reconnaissance missions that is the responsibility of every soldier and unit. The goal is to create a layered defense through a combination of active and passive measures that prevent threat UASs from detecting, targeting, or destroying its intended target

- The document is designed to provide brigades and below with actions and considerations for conducting local security and counter reconnaissance to deny enemy unmanned aircraft systems (UAS) from accomplishing their mission.
- It includes a description of threat unmanned aircraft systems, how to plan for them at brigade and below, defensive and offensive actions for Soldiers and units to take, resources for additional training, and example counter-unmanned aircraft system equipment a unit.
- The principal audience for this manual is brigade and below commanders and staff, junior leaders at the company, platoon, and squad level.
- The manual provides the foundation for counter-unmanned aircraft systems, training and Army education system curricula and future capabilities development across doctrine, organization, training, materiel, leadership and education, personnel, facilities, and policy (known as DOTMLPF-P).
- Commanders, staffs, and subordinates are expected to ensure that their decisions and actions comply with applicable United States, international, and in some cases, host-nation laws and regulations, and all applicable international treaties and agreements.
- It applies to the Active Army, Army National Guard, and United States Army Reserve unless otherwise stated.
- The proponent is the Commanding General, United States Army Fires Center of Excellence and Fort Sill

B. Threat Unmanned Aircraft Systems

1) Introduction

The proliferation of Unmanned Aircraft Systems (UASs) presents a significant challenge to United States forces, allies, and partners. Adversaries are leveraging these relatively inexpensive, flexible, and expendable systems while exploiting inherent difficulties with attribution and its implications for deterrence.

UASs come in a variety of sizes and capabilities. Larger UASs can have similar lethality to cruise missiles and can launch from a wide array of locations. Smaller UASs can launch virtually undetected and are difficult to detect as they maneuver across the battlefield, making them an increasingly preferred method to carry out tactical-level strikes.

UASs can conduct several different missions separately or simultaneously while on one flight. These missions include intelligence, surveillance, and reconnaissance; situational

awareness; communications relay; weapon delivery; fire support; and psychological warfare.

UASs are categorized into Groups 1 through 5 based on weight, operating altitude, and speed. The larger the platform, the more robust its suite of capabilities. The lines of differentiation between different groups operationally are not rigid.

A UAS is composed of everything required to operate an unmanned aircraft vehicle (UAV). This includes the personnel, UAV, payload (sensors or weapons), control station, communication links, launch system, and recovery system. Different echelons and capabilities focus on defeating different parts of the system.

The document emphasizes that countering UASs is a shared joint and combined arms responsibility. Commanders and staffs must be prepared to address these across the entire competition continuum

2) UAS Missions

UAS technology and capability are growing, and as a result, their military employment is also expanding. A UAS may conduct several different missions separately or simultaneously while on one flight.

- **Intelligence, surveillance, and reconnaissance:** UASs can provide adversaries with contemporary intelligence, surveillance, and reconnaissance capabilities in near real time via a video downlink.
- **Situational awareness:** UASs can provide an aerial view for the threat to know "what is around a hill" and allow the enemy commander to adjust operational orders based on real-time intelligence.
- **Communications relay:** UASs can serve to extend the communications between ground forces in an otherwise degraded or limited communications environment.
- **Weapon delivery:** UASs have been used to either deliver ordnance to a target or the UAS itself can become a loitering munition. This includes chemical and radiological attacks.
- **Fire support:** UASs can be used to provide forward observer functionality that can enable adjustment of indirect fire.
- **Psychological warfare:** UASs seen as a weapon delivery platform or conducting intelligence, surveillance, or reconnaissance prior to an attack can cause panic by their presence alone.
- A loitering munition is a type of UAS designed to engage beyond line-of-sight ground targets with an explosive warhead. They are equipped with high-resolution electro-optical and infrared cameras that enable the controller to locate, surveil, and guide the vehicle to the target. A defining characteristic of loitering munitions is the ability to "loiter" in an area of airspace for an extended period before striking, giving the controller time to decide when and what to strike

3) UAS Groups

It provides an overview of the different groups of Unmanned Aircraft Systems (UAS) based on their weight, operating altitude, and speed.

UAS are categorized into five groups, from Group 1 to Group 5. The categorization is based on the weight, operating altitude, and speed of the UAS. The larger the platform, the more robust its suite of capabilities.

- **Group 1 UAS**, also known as micro/minи UAS, weigh between 0-20 lbs, operate at speeds less than 100 knots, and at altitudes less than 1,200 feet above ground level (AGL). They are generally hand-launched, commercial-off-the-shelf, radio-controlled platforms with limited ranges and small payload capabilities.
- **Group 2 UAS**, or small tactical UAS, weigh between 21-55 lbs, operate at speeds between 101-250 knots, and at altitudes less than 3,500 feet AGL. They have small airframes with low radar cross sections, providing medium range and endurance.
- **Group 3 UAS**, or tactical UAS, weigh between 56-1,320 lbs, operate at any speed, and at altitudes less than 18,000 feet (FL 180). They require a larger logistical footprint and their range and endurance vary significantly among platforms.
- **Group 4 UAS**, or strategic/theater UAS, weigh more than 1,320 lbs, operate at any speed, and at altitudes less than 18,000 feet (FL 180). They are relatively large systems operated at medium to high altitudes with extended range and endurance capabilities. They normally require a runway for launch and recovery.
- **Group 5 UAS**, or strategic UAS, weigh more than 1,320 lbs, operate at any speed, and at altitudes greater than 18,000 feet (FL 180). They operate at medium to high altitudes and have the greatest range, endurance, and airspeed. They require a large logistical footprint and have a suite of optics for targeting and weaponry for engagements.

UAS Groups 1 and 2 are commonly known as small-unmanned aircraft systems (sUASs). They have a lower radar cross-section than **Group 3, 4, and 5 UASs**, making them harder to detect by friendly forces' early warning and detection capabilities. For instance, the DJI MAVIC and Enterprise Dual are examples of threat Group 1 UAS, while the RQ-11 Raven is a friendly example

4) UAS Components

- A UAS is composed of the personnel, the unmanned aircraft vehicle (UAV), payload (sensors or weapons), control station, communication links, launch system, and recovery system. Different echelons and capabilities focus on defeating different parts of the system.
- When a UAV is in use, there are potentially up to four different communication links in action: L1 channel Global Positioning System (GPS) downlink, Command-and-control (C2) link, video downlink, and data link.

Each of these links can be targeted for disruption or exploitation.

- The L1 channel GPS downlink is needed to establish which way is up or down and its altitude. It is required if the UAS needs to fly to a specific point.
- The C2 link is the communication between the controller and the UAV. It is used to control the UAV and can be disrupted to cause the UAV to return to its home point or to land.
- The video downlink is used to send real-time video from the UAV to the controller. Disrupting this link can blind the operator.
- The data link is used to send other data from the UAV to the controller. This could include system status, GPS coordinates, or other sensor data.
- Targeting cells should focus on the three main components: the UAV, the controller, and the communication links.

5) UAV Types

UAS falls into groups based on weight, operating altitude, and speed. Each type of UAS has its advantages and limitations. Fixed-wing UAS have long endurance and can cover large areas, but they require a runway for takeoff and landing. Rotary-wing UAS can take off and land vertically, making them suitable for operations in confined areas, but they typically have shorter range and endurance compared to fixed-wing UAS. Balloon UAS can stay aloft for extended periods, providing persistent surveillance over an area, but they are subject to wind and weather conditions and have limited maneuverability.

a) Fixed-wing UAS

Fixed-wing UAS are typically found in Groups 4 and 5, which are characterized by weights greater than 1,320 lbs and can operate at any speed. These UAS operate at medium to high altitudes and have the greatest range, endurance, and airspeed. They require a large logistical footprint similar to manned aircraft and have a suite of optics for targeting and weaponry for engagements. Examples of fixed-wing UAS include the MQ-1C Gray Eagle, MQ-1A/B Predator, RQ-4 Global Hawk, and MQ-9 Reaper.

b) Rotary-wing / Multirotor UAS

Rotary-wing or multirotor UAS are typically found in Groups 1 and 2, which are characterized by weights ranging from 0 to 55 lbs and speeds less than 100 knots. These UAS operate at altitudes less than 1,200 feet above ground level (AGL) for Group 1 and less than 3,500 feet AGL for Group 2. They are generally hand-launched, radio-controlled platforms with limited ranges and small payload capabilities. They offer real-time video and are operated within the line of sight of the user. Examples of rotary-wing UAS include the DJI MAVIC and the RQ-11 Raven.

c) Balloon UAS

The balloon UAS could potentially fall into any of the groups depending on their weight, operating altitude, and speed. They

are typically used for surveillance and reconnaissance missions due to their ability to stay aloft for extended periods.

C. Planning

It emphasizes the importance of a comprehensive and integrated approach to C-UAS planning and execution, involving coordination across all echelons and warfighting functions to ensure effective defense against UAS threats.

1) Planning considerations

Effective counter-UAS (C-UAS) planning requires a combined arms approach that employs capabilities from all warfighting functions. Planning considerations include a layered defense approach, rules of engagement, airspace control, air defense warning conditions, weapon control status, early warning networks, and the Prioritized Protection List (PPL).

2) Layered approach

It emphasizes the importance of a layered defense strategy in countering unmanned aircraft systems (UAS). This approach combines active and passive measures to prevent threat UASs from detecting, targeting, or destroying their intended targets. Every action taken at each echelon makes the threat UAS harder to employ by increasing its risk and range it travels to accomplish its mission.

Every echelon contributes to Soldier survivability by creating a layered defense. This layered defense is a combination of active and passive measures that prevents threat UASs from detecting, targeting, or destroying its intended target. Every action taken at each echelon makes the threat UAS harder to employ by increasing its risk and range it travels to accomplish its mission.

A layered defense provides multiple engagement opportunities, ideally starting at the maximum range from friendly forces and before any attacking UAS can release their weapons.

The airspace control plan and area air defense plan should include detailed procedures for threat UAS detection, identification, decision-making, and engagement.

3) Rules of engagement

It outlines the responsibilities and considerations for commanders in engaging threat Unmanned Aircraft Vehicles (UAVs). Here are the rephrased key points:

- Commanders are tasked with the duty to take necessary actions to safeguard their forces and assets from attacks while ensuring that operations adhere to the established rules of engagement (ROE).
- The authority to engage threat UAVs can be delegated to lower levels to enable a swifter response. However, this delegation must be balanced against the risk of mistakenly engaging friendly UAVs, known as fratricide.

4) Airspace control

Divisions and brigades distribute the airspace coordination order (ACO), the unit airspace plan, and the current air picture via command-and-control systems accessible to subordinate units.

Control of airspace is managed by divisions and brigades through the distribution of the airspace coordination order (ACO), the unit airspace plan, and the current air picture. These are disseminated via command-and-control systems that are accessible to subordinate units. These systems include the command post computing environment (CPCE) and the joint battle command-platform (JBC-P). However, not all brigades and battalions have access to the tactical airspace integration system (TAIS), which is the command-and-control system that manages the air picture, forward area air defense command-and-control (FAADC2), or air and missile defense early warning systems (AMDWS). Units that lack air defense and air management (ADAM) cells and access to these systems are unable to maintain awareness of the current friendly air picture. They rely on higher echelons with these systems to share and create products they can use.

Brigades and battalions distribute airspace coordination orders and the current air picture to subordinate units through a combination of planning, active and passive measures, and the use of specific equipment. The planning phase includes considerations for each echelon, and the active and passive measures are part of a layered defense strategy to prevent threat Unmanned Aircraft Systems (UASs) from detecting, targeting, or destroying their intended target.

For command-and-control systems that subordinate units have access to for airspace coordination, the manual mentions that while there are many systems at division and above dedicated to counter enemy air threats, each echelon works to ensure that every soldier - no matter where they are on the battlefield, has the necessary information and ability to detect, identify, decide, and if needed to engage any air threat.

Brigades and battalions distribute airspace coordination orders (ACOs) and the current air picture to subordinate units through command-and-control systems that are accessible to these units. These systems include the Command Post Computing Environment (CPCE) and the Joint Battle Command-Platform (JBC-P). However, not all brigades and battalions have access to the Tactical Airspace Integration System (TAIS), which is the command-and-control system that manages the air picture, as well as the Forward Area Air Defense Command-and-control (FAADC2), or Air and Missile Defense Workstation (AMDWS). Units that lack Air Defense and Air Management (ADAM) cells and access to these systems rely on higher echelons with these systems to share information and create products for their use.

5) Air defense warning condition

Air defense warning (ADW) conditions are color-coded to correspond to the degree of air threat probability and are used to prepare units based on the assessed threat.

To assess their unit's ability to conduct both passive and active defensive measures against threat UAS, leaders can use video and other data collected from the flown threat UAS. This data can provide insights into the unit's performance and areas for improvement.

Units should integrate the following key tasks into their training for air defense warning condition:

- Train visual observers on how to look for and track Unmanned Aircraft Systems (UAS).
- Perform visual air threat recognition training.
- Practice various passive measures.
- Establish and use an early warning notification network

6) Weapon control status

It outlines the conditions under which air defense weapons are authorized to engage aerial threats, including Unmanned Aircraft Systems (UAS).

Weapon control status establishes the conditions under which air defense weapons are permitted to engage threats, with three levels: weapons free, weapons tight, and weapons hold.

- **Weapon Control Status (WCS):** WCS is a set of measures that dictate the conditions for engaging air threats. It is tailored to the tactical situation and can vary based on the weapon system, volume of airspace, or type of air platform.
- Three WCS for C-UAS:
 - **Weapons Free:** Units are allowed to engage any UAS not positively identified as friendly according to the rules of engagement (ROE). This status is the least restrictive.
 - **Weapons Tight:** Units are only permitted to engage UASs that are positively identified as hostile according to the ROE.
 - **Weapons Hold:** Units may only fire in self-defense or when ordered by a higher authority. This status is the most restrictive.
- **Brigade AMD Cell:** The brigade Air and Missile Defense (AMD) cell may establish separate WCS for different air threats or an overall control status for any air engagement. The cell is responsible for integrating these measures into the broader air defense strategy.
- **Decision-Making:** The WCS reflects the level of control necessary over air defense weapon systems and is influenced by the current tactical situation. Commanders at all levels must balance the need for rapid response against the risk of fratricide or other unintended consequences.

The WCS is a critical component of air defense planning, ensuring that units have clear guidance on when and how to engage potential air threats while minimizing the risk of friendly fire and collateral damage.

7) Early warning network

It discusses the establishment of an air threat early warning network as part of counter-reconnaissance efforts. Units establish an air threat early warning network, usually communicated over frequency modulation (FM), to share air threat situational understanding for units without dedicated air defense command-and-control systems.

- **Establishment of an Early Warning Network:** All units are advised to set up an air threat early warning network, which is typically communicated over frequency modulation (FM). This network is a means of sharing air threat situational understanding for units that do not have dedicated air defense command-and-control systems.
- **Alerting Everyone:** The early warning network is designed to alert all units of potential air threats, enhancing the overall situational awareness and preparedness of the force.
- **Practice and Efficiency:** Units are encouraged to practice relaying information using this network to reduce the time required to notify everyone of air threats. This practice is crucial for ensuring that the network functions efficiently and effectively when real threats are detected.

8) Prioritized protection list (PPL)

Units develop a PPL to prioritize the use of assigned or allocated protection capabilities, focusing on defending critical assets.

In military operations, the purpose of a Prioritized Protection List (PPL) is to identify and prioritize the protection of critical assets that are essential for mission success. The PPL helps commanders focus their limited protection resources on defending the most important elements within their area of responsibility, such as command-and-control nodes, logistics areas, or high-value units.

The key components of a PPL include:

- **Critical Assets:** These are the people, property, equipment, activities, operations, information, facilities, or materials that are deemed essential for the mission.
- **Criticality:** The importance of the asset to the mission.
- **Threat Vulnerability:** The susceptibility of the asset to potential threats.
- **Threat Probability:** The likelihood that a threat will target or impact the asset.

A PPL can be used to prioritize protection measures for personnel and equipment by:

- **Identifying Critical Assets:** Determining which assets are vital to the mission's success.
- **Assessing Risks:** Evaluating the vulnerability and threat probability to each critical asset.
- **Prioritizing Assets:** Ranking the critical assets based on their criticality and the assessed risks.
- **Allocating Resources:** Directing protection capabilities, such as air defense assets, physical security measures, or camouflage and concealment efforts, to the highest-priority assets.

- **Continuous Assessment:** Regularly reviewing and updating the PPL to reflect changes in the operational environment, asset criticality, or threat assessment.

The PPL is a dynamic tool that is continuously assessed and revised throughout each phase or major activity of an operation. It is developed by the brigade's protection cell using guidance from the brigade commander and division's PPL during mission analysis. The protection working group recommends protection priorities and establishes the brigade's PPL based on criticality, threat vulnerability, and threat probability.

A PPL, or Prioritized Protection List, is the most critical assets in an organization that need to be protected. These assets can include physical assets, such as buildings or equipment, as well as digital assets, such as data or software systems. The PPL is typically used in the context of military or cybersecurity operations, where it helps to guide resource allocation and strategic planning for defense and protection efforts.

On the other hand, a protection plan is a broader term that can refer to any strategy or policy designed to protect something. This could include insurance policies, security protocols, or disaster recovery plans. A protection plan outlines the steps that will be taken to protect the assets or individuals covered by the plan.

The frequency of updating a PPL can depend on various factors such as changes in the threat landscape, introduction of new assets, or changes in the value or importance of existing assets. However, it's generally recommended to review and update the PPL regularly, at least annually, or whenever significant changes occur.

Examples of protection measures that can be prioritized on a PPL could include:

- Implementing robust cybersecurity measures for critical digital assets, such as firewalls, encryption, and intrusion detection systems.
- Physical security measures for important buildings or equipment, such as surveillance systems, access controls, and security personnel.
- Regular audits and inspections to ensure the effectiveness of the protection measures.
- Training and awareness programs for personnel to ensure they understand the importance of the assets and how to protect them.

9) Planning capabilities and considerations by echelon

Brigades and higher headquarters integrate C-UAS into the military decision-making process, targeting, intelligence preparation of the battlefield (IPB), and protection processes.

Each echelon employs different air defense capabilities, with divisions and above analyzing and planning to mitigate the UAS threat.

Brigade and higher headquarters are tasked with incorporating C-UAS into the military decision-making process, including targeting, intelligence preparation of the battlefield (IPB), and protection strategies. The Air Defense and Airspace

Management (ADAM) and Brigade Aviation Element (BAE) cells support airspace management and the deployment of air defense weapons. A multi-echelon approach is required for the C-UAS fight, with higher echelons providing resources to help lower echelons mitigate UAS threats. Brigades and below are responsible for executing protection and survivability measures against UAS threats and engaging any immediate threats.

Divisions and higher echelons analyze and plan to counter the UAS threat, directing C-UAS capabilities to improve the survivability of subordinate forces and protect critical assets. These assets may be allocated to a brigade to ensure overlapping and mutual support with the brigade's own weapon systems. Divisions also ensure that a real-time common threat air operating picture is maintained. While most brigades lack dedicated air defense capabilities, they have air defense personnel on staff who assist with planning and coordinating air defense activities with both higher and subordinate echelons. Battalions, with less extensive staff than brigades, rely on brigade products and systems to support their companies. Companies and below, which do not have dedicated staff, treat threat UASs as they would any other threat.

Each echelon possesses distinct air defense capabilities. Divisions and higher echelons analyze and plan to counter the UAS threat, directing C-UAS capabilities to protect subordinate forces and critical assets. These assets may be allocated to a brigade to provide mutual support with the brigade's own weapon systems. Divisions also ensure that a real-time common threat air operating picture is maintained. While most brigades lack dedicated air defense capabilities, they have air defense personnel to assist with planning and coordination. Battalions, with less robust staff, rely on brigade products and systems to support their companies. Companies and below, without dedicated staff, treat threat UASs as they would any other threat.

10) Brigade planning considerations

Brigades establish C-UAS plans to protect friendly forces, direct asset positioning, plan sensor coverage, and conduct force movement in line with higher echelon plans.

Brigade planning considerations include reporting techniques, positive identification, alert dissemination, rules of engagement, and coordination with friendly mission command nodes and airspace users.

Brigades are responsible for creating C-UAS plans to safeguard friendly forces within their designated areas. They are tasked with the strategic placement of assets, planning for sensor coverage, and coordinating the movement of forces in alignment with the plans and objectives of division and corps. This includes updating priority tasks and ensuring the security of vital assets.

Brigade planning should consider reporting methods, clear identification of threats, the dissemination of alerts, and adherence to rules of engagement.

- Circulating air defense warnings and weapons control statuses.
- Setting up general and specific air defense warnings based on current assessments of air threats.

- Adjusting the Prioritized Protection List (PPL) according to intelligence preparation of the battlefield, risk levels, and the commander's evaluation.
- Refining the rules of engagement for UAS.
- Establishing who has the authority to identify threats.
- Updating and sharing the division's engagement authority.
- Coordinating sensor coverage that might exceed the brigade's inherent sensor capabilities.
- Collaborating with allied mission command nodes and airspace users to minimize the risk of fratricide.
- Instituting notification procedures.
- Forming suitable command or support relationships among the deployed C-UAS capabilities.

11) Brigade ADAM/BAE Cell

The brigade Air Defense and Airspace Management (ADAM) cell and Brigade Aviation Element (BAE) cell work together to maximize the combat effectiveness of counter-air systems and minimize the risk of friendly fire incidents and collateral damage.

The Brigade ADAM cell and the BAE cell collaborate to enhance the combat efficiency of counter-air systems and reduce the likelihood of friendly fire incidents and collateral damage.

- Creating, managing, and executing a C-UAS layered defense plan, which involves planning the use of C-UAS equipment, sensors, and capabilities, understanding the optimal use of various C-UAS systems, and understanding how C-UAS capabilities impact friendly operations.
- Developing and sharing the brigade's airspace plan, creating standard operating procedures for friendly air actions and responses to air threats, and developing counter-air tactics, techniques, and procedures tailored to the estimated threat environment.
- Integrating friendly C-UAS capabilities into the brigade common operational picture.
- Collaborating with the intelligence section to develop the enemy air situational template (SITEMP).
- Implementing higher headquarters' C-UAS rules of engagement (ROEs), rules for use of force, and special instructions (SPINS).
- Recommending unit ROEs, rules for use of force, and SPINS to the brigade commander.
- Implementing and adhering to required host-nation policies and procedures for C-UAS.
- Assessing the effectiveness of the C-UAS layered defense after a C-UAS engagement, adjusting as necessary, and providing feedback via lessons learned to both higher echelons and subordinate units.

It's important to note that the ADAM capabilities in a combat aviation brigade and maneuver enhancement brigade do not have an aviation operations component and therefore have a very limited capability to perform BAE functions.

The Brigade ADAM/BAE cell also maintains a C-UAS running estimate, which includes the location and status of all brigade C-UAS assets, capabilities of available C-UAS equipment, and past, current, and anticipated enemy UAS activity.

12) Battalion planning considerations

Battalions integrate brigade guidance to form a coherent scheme of protection and shape their C-UAS planning and actions accordingly.

Battalions develop a cohesive scheme of protection by integrating guidance from brigades. To effectively counter unknown UAVs, battalions need situational awareness of friendly aircraft in their area. Battalion C-UAS planning and actions are shaped by:

- Incorporating and sharing the unit airspace plan to maintain awareness of friendly aircraft, aiding in C-UAS identification and reducing fratricide.
- Utilizing attack guidance, targeting processes, and reporting requirements to support the targeting process.
- Following air defense coordinating instructions and ROE guidance, which informs the employment of air defense and C-UAS assets and capabilities.
- Selecting the best combination of C-UAS capabilities to establish a layered defense.
- Understanding and integrating brigade collection efforts and reporting requirements.

The battalion intelligence section, as part of the Intelligence Preparation of the Battlefield (IPB), produces materials that help the battalion develop a concept of protection, including a threat assessment. This assessment covers:

- Potential threat UAS groups in the battalion's area of operations.
- Threat UAS capabilities.
- Expected number of threat UASs.
- UAS employment techniques.
- Likely launch and recovery sites.
- Probable payload capabilities.
- Threat UAS flight profiles.
- Coordination of sensors with the brigade.

The battalion then develops a concept of protection that incorporates C-UAS actions based on intelligence estimates and analysis, focusing resources to effectively mitigate UAS and other threats. Additional instructions for companies, such as threat UAS reporting procedures, weapon control status, and engagement criteria, are included under coordinating instructions. The battalion staff ensures that all subordinate unit

C-UAS battle drills align with the battalion's concept of protection.

Companies and below implement the concept of protection developed at the battalion level, focusing on reacting to air contact battle drills and examining their unit's active and passive measures.

The concept of protection, as developed at the battalion level, is implemented by companies and below. The primary emphasis during troop leading procedures is on responding to air contact battle drills. Leaders at the company level and below conduct rehearsals and assess their unit's active and passive measures. These rehearsals evaluate aspects such as air guard locations, assigned sectors, UAS reporting procedures, communication plans, ADW status, weapon control status, engagement criteria, and threat UAS identification."

D. Defensive C-UAS Actions

It focuses on defensive actions against unmanned aircraft systems (UAS).

- **C-UAS Training:** emphasizes the importance of C-UAS training, which can be a stand-alone situational training exercise. However, greater training benefits would come from incorporating it into already planned training. Units should focus on UAS threat capabilities, the dangers that threat UASs may impose on the unit, and associated battle drills once the UAS is detected.
- **Key Tasks:** Examples of key tasks to integrate into unit training include training visual observers how to look for and track UAS, performing visual air threat recognition training, practicing various passive measures, and establishing and using an early warning notification network.
- **Training Aids and Simulations:** Leaders can leverage specifically designed training aids, devices, simulators, and simulations from their installation's training support center to enhance collective task training in the defeat and mitigation of CUAS threats.
- **Assessment of Defensive Measures:** Leaders use video and other data collected from the flown threat UAS to assess their unit's ability to conduct both passive and active defensive measures.
- **Updating Training and Education:** Threat UASs and their employment techniques change faster than doctrine does. Leaders are encouraged to update their training and education with the most current and relevant information based on lessons learned, enemy trends, and friendly C-UAS tactics, techniques, and procedures.

1) Passive measures

Passive measures are the first line of defense against air threats and are designed to improve survivability by reducing the likelihood of detection and targeting of friendly assets.

These measures include camouflage and concealment, deception, dispersion, displacement, and hardening and protective construction.

Effective camouflage and concealment techniques are crucial, especially against visual sensors, as they make it difficult for threat UAS to detect or identify targets.

Units must consider various sensor types, such as near-infrared and ultraviolet sensors, and employ appropriate countermeasures like light discipline and terrain masking.

Passive measures against Counter-Unmanned Aircraft System (C-UAS) threats are those that do not involve active engagement or destruction of the threat. They are primarily focused on reducing the effectiveness of the threat through methods such as detection, identification, and avoidance.

- **Fundamentals:** Emphasizes the importance of making targets resemble their background to reduce detection by UAS. This involves skills in camouflage and concealment and understanding of threat electromagnetic sensors.
- **Environmental Modification:** Suggests altering the physical environment or employing camouflage to improve concealment and prevent observation.
- **Sensor Challenges:** Highlights the need to plan camouflage and concealment activities to defeat enemy sensors across the electromagnetic spectrum.
- **Signal Management:** Advises on removing signal sources, like Wi-Fi or Bluetooth emissions, that could lead to detection in non-urban environments.
- **Visual and Near-Infrared Sensors:** Discusses effective camouflage against visual sensors and the importance of light discipline to counter near-infrared sensors.
- **Infrared and Ultraviolet Sensors:** Recommends natural materials and terrain to shield heat sources from infrared sensors and specific countermeasures against ultraviolet sensors in snow-covered areas.
- **Movement and Patterns:** Stresses minimizing movement and avoiding operational patterns to reduce detection risk.

a) *Defensive C-UAS Actions*

It outlines the importance of blending in with the environment to reduce the likelihood of detection by enemy UAS.

- **Principle of Camouflage and Concealment:** The more a target resembles its background, the harder it is for threat UAS to distinguish between them. Proper skills and awareness of threat electromagnetic sensors are crucial for effective camouflage and concealment.
- **Altering the Environment:** When natural concealment is insufficient, military forces can alter the physical environment to improve concealment for personnel and assets. They can also employ camouflage to confuse or mislead the enemy.
- **Sensor Challenges:** Camouflage and concealment must consider the variety of sensors that operate across the electromagnetic spectrum. Leaders must assess their tactical situation and plan accordingly to defeat enemy sensors in visual, infrared, or radar spectrums.

- **Signal Management:** Sometimes it is more effective to remove the source of a signal, such as Wi-Fi or Bluetooth emissions from smart devices, rather than trying to camouflage it, especially in environments where civilian signals do not mask military signatures.
- **Visual and Near-Infrared Sights:** Effective camouflage and concealment techniques in the visual portion of the electromagnetic spectrum are vital. Field uniforms, camouflage screening paint, and battlefield obscurants can provide effective camouflage against visual and near-infrared sensors.
- **Infrared and Ultraviolet Sensors:** Natural materials and terrain can shield heat sources from infrared sensors. In snow-covered areas, winter paint patterns and terrain masking are critical for defending against ultraviolet sensors.
- **Camouflage Techniques:** Units should minimize movement, avoid operational patterns, and manage equipment patterns to reduce detection. They should also consider the reflectance, shape, shadow, texture, and patterns of objects when applying camouflage.
- **Camouflage Discipline:** Camouflage and concealment discipline is continuous and applies to every soldier. It involves regulating light, heat, noise, spoil, trash, and movement to avoid giving away unit positions or activities.
- **Camouflage and Concealment Techniques:** Techniques include hiding, blending, disguising, disrupting, and decoying. These techniques are used to screen, alter, or eliminate target characteristics and create false targets to draw enemy attention away from actual assets.
- **Deception with Decoys:** Decoys can be used to attract enemy attention and draw fire away from real targets, enhancing friendly survivability and deceiving the enemy about the strength and location of friendly forces.
- **Dispersion and Displacement:** Dispersion spreads out troops and material to reduce vulnerability, while displacement involves moving to alternate locations to avoid further attacks or to render the current attack ineffective.
- **Hardening and Protective Construction:** This involves enhancing physical protection of key assets through measures such as adding sandbags or constructing bunkers to protect against UAS-delivered ordnance

b) *Threat Sensor Systems*

The importance of effective camouflage and concealment techniques in the visual portion of the electromagnetic spectrum cannot be overstated, as visual sensors are the most abundant, reliable, and timely enemy sensors. Being invisible often makes it challenging to detect, identify, and target. Field uniforms, standard camouflage screening paint patterns, ultra-lightweight camouflage-net system (ULCANS), and battlefield obscurants are effective against visual sensors. Full-coverage camouflage

and concealment, including vertical camouflage, help evade visual detection by the enemy. When time is limited, prioritize camouflage and concealment to protect from the most probable direction of attack, then address the rest as time permits.

Near-infrared sights are effective at shorter ranges. Red filters, while preserving night vision, cannot prevent near-infrared sensors from detecting light from long distances. Therefore, strict light discipline is a crucial countermeasure to near-infrared sensors and visual sensors, such as image intensifiers. Standard camouflage screening paint patterns, battlefield obscurants, and certain uniforms are designed to counter near-infrared sensors.

Natural materials and terrain can shield heat sources from infrared sensors and disrupt the shape of cold and warm military targets viewed on infrared sensors. Avoid raising vehicle hoods to break windshield glare as this exposes a hot spot for infrared detection. Even if the infrared system can locate a target, the identity of the target can still be disguised. Avoid building fires and using vehicle heaters. Infrared-defeating obscurants, chemical-resistant paints, and certain uniforms are designed to help break up infrared signatures, but they do not defeat infrared sensors.

Enemy use of ultraviolet sensors poses a significant threat in snow-covered areas. Winter paint patterns, the arctic-style lightweight camouflage screen system (known as LCSS), and terrain masking are critical means for defending against these sensors. Any kind of smoke defeats ultraviolet sensors. Field-expedient countermeasures, such as constructing snow walls, also provide a means of defeating ultraviolet sensors.

To defeat these various sensors, units need to minimize movement and avoid operational patterns. Movement attracts enemy attention and produces several signatures (tracks, noise, hot spots, dust). In operations that inherently involve movement (such as offensive tasks), leaders plan and manage movement so that signatures are reduced as much as possible. If movement must be done, slow, regular movement is usually less obvious than fast, erratic movement.

An enemy can often detect and identify different types of units or operations by analyzing the signature patterns that accompany their activities. For example, an offensive is usually preceded by the forward movement of engineer obstacle reduction assets; petroleum oils, and lubricants; and ammunition. Such movements are very difficult to conceal; therefore, as an alternative, the pattern of resupply can be modified. An enemy recognizes repetitive use of the same camouflage and concealment techniques.

To effectively camouflage from aerial observation, units consider the threat viewpoint. Prevent patterns in anti-detection countermeasures by applying the following recognition factors to tactical situations. These factors describe a target's contrast with its background: Reflectance, Shape, Shadow, Texture, and Patterns

Effective camouflage and concealment techniques against visual sensors include:

- **Natural camouflage:** Use of natural elements like foliage, trees, and terrain to blend into the environment.

- **Artificial camouflage:** Use of camouflage nets, paints, and uniforms that match the environment.
- **Disguise:** Altering the appearance to resemble something else, like a natural feature or a harmless object.
- **Shadow and light control:** Utilizing shadows and controlling reflective surfaces to avoid detection.
- **Movement control:** Limiting unnecessary movement, especially during daylight hours, to avoid attracting attention.

To defeat near-infrared sensors, units can:

- **Use IR-blocking materials:** Certain materials can block or absorb IR radiation, making them effective for camouflage.
- **Control heat signatures:** Minimizing heat emissions from bodies, equipment, and vehicles can help evade detection by near-infrared sensors.
- **Use smoke:** Certain types of smoke can block near-infrared sensors.

Countermeasures against ultraviolet sensors in snow-covered areas include:

- **UV-absorbing materials:** Using materials that absorb UV radiation can help camouflage against UV sensors.
- **Snow camouflage:** Using white or snow-patterned camouflage can help blend into the snowy environment.
- **Avoiding UV-reflective materials:** Certain materials, like some metals, can reflect UV light and should be avoided

Effective camouflage and concealment techniques against near-infrared sensors include:

- **Using materials that absorb infrared radiation:** Certain materials, such as specialized paints and fabrics, can absorb infrared radiation, making objects coated or covered with them less visible to near-infrared sensors.
- **Thermal camouflage:** This involves managing heat signatures to blend with the surrounding environment. This can be achieved by using thermal blankets or suits that mask the heat emitted by the human body or equipment.
- **Natural cover:** Using natural elements like trees, bushes, and terrain can help to break up and conceal infrared signatures.

Effective countermeasures against ultraviolet sensors in non-snow-covered areas include:

- **UV-absorbing materials:** Using materials or coatings that absorb UV radiation can help to reduce visibility to UV sensors.
- **Natural cover:** Similar to infrared camouflage, using natural elements can help to conceal UV signatures.

- **Smoke:** Certain types of smoke can effectively scatter UV radiation, making it harder for UV sensors to detect objects.

Effective ways to detect visual sensors used by enemy units include:

- **Visual observation:** Training visual observers to look for and track UAS (Unmanned Aircraft Systems) can be an effective method of detecting visual sensors
- **Electromagnetic warfare packages:** These can assist in detecting threat UAS, which often carry visual sensors.
- **Use of radar systems:** Systems like the AN/APG-78 Longbow fire control radar on the Apache attack helicopter can assist in detecting threat UAS.
- **Early warning notification network:** Establishing and using an early warning notification network can help in detecting and responding to visual sensors used by enemy units

2) Active measures

Active measures involve a multi-step sequence to detect, identify, decide, and potentially engage an unknown UAS.

Detection is challenging due to the small, maneuverable, and quiet nature of UAS. Environmental conditions and tactical maneuvers by experienced operators can further complicate detection.

Identification is critical to avoid fratricide and requires early determination of the UAS's friendly or hostile characteristics.

Decision-making involves determining the necessity to engage and selecting the appropriate methods, which can be physical (e.g., small arms, projectiles) or nonphysical (e.g., jamming, spoofing)

Active measures includes tactics, techniques, and procedures for detecting, identifying, deciding, and engaging any air threat, including UASs. These measures may involve the use of various technologies and systems to counter enemy air threats. Every Soldier, regardless of their location on the battlefield, should have the necessary information and ability to implement these active measures

a) Detection

Unmanned Aerial Systems (UAS) are compact, agile, and silent, making them challenging to spot, even for trained observers. Factors such as time of day, light conditions, weather, and observer alertness can affect the ability to detect a potentially hostile UAS. Specialized tracking and identification technology may be necessary due to these environmental conditions.

Experienced UAS operators can employ various tactics to exploit the characteristics of these systems, including:

- Flying at low altitudes, using terrain, vertical obstacles, or urban environments to conceal their approach to a target.

- Performing multiple false take-offs and approaches to the intended target.
- Adopting erratic flight patterns to confuse personnel and make visual tracking difficult.
- Using sunlight or cloud cover to hide the UAS from view.
- Flying against the wind to reduce the detectable sound of the UAS.
- Utilizing sport flying modes to increase speed and agility, reducing observation time.
- Deploying multiple UAS to confuse and overwhelm observers, making tracking and neutralization more challenging.
- Flying a pre-programmed flight path to reduce risk to the operator, allowing for the control link to be disconnected in-flight and re-established over the target area from a different location.

The detection capability of a unit is determined by the types and placement of sensors. Factors such as the types of threat UAS, threat axis of advance, terrain, weather, time-distance analysis, friendly defended assets, desired engagement zone, surveillance requirements, and the number of available assets influence the optimal placement and use of sensors.

Various sensor capabilities, including RADAR, radio frequency, audible, and optical devices, can be used to form an integrated sensor network. Regardless of the sensor capabilities a unit possesses, all soldiers need to be aware of air threats and constantly look up before and during any movements. Dedicated air guards can assist in air threat detection and engagement.

The types of sensors and their placement determine the unit's detection capability. For sensor placement, integrating and networking sensors to develop the enemy threat UAS situation should be applied. The use of various types of sensors is warranted as currently there is no one type of sensor that is 100% effective.

Various sensor capabilities outside of visual (observer) could include RADAR, radio frequency, audible, and optical devices. The goal is to form an integrated sensor network that includes various sensor types. Sensor capabilities in support of low-level air threats are planned accordingly and coordinated in advance. Leaders may have to coordinate through higher echelons for additional sensor capabilities. No matter what sensor capabilities a unit has, all soldiers need to be aware of the air threats and constantly look up before and during any movements. Dedicated air guards are another way units can assist in air threat detection and engagement

b) Air Guards

Air guards play a vital role in spotting aerial threats and providing early warnings. They must be vigilant and equipped with the necessary optical gear to perform search and scan techniques.

Air guards should be aware of the air threats and maintain visual contact with the target throughout the engagement.

Air Guards are tasked with maintaining constant vigilance, with their focus on the horizon. They are responsible for identifying aerial threats near the unit's location and providing early warnings of potential air threats. They cover sectors that include likely approaches for enemy aircraft and are utilized during both mounted and dismounted offensive and defensive operations.

If equipped with C-UAS capabilities, air guards are authorized to engage targets following the rules of engagement (ROE) and weapon control status. They should be positioned within visual range of the unit, typically between 500 meters and 1.5 kilometers, to effectively spot, hear, and report threats.

Air guards must be capable of operating in all conditions and should be equipped with the necessary optical equipment to conduct search and scan techniques, reducing the enemy's ability to avoid detection.

When scanning for UAS, air guards should not focus solely on the horizon, as this may cause them to miss higher or lower flying aircraft. The optimal search range is 20 degrees above and below the horizon. An outstretched arm with extended fingers can approximate this 20-degree range.

The vertical scan technique optimizes a soldier's vision for finding air threats by moving the eyes upward towards the sky and then down to the horizon, continuing across the terrain. The horizontal scan involves eye movements across the sky, working upward to about 20 degrees, and then scanning down to detect low-flying threats.

Before starting duty, air guards undergo a precombat inspection to ensure they have the correct equipment and are briefed on the current threat. The air guard checklist includes understanding the types and characteristics of threat UAS, current UAS trends, local air threats, detection equipment, available C-UAS equipment, secure radio operations, unit call signs, military maps, orientation techniques, and range cards.

c) Warning

Engagement decisions are made based on the threat's severity, potential impact on unit effectiveness, and engagement area. Volume fire is an effective method when using small arms against aerial threats.

Upon detection of an air threat, it is crucial to promptly alert all allied forces. This can be achieved through two strategies: a top-down or a bottom-up approach. Small Unmanned Aerial Vehicles (UAVs) are often first spotted by forward units, making it essential to practice the use of the unit early warning network and bottom-up rehearsals. Regardless of the method employed, the SALUTE report format is used to relay the information. Receiving this report should prompt further actions for all units, such as halting in place or engaging the threat with lethal or non-lethal means. If feasible, units that detect air threats should notify neighboring units.

In the top-down approach, Air and Missile Defense (AMD) cells at the brigade level and above identify threats and alert sites by disseminating early warnings both digitally and vocally to all their subordinate units. This is done automatically from the staff planning and battlespace situational awareness tool (currently AMDWs) through the JBC-P. However, as not all digital

systems function properly or are monitored, voice communication is also used. The brigade AMD cell uses frequency modulation (FM) radio to transmit a flash message that a threat UAS has been spotted in the area of operations over the brigade operations and intelligence network. This message is quickly relayed over their operations and intelligence networks by battalions, then by companies over their company network, and finally by platoons over their internal networks, and if necessary, over the required squad communication systems to ensure everyone is informed. This process is time-consuming, so the faster these flash messages are relayed, the quicker the force can respond appropriately.

In the bottom-up approach, any observer who detects an air threat initiates the process in reverse. They use their local platoon network to pass their flash message, which is then relayed to the company network, then to the battalion operations and intelligence network, and finally to the brigade operations network. Here, the brigade AMD cell inputs the necessary information into the appropriate system to ensure early warning across the entire formation. The first echelon with a battlefield situational awareness tool (such as the JBC-P) creates a digital warning to assist in quickly alerting the entire formation.

Regardless of how a soldier is alerted, their initial reaction upon receiving the air threat warning should be to freeze, as the threat can detect movement. After quickly assessing that they are not currently being observed, they should move to cover and concealment and wait for the all-clear report before resuming their current mission.

Simultaneously with providing warning, friendly forces track the target and monitor its movement. This tracking should continue until a decision is made to engage or not engage the target and is successful. A location is a static estimated report or display of where an air threat is located at a given moment. A system track is a compilation of location reports over a period of time. Depending on the system used, the system track can be reported as a heat map display, quadrant alert, or a circle to indicate estimated center and location error or line of bearing. The detection plan directly contributes to the unit's ability to continuously and efficiently track airborne objects

d) Identify

Identification is the process of discerning whether an unknown detected contact is friend or foe. For the effective use of Counter-Unmanned Aerial Systems (C-UAS) capabilities, early identification of Unmanned Aerial Systems (UAS) is crucial to maximize engagement times and prevent friendly fire. The challenge lies in differentiating between friendly, neutral, and hostile aerial objects while deploying various weapon systems against threatening UAS, as the same UAS could be operated by both friendly and enemy forces. Accurate identification enables leaders to make engagement decisions and improves situational awareness. Prompt identification enhances weapon employment options, aids in preserving friendly resources, and minimizes the risk of friendly fire.

There are two identification methods: procedural and positive. Positive identification, which is the preferred method, is derived from observing and analyzing target characteristics, including visual recognition, electronic support systems, non-

cooperative target recognition techniques, identification friend or foe systems, or other physics-based identification techniques. Procedural identification, on the other hand, differentiates airspace users based on geography, altitude, heading, time, and maneuver. Generally, a combination of positive and procedural identification is used.

Identification of a UAS should ideally lead to a specific name or category or the exact make and model of the UAS. It's also important to identify its payload if possible. The process of assigning an identification to a track will likely depend on several criteria.

e) Decision

The "Decide" phase involves two key decisions. The first is determining whether engagement is necessary. If the decision to engage is made, the second decision involves choosing the methods to mitigate or neutralize the threat posed by a UAS. These methods can be physical or nonphysical, and some organizations may have cyber capabilities that encompass both types. The level of delegation aligns with the rules of engagement, available airspace, potential for collateral damage, and the inherent right of self-defense.

Physical methods aim to destroy or damage the device to render it non-operational.

- Explosive munitions
- Small arms
- Projectiles
- Entanglement methods such as streamers or spray foam
- Directed Energy methods like lasers or high-power microwaves
- Capture methods like nets

Small arms techniques used in air defense involve the use of volume fire and proper aiming points based on the target's direction. These techniques are most effective against low flying UASs due to the range and destructive capability limitations of small arms. The decision to use small arms against threat UASs is made by the unit commander and is based on the situation, including the severity of the threat, potential impact on the unit's effectiveness, and the area of engagement (urban versus rural).

Volume fire is an effective method when using small arms fire against aerial threats. The key to success is to put out a high volume of fire towards the immediate threat. Even if these fires do not hit the enemy, creating a "wall of lead" in the sky can intimidate threat UAS pilots, potentially causing them to break off their attack or distracting them from taking proper aim.

When the decision is made to engage an aircraft with small arms, every weapon (M4, M240, M249, and M2) should be used with the goal of placing as many bullets as possible in the enemy's flight path. This does not mean that everyone fires in some random direction. Instead, everyone selects an aiming point in front of the target and fires at that point. This aiming point is determined using the football field technique. Practical considerations need to be taken into account before engaging, such as the range and capabilities of the available weapons. For

example, engaging a UAS from a range of 3 kilometers with small arms is ineffective, while the best possibility may be the use of the main gun on a tank or tracked vehicle. Small arms have a low probability of kill against attacking UAS due to their size, speed, and maneuverability

f) Defeat Techniques

Defeat techniques are initiated once airspace deconfliction and target engagement authority are passed to the tactical level. These techniques can be non-lethal or lethal, and they may require RF deconfliction to prevent frequency fratricide.

g) Exploitation

Exploitation is crucial for developing UAS countermeasures. Efforts should be made to collect downed UAS systems and their components for intelligence and analysis

h) Football Field Technique

The "Football Field Technique" is a straightforward approach to gauge lead distance. The idea is based on the assumption that most individuals have either played or watched football and thus have a sense of the length of a football field. When instructed to lead the target by the length of one football field, everyone aims at roughly the same point in space. Any inaccuracies in one person's estimation of the football field's length will be counterbalanced by another person's estimation. This variation in aiming points ensures that concentrated fire is delivered into a space ahead of the target rather than at a single point. Additionally, the different viewpoints from which soldiers observe the target will further distribute the fire over a larger space.

"Aiming Points" used to engage threat Unmanned Aerial Vehicles (UAVs) vary but can be applied to different threats. For instance, if enemy helicopters are detected and the decision is made to engage, they should be treated as a group 5 rotary wing UAV. The rules for selecting aiming points are straightforward, easy to learn, and remember.

"Firing Position Techniques For Small Arms" are the same for rifle marksmanship and countering threat UAVs with small arms, except for the prone position. When firing at UAVs, soldiers lie on their backs (supine), aiming their rifles into the air. If you are in an individual fighting position, stay there and return fire from the supported standing position. If you are not in an individual firing position, you should look for a tree, a large rock, or supportive object to help stabilize the weapon and provide protection. The following firing positions should be used accordingly.

"Engaging With Machine Guns" is effective against slow-moving UAVs. To maintain the volume of fire and destroy a target, a continuous burst of 20-to-25 rounds should be fired using a tracer on target method, allowing the gunner to adjust rounds on target.

"Nonphysical methods" defeat the device by disrupting, blocking, or controlling the signal between the UAV's optical, flight control, and ground control station. Even though nonphysical methods are used on the UAV, these methods may still cause it to crash and cause collateral damage. Examples of nonphysical methods include, but are not limited to, radio

frequency jamming, GPS jamming, GPS spoofing, dazzling, and position, navigation, and timing (known as PNT) jamming

i) Defense

The process of defeating a small Unmanned Aircraft System (sUAS) begins once airspace deconfliction and target engagement authority are delegated to the tactical level. To avoid friendly fire and confirm the identity of the sUAS, several procedures and processes are implemented. Depending on the method of engagement, Radio Frequency (RF) deconfliction might be necessary. There could be instances where operational RF spectrums overlap with the control frequency of the sUAS. It is the responsibility of key leaders to identify and mitigate frequency fratricide during defeat measures.

Defeat measures can be either non-lethal or lethal. In non-lethal responses, continuous jamming is crucial until the UAS is rendered inoperable. After a lethal or non-lethal response, and once the UAS has lost its control-link, explosive ordnance disposal should be requested to ensure the UAS is safe. Once the UAS is deemed safe, it can be submitted for weapons intelligence and analysis.

Once the decision to engage is made and the capability to do so is determined, the chosen capability is deployed. Other capabilities continue to track the target in case the initial engagement misses, allowing for re-engagement as necessary.

Exploitation is a key aspect in the development of UAS countermeasures. Efforts should be made to collect downed UAS systems and their components. When soldiers encounter a downed UAS, they should use their optics from a safe distance to look for indicators of suspicious items such as explosives, modifications, or other types of explosive payloads. If possible, they should check the immediate area for potentially dropped payloads or additional grounded UAVs. If no explosive hazards are found, they should collect as much of the UAV as possible and expedite its movement to their higher echelon for exploitation.

If an explosive hazard is suspected, the UAV should be marked and reported for action by explosive ordnance disposal or other trained personnel once operational conditions allow. Units should mark the hazard with engineer tape, VS-17 panel, or any other high visibility durable material that allows the explosive ordnance disposal team to identify the hazard's location from 50 to 100 meters. The location of the item should be marked on the units' situational awareness system (such as JBC-P) or Joint Capabilities Release (known as JCR) with a ten-digit grid. Units request explosive ordnance disposal through their chain of command using the necessary reports.

E. Offensive C-UAS Actions

It underscores the importance of offensive actions in countering UAS threats. It provides a comprehensive guide for planning and executing offensive C-UAS operations, emphasizing the need for intelligence, information collection, and effective targeting strategies. It focuses on offensive C-UAS actions.

1) Intelligence Preparation of the Battlefield

IPB is crucial for identifying threat UAS capabilities, employment concepts, strategies, and tactics. It is a continuous

process involving defining the operational environment, describing environmental effects, evaluating the threat, and determining the threat course of action.

UAS are small, maneuverable, and quiet, making them difficult to observe in flight. Environmental conditions, time of day, light levels, and observer alertness all impact the ability to detect a potential hostile UAS.

Experienced operators can exploit UAS characteristics to enhance their ability to remain undetected. Tactics include flying at low levels, using terrain and urban environments to mask an approach, making false take-offs and approaches, using erratic flight profiles, and using multiple UAS to confuse and overwhelm observers.

The types of sensors and their placement determine the unit's detection capability. Factors such as threat UAS types, terrain, weather, and the number of available assets impact how best to place and employ sensors.

Various sensor capabilities outside of visual (observer) could include RADAR, radio frequency, audible, and optical devices. The goal is to form an integrated sensor network that includes various sensor types.

2) Information Collection

Information collection is adjusted to include threat UAS information requirements developed during IPB. Analysts identify areas and times where the threat is most likely to employ UASs and task information collection assets to answer priority intelligence requirements. Air guards are responsible for spotting aerial threats within proximity to the unit's location and to provide early warning by alerting the unit of air threats.

Air guards should have the ability to conduct operations under all conditions. They should be equipped with the necessary optical gear to perform search and scan techniques to reduce the enemy's ability to evade detection.

The air guard checklist includes understanding on types and characteristics of threat UAS, understanding of current UAS trends, specific data on local air threats and named areas of interest, detection equipment, secure radio operations and frequencies to send out early warning, and unit call signs to request support.

3) Targeting

Effective targeting of threat UASs builds on the knowledge gained during IPB and execution of information collection activities. Units align delivery assets to provide lethal and nonlethal means to attack UASs. Identification is the process of determining the friendly or hostile characteristics of an unknown detected contact. The employment of Counter-UAS (C-UAS) capabilities requires early identification of UAS to maximize engagement times and avoid fratricide.

There are two methods of identification, procedural and positive. Positive identification is an identification derived from observation and analysis of target characteristics including visual recognition, electronic support systems, non-cooperative target recognition techniques, identification friend or fore systems, or other physics-based identification techniques.

The decision to engage is based on the severity of the threat versus the potential impact of the unit's effectiveness and the area of engagement (urban versus rural). Physical methods engage with and either destroy or damage the device so that it is not operational. Nonphysical methods defeat the device by disrupting, blocking, or controlling the signal between the UAV's optical, flight control, and ground control station.

Defeat techniques begin once airspace deconfliction and target engagement authority has been passed down to the tactical level. To confirm the identity of the sUAS and prevent fratricide multiple processes and procedures are used

4) Joint Considerations

Countering UASs is a joint responsibility, with U.S. Air Force, Navy, and Marine Corps aviation assets assisting against larger UAS groups through air interdiction. Elevated sensors and Army assets like the AN/APG-78 Longbow fire control radar on the Apache attack can also assist in detecting threat UAS

F. Example C-UAS Equipment'

It provides detailed information on the detection, identification, decision-making, and defeat of Unmanned Aerial Systems (UAS). It discusses various techniques and equipment used in these processes, including the BLA CHATRI 2, DRONE BUSTER, MODI, and SMART SHOOTER.

- **Detection:** UAS are small, maneuverable, and quiet, making them difficult to observe in flight. Detection can be influenced by environmental conditions, time of day, light levels, weather, and observer alertness. It emphasizes the importance of sensor placement and the use of an integrated sensor network.
- **Identification:** The document discusses the importance of identifying the friendly or hostile characteristics of a detected UAS. Accurate identification allows leaders to make engagement decisions and enhances situational awareness. Identification of a UAS should lead to a specific name or category or the exact make and model of the UAS.
- **Decision-making:** The document discusses the decision-making process in engaging a UAS. This includes deciding whether there is a need to engage and, if so, the methods used to lessen or eliminate the threat posed by a UAS. These methods include physical and nonphysical methods.
- **Defeat:** The document discusses various techniques for defeating a UAS. These include physical methods such as explosive munitions, small arms, projectiles, entanglement, directed energy, and capture, as well as nonphysical methods such as radio frequency jamming, GPS jamming, GPS spoofing, dazzling, and position, navigation, and timing (PNT) jamming.

The Bal Chatri 2 is a system designed for passive detection of radio frequencies, primarily used for identifying potential threat Unmanned Aerial Systems (UASs). It utilizes a software-defined radio frequency detection system specifically for detecting and identifying drones. The system can be adjusted for personal wear or for use in a small, stationary location.

Bal Chatri is a drone detection system that operates passively on radio frequencies. Key specifications of this system include a detection range of 3-5 kilometers, a power source that can either be a PRC-148 battery or a plug-in, a battery life of 4 hours, and a weight of 2.5 lbs.

The Drone Buster is a handheld, battery-powered device designed to counteract threats from Unmanned Aerial Systems (UASs). It is specifically engineered to neutralize Group 1 and 2 UASs. The device takes advantage of vulnerabilities in commercial drone communication protocols, allowing the operator to jam the control signal and trigger the drone's pre-set "lost signal" procedures.

The Drone Buster operates on a line-of-sight basis, necessitating the operator to keep the target in view throughout the engagement. If the line of sight is lost during the engagement, the threat may regain control of the UAV. The device is designed to disrupt both remote-controlled and GPS-guided UASs. Key specifications for the Drone Buster include:

- Range: 400m
- Power source: 1x BB2847 rechargeable battery
- Battery life:
 - **Continuous jamming:** approx 1 hour
 - **Continuous detection:** approx 4-6 hours
 - **Complete battery discharge:** approx 10 days

The Modi is a portable electronic warfare system designed for dismounted use. It offers the ability to detect and neutralize threats, with a particular focus on unmanned aerial systems (UASs). The system can function independently or be enhanced with a mounted power amplifier for use in fixed or mounted configurations and can be dismounted as needed. It operates within a temperature range of -4 to 140 degrees Fahrenheit. Key specifications of the Modi system include:

- **Operational range:** 400 meters.
- **Power source:** Three BB2590 batteries.
- **Battery life:** Not specified.
- **Weight:** 40.25 pounds when dismounted and packed.

Smart Shooter is a sight attachment for individual weapon systems, designed to counter Unmanned Aircraft System (UAS) threats. It can be fitted onto any rail of a weapon system and is compatible with existing military rifles. The Smart Shooter only allows the weapon to fire when the sight is correctly aligned with the target, including accounting for the necessary "lead" for moving targets. Key specifications of this system include a range of 120 meters, a power source of a rechargeable smart lithium-ion battery, a battery life of 72 hours or up to 3,600 assisted shots, and a weight of 2 pounds and 1 ounce

Read more: [Boosty](#) | [Sponsr](#) | [TG](#)



SNARKY SECURITY

Read more: [Boosty](#) | [Sponsr](#) | [TG](#)



SNARKY SECURITY