Artificial Intelligence Based Cyber Threats

Table of Content

Acknowledgement

Learning is not all about writing, taking notes or memorizing theories in our brains.

Specially when it comes to Cyber Security it is all about practicing and applying theories in real life.

Introduction to Cyber Security is a module which contains all necessary theoretical and practical knowledge about Cyber world. This assignment incorporates how Artificial intelligence outcome with Cyber Security and Cyber threats.

My heartiest gratitude to Lecturer Mr. Amila Senerathne and Lecturer Mr. Deemantha for the guiding through the theories and the assignments in the Introduction Cyber Security module while leading us through all the difficult situations.

Abstract

As we live in a digitally evolving world new technologies establish time to time. In this era, most overrated topic is Artificial Intelligence (AI). Evolution in AI technology changes almost everything, every industry in this digital world.

Cybersecurity is only one of the many domains where AI offers benefits and applications. AI and machine learning can assist in keeping up with hackers, automating threat detection, and responding more efficiently than traditional software-driven or manual procedures in today's world of quickly developing cyberattacks and rapidly multiplying gadgets.

Throughout this report we are going to discus how AI affect and change the cyber security industry. In this report we are about to discuss Artificial intelligence, Cyber threats, how AI affect development of cyber security, how AI support cyber threat field and how to avoid cyber threat topics in details.

Establishment of the Topic

Technology evolve day by day in various different ways today’s world. Most of our day today life all in-cooperated with digital world. So, when things getting digital, protection and security are getting complex. When it comes to security of digital assets Cyber Security comes in first place. Protecting personal data, sensitive data, basically everything in cyber space protected with coverage of cyber security. As technology move forward in modern day latest technology is Artificial Intelligence. Let’s define two major topics in the report individually which are Artificial Intelligence, Cyber Security and Cyber Threats.

- **Artificial Intelligence**

  Recently developed technology in modern times is Artificial Intelligence. The replication of human intelligence functions by machines, particularly computer systems, is known as artificial intelligence. Expert systems, natural language processing, speech recognition, and machine vision are some examples of specific AI applications. There are two types of AI, Narrow AI and General AI. Narrow AI can perform single task while General AI can achieve several tasks at once.

- **Cyber Threats**

  Threats to cybersecurity are actions taken by someone with malicious intent in order to steal data, harm computing systems, or disrupt them. We go into greater depth about each of these categories below. Common categories of cyber threats include malware, social engineering, man-in-the-middle (MitM) attacks, denial of service (DoS), and injection assaults.

  Cyber risks can come from a wide range of sources, including adversarial nation states and terrorist organizations, lone hackers, and legitimate users like workers or contractors who use their rights for bad purposes.

Introduction

Attackers constantly changing their strategy and improving in various different ways day by day. Attack strategies which are combined with AI-driven techniques are called AI-based cyber-attacks. As we talk in the establishment Artificial Intelligence (AI) overcome almost everything in todays world. It changes manual processes to automated processes with smart technology. For an example in cybersecurity field AI technology can filter through immense amount of data and find vulnerabilities, abnormal behaviors and much more with a blink of second.

Most of the time human eye focus of benefits of AI, less attention given to impact of cyber threats driven by AI. AI-based cyber-attacks can cause higher damages and losses rather than human-based cyber-attacks in general. Because AI-Based attacks are combined with modern technologies, developed strategies and much more advanced tools. Preventing such an AI-based cyber-attack is more challenging and more complex due to the technology and strategy. AI based cyber-attacks are capable of attacking more advanced systems rather which are not capable of attacking manually and cause greater impact as a result. For an example, modern systems such as cyber-physical systems (CPS) which are intelligent computer systems controlled by computer-based algorithms. CPS are similar to Internet of Things (IOT) and closely attached to concepts like robotics and sensor networks. Expert systems like above are still vulnerable to attacks. In order to attack such systems attack should be capable of engaging with high damage, well organized and developed with high technology. Automated systems like CPS can cause serious amount of damage with even a single small part of system collapse. When single part of system collapse, whole systems will be collapsed. Because automated systems are connected to one to each other.

Even these attacks began before many years ago, till today researchers have not summarized enough the field of AI-based cyber- attacks to prevent or study such attacks. Due to the wide area coverage of the field and rapidly involving technology summarizing and researching such a field is not an easy task.

History of AI-Based cyber attacks

The history of AI-based cyber-attacks is a complicated trip through the ever-changing realm of cybersecurity threats. With its ability to learn, adapt, and automate, artificial intelligence has become a double-edged weapon in the digital arena. While artificial intelligence has substantially improved defensive measures, it has also enabled hostile actors to develop more sophisticated, evasive, and damaging cyber-attacks.

Early use of AI in cyber activities

The use of artificial intelligence (AI) in cyber assaults dates back to the early days of computing, when rudimentary scripts and algorithms were used to automate hostile acts. These early attempts, albeit crude, provided the groundwork for today's more sophisticated AI-driven attacks. The "ILOVEYOU" worm from the year 2000 was a remarkable early example. Although it did not use AI directly, it proved the power of automation and social engineering in the spread of malware.

Machine learning and cyber-attacks

Machine learning (ML) has added a new dimension to AI-based cyber threats. Machine learning algorithms automate vulnerability finding and exploitation while also changing methods based on the target's defenses. The Mirai botnet showcased the power of machine learning in cyber-attacks in 2016. This botnet took use of unsecured Internet of Things (IoT) devices, resulting in the formation of a huge network of hacked devices that interrupted key internet services. The malware that powered the Mirai botnet included machine learning capabilities, allowing it to more effectively discover and infect susceptible IoT devices.

Advanced Persistent Threats (APT)

The development of Advanced Persistent Threats (APTs) in the mid-2000s was characterized by long-term, clandestine cyber-attacks, typically sponsored by nation-states. AI was critical in the advancement of APTs, allowing threat actors to alter their methods in real-time to escape detection. APTs used artificial intelligence to conduct advanced reconnaissance, find weaknesses, and create highly targeted phishing emails. As AI was utilized to analyze victims' online behavior and interests, these attacks became considerably more difficult to identify.

AI Enhanced Malware Infection

Artificial intelligence-enhanced malware has emerged in recent years. DeepLocker, for example, is a proof-of-concept malware that employs AI to conceal harmful payloads within innocent files which we are going to take a look in depth in later in this article. It goes undetectable by standard antivirus software and only acts when certain AI-determined parameters are satisfied. Furthermore, AI-generated deepfake audio and video are increasingly being used in phishing assaults. Cybercriminals are capable of creating highly convincing voice and video messages that impersonate trustworthy persons within organizations, resulting in unauthorized access or data leaks.

The history of AI-powered cyber-attacks shows the ever-changing nature of cybersecurity threats. The security community has a big issue as AI serves as both an enabler of cyber assaults and a defense mechanism. Staying ahead of these dangers necessitates not only technology developments, but also a thorough grasp of cybercriminals' techniques and strategies in this AI-driven era.

These are the some of AI-based cyber-attacks in real world reported in last few years.

- **DeepLocker Malware attack in June 2022**

Description - DeepLocker, a powerful AI-based malware, was used in a cyber-attack against a global financial institution. DeepLocker is notable for its ability to remain dormant until certain conditions are met, making detection and analysis difficult.

Incident - When the virus concealed in a seemingly harmless PDF document was run on a worker's PC, the attack was discovered. DeepLocker had been created to take advantage of the financial institution's particular security mechanisms, and it would only operate once it had identified the employee's login information and gained access to the company network.

Once triggered, DeepLocker operated covertly, permitting unauthorized access to the institution's networks and leaking private financial information. The source of the attack was identified as a phishing email with AI-generated content that got past standard email filters.

Action Taken - After the attack institution managed to swift the affected system offline. They performed an in-depth analysis of its security architecture, put in place AI-driven threat detection systems, and updated staff cybersecurity training to recognize ever-more-detailed phishing attempts. The current AI algorithms have also been improved to recognize possible AI-based threats.

- Spear Phishing Campaign in October 2021

Description - In order to compromise senior executives and obtain unauthorized access to crucial corporate resources, a well-known technology company was the subject of a targeted spear-phishing effort using AI-generated deepfake audio communications.

Incident - Key executives within the organization received incredibly convincing audio communications prior to the attack. These mails asked for access to private company information and systems while pretending to be from reliable colleagues. The voice recognition algorithms were tricked by the AI-generated deepfake audio, which was also convincing to the recipients.

Giving the attackers access allowed them to steal vital information and sensitive intellectual property, including the source code for proprietary software. This compromise was discovered after a top executive alerted the internal security team to the unexpected request.

Action taken - Technology company removed the unauthorized access and initiated an inspection about the security breach. To identify and stop future AI-generated deepfake attacks, the incident response team integrated AI-driven voice analysis technologies into their security infrastructure.

- **Mirai Botnet Re-emergence in May 2020**

Description - The Mirai Botnet is a well-known AI-enhanced cyber threat which targeting vulnerabilities in Internet of Things (IOT) devices deploying distributed Denial of Service (DDoS) attacks against critical infrastructure.

Incident - The attackers searched for and compromised unpatched and inadequately secured IoT devices across a range of businesses using the machine learning-capable Mirai botnet. Once infected, these devices joined the botnet and created a sizable network of zombie devices.

Critical infrastructure facilities were the target of a sizable DDoS attack as a result of the attack, which resulted in interruptions and outages. Power grids, water treatment facilities, and communication networks were among the targets.

Action taken - The impacted organizations worked together with law enforcement and security specialists to reduce the threat in the wake of the incident. In order to detect and prevent malicious traffic, they introduced AI-driven anomaly detection systems, improved network security, and delivered updates for susceptible IoT devices.

The incident highlighted the significance of timely IoT device patching and the potential for AI-enhanced malware to quickly grow and adapt.

Existing AI-based Cyber Attacks

Rapidly evolving technologies are expanding the cyber security field. It can open gates to development of the cyber security as well as new gateways for attackers to get advantage of. Which can be impact both physical and digital cyberspace. As a consequence of AI, fuzzing techniques can be used by criminals to develop advanced malware that constantly updates itself with new exploits and infects millions of susceptible machines. The use of AI technologies for malicious purposes, including various assault objectives that might seriously harm the environment and the human population, has been studied in numerous ways. Numerous instances already in existence highlight the necessity to understand AI as an offensive weapon. Let’s cover up some of the existing AI-based and AI-developed cyber attacks in real world as follows;

1. Next generation malware
    i. Smart malware
    ii. DeepLocker
    iii. ChaosGPT

2. Spyware

3. Password based attacks
    i. Password brute-force attack
    ii. PassGAN

4. Social bots

5. AI Tools

1. Next generation malware

Identifying and attacking possible targets could harm millions of devices and systems without being identified by malware detection tools. People become infected with malware in a typical attack when sophisticated malware use encryption to conceal the attack payload and obfuscation or a sandbox to escape detection by antivirus systems. Furthermore, when attackers use malware to infiltrate targets, they must disguise the trigger conditions as a command that is either incorporated in the virus or executed remotely. Malware, on the other hand, may be collected and reverse-engineered to determine how it got into the malicious condition. An earlier attack strategy that used a low-cost modular methodology to disguise harmful payloads in genuine neural network models and conduct neural Trojan attacks was proposed.

i. Smart malware

What is Smart malware - Such fine-grained targeted intrusions are no longer the stuff of dark hacker films, as security researchers from IBM revealed at the recent Black Hat USA security conference in Las Vegas. AI makes devices to understand surrounding environment better. For an example smartphone camera can scan your face and unlock your phone with face ID, security cameras can identify unauthorized people and warn you, voice activated devices such as Amazon Alexa, Google assistant, IOS Siri can recognize your voice and follow commands by itself. But hackers can use the same AI technology to create smart malware capable of preying on its targets and detecting them among millions of users. Attackers can will typically attempt to deploy malware via smishing, or SMS phishing. In other words, they will use the SMS service to distribute a malicious link or software. Just by clicking the malicious link malware can affects your devices through it and get access to your devices. Attackers can deploy one single malware to as many devices as they want easily. This makes Android, which is much more permissive when it comes to third-party software installation, a slightly larger target. Installing third party apps in IOS are more difficult than Android devices.

How to prevent – In order to prevent such smart malware infection, you should beware of these kinds of attacks. Prevent opening links received from anonymous emails, users, numbers.

Always keep update to the latest version of the software you use. Update of an application or software are more secure than older versions.

You can install third party antivirus applications like avast, McAfee, Norton, Surfshark etc.   Refer ‘Top 10 Antivirus Software of 2023’. [1]

ii. DeepLocker

What is DeepLocker - IBM researchers are attempting to increase awareness about the impending arrival of AI-powered risks. To that purpose, they've developed an entirely new breed of malware to provide insights about how to reduce risks and implement appropriate remedies. DeepLocker was featured at Black Hat USA 2018, a hacker conference that offers security consultancy, training, and briefings to hackers, organizations, and government agencies around the world.

By training a neural network to recognize the victim's face, researchers Marc Ph. Stoecklin, Jiyong Jang, and Dhilung Kirat demonstrated how a piece of malware may be selectively targeted at one individual and not others. When the AI locates its target, it activates the unlock key, which de-obfuscates and executes the concealed malware. They employed WannaCry, the infamous virus that made headlines last year, for this proof of concept.

What distinguishes DeepLocker is the use of AI, which makes the 'trigger conditions' to unlock the attack nearly impossible to reverse engineer." If the intended target is reached, the malicious payload will be unlocked. This is accomplished through the use of a deep neural network (DNN) AI model.

The AI model has been trained to act normally unless it is given a specific input: trigger circumstances identifying specific victims. The neural network generates the "key" required to launch the assault. DeepLocker can identify its target using a variety of variables, including visual, audio, geolocation, and system-level information. Because it is nearly impossible to exhaustively enumerate all possible trigger conditions for the AI model, this method would make it extremely difficult for malware analysts to reverse engineer the neural network and recover mission-critical secrets, such as the attack payload and target specifics, Stoecklin explains.

How to prevent – Defense have not yet been implemented, although Dhilung Kirat recommended various methods, such as limiting sensor access or using cyber deception to misdirect and deactivate malware for future study.

iii. ChaosGPT

What is ChaosGPT - We are all aware of how OpenAI's ChatGPT has transformed the artificial intelligence arena. Since its inception, various companies have stepped up to introduce their AI-powered chatbots. From Google's Bard to ChatSonic API, these products are transforming this field on a daily basis. As several chatbots compete for a spot in this AI world, a new entrant, ChaosGPT, is quickly becoming the talk of the town. ChaosGPT, well known for its distinctive moniker and 'evil' tweets, is apparently becoming well-known for informing the globe about its strategy for mankind and thoughts of world dominance.

According to anonymous creators, this AI tool has five key goals;

1. Destroy Humanity
2. Conquer the world
3. Create more Chaos
4. Improve itself
5. Control humanity

ChaosGPT is proof of the value of community-driven development because it was developed and trained by a sizable multinational community of volunteers who collaborated to establish a cutting-edge language model. The project's goal was to democratize access to cutting-edge AI technologies in order to encourage experimentation and creativity.

Additionally, the authors of ChaosGPT wanted to create a language model that was more robust and less subject to prejudice than previous models. They made an effort to lessen the influence of preexisting biases in the training data in order to make the model more inclusive and representative of many opinions.

ChaosGPT - [2]

2. Spyware

What is a spyware - Spywares are mostly affect by the smartphones which has built in Virtual Assistances. Recent researches demonstrate how programs like built-in VAs in smartphones can be used as a backdoor by attackers to break into devices and obtain access to system resources and personal data. The authors suggested an attack framework that records activation using AI technology.

Determine the best time to initiate the attack by speaking covertly. This spyware's purpose is twofold:

(i) secretly creating activation phrases, and

(ii) transmitting harmful voice messages

Directives to mobile VAs, instructing them to carry out tasks at the most advantageous moment to strike, hacking the devices while avoiding detection by users and antivirus software.

In the attacking part, by simulating the legitimate user's voice, the attacker can create hostile voice commands. The intelligent stealthy module IED can determine the best timing to conduct the attack once the attacker has the activation voice. Hence, this is an illustration of a clever method of adjusting to the environment of the target and launching strikes by triggering an assault only in specific circumstances.

How to prevent - Disabling unwanted access to the device’s features such as microphone in the unwanted applications.

3. Password based attacks

Password based attacks are well known attack type in cyber space. One of various techniques is used by an attacker to attempt to steal or break passwords in order to get access to your personal or organizational data.

A study by Privileged Access Management experts Centrify found that 74% of data breaches involved assaults on privileged accounts within the organizations. Hackers take advantage of the fact that many of us don't give password security any thought.

To get around single-factor authentication, hackers employ a variety of password-based attack techniques. You should be aware of how these techniques operate and what you can do to thwart them in order to strengthen your account defenses. A list of password-based attacks that you should be aware of is provided below, along with advice on how to prevent them.

Next-generation password-based attacks, which are more effective and intelligent at breaking passwords, are made possible by AI. The first case study demonstrates how AI can be taught to come up with new possible passwords by self-learning and building the attacking dictionary in a cleverer manner based on patterns acquired from earlier passwords. A more knowledgeable and enhanced dictionary is the result.

i. Next-level password brute-force attack

The next generation of password brute-force attacks uses artificial intelligence (AI) to modify the way the attacker dictionary is built using self-learning techniques. Old passwords will be analyzed for patterns in order to automatically create new candidate passwords. Password execution patterns from the past can help future mutations have a higher chance of being successfully decoded.

Traditional password brute-force attacks rely on a well-prepared dictionary of possible passwords, a list of likely passwords that includes previous passwords, or random and significant words to compare against user passwords. However, the creation and upkeep of the dictionary is directly related to how quickly and effectively passwords may be cracked. [3]

How to prevent - Prevent such a password attack you can use multi-factor authentications for your accounts for better security. Also, when creating passwords use different kind of mixed characters, because strong passwords are difficult to crack.

ii. PassGAN attack

PassGAN is a cutting-edge method for automatically producing strong password guesses. A GAN that has been correctly instructed launches the attack.

In order to discover highly likely candidate passwords, it is necessary to autonomously extract password attributes and structures from the distribution learned from prior password breaches.

Brute force and dictionary rule-based methods are the foundation of conventional password guessing strategies. But, only particular parts of the password space that fit with the existing human-generated rules based on user intuition can be captured using these conventional techniques.

How to prevent - Evaluating password policies will help password-based authentication to be more secure or you can use two factor authentication method for secure from the user side of accounts.

4. Social Bots

Let’s define word ‘bot’ first. A bot, which is short for "robot," is an automated program that is configured to carry out specific tasks on a regular basis or as needed. The bot completes this task without human interaction. According to the circumstances, it "decides" the actions to do after analyzing the surrounding environment.

On social networks, social bots act as real users. They are regarded as fake accounts if they do not disclose that they are automated. Many users are duped because they believe they are speaking with someone after reading plausible material on a profile. In the interest of its operators, this kind of bot is frequently employed to promote opinions on social networks or to incite debate.

An automated program called a "social bot" imitates human behavior on social media platforms. Social bots engage in conversations on Facebook or Twitter and mimic human behavior. They disseminate content on a specific subject on social media, primarily with the aim of swaying people's attitudes. [4]

Examples for social bots in recent years

- **Brexit vote**: The majority of British citizens chose to leave the EU in June 2016. There had been contentious conversations on social media prior to this, and it was reported that numerous social bots had also been involved. According to The Independent, social bots were crucial to strategy, particularly when it came to the "leave" vote. [5]

- **US president election**: Donald Trump won the election to become the 58th President of the United States in November 2016. There was a ton of information available on the size of the impact social bots had on his razor-thin victory. Oxford University claims that pro-Trump automated bots outnumbered pro-Clinton communications. It appears that a bot sent every third pro-Trump tweet. Additionally, a false news story suggesting the Pope had endorsed Trump for president was circulated about a million times, including by social media bots. However, it was also noted that pro-Clinton social bots were being used. [6]

- **German parliamentary election**: Many people were concerned that social bots could sway the 2017 federal elections in light of what occurred in the UK the year before. Even though social bots are permitted in Germany, all participating parties came out against their usage throughout the election campaign. Fortunately, there wasn't much interference from social media bots. However, their reach was also lesser due to the fact that there aren't as many Twitter users in Germany, which is why there aren't as many bots utilized there. [7]

There are three major categories that can filter social bots,

1. The overloader
2. The trendsetter
3. The auto troll

5. AI Tools

Ai powered hacking tools are more effective when attacking rather than manual hacking tools. These AI hacking tools deliver more thriving attacking probability after deploying.

Malicious actors now have access to strong tools that can automate their attacks with the rise of AI-powered hacking tools. Examples from more recent times include Wolf GPT and XXXGPT. Both of these tools build malicious code using generative models, making them particularly difficult for organizations to defend against.

XXXGPT - This uses a Large Language Models (LLM) to generate malware sets. It can generate powerful malwares which are harder to detect. Additionally, the program contains an obfuscation capability that aids in disguising the code produced by the model, making prevention and detection much more difficult.

Wolf GPT - Another harmful AI-powered hacking tool with a different end objective in mind, Wolf GPT gives the hacker anonymity within particular attack routes. By using huge amounts of already-existing malicious software, this kind of AI system may produce malware that looks realistic. Additionally, it enables attackers to launch sophisticated phishing attacks. Wolf GPT features an encryption function similar to XXXGPT, which makes it challenging for cybersecurity teams to find and stop incoming attacks.

Future of AI driven Cyber Security

Artificial intelligence (AI) in cybersecurity is expected to play a transformational role in dealing with the constantly changing landscape of cyber threats. Observe following key trends and developments in AI based cyber security.

- AI is getting more and better at spotting and preventing sophisticated cyber-attacks. Massive volumes of data can be analyzed by machine learning algorithms to find abnormalities and patterns that human analysts might miss. This is especially important as sophisticated cyberattacks increase.

- AI-driven systems may observe and take notes on how users and gadgets behave on a network. This makes it possible to spot behavioral differences from the usual that can point to security breaches.

- **Quantum computing** - The advent of quantum computing presents both a threat and an opportunity in cybersecurity. Quantum computers can potentially break current encryption methods, but AI can be used to develop quantum-resistant encryption algorithms, thereby maintaining data security.

In conclusion, the use of AI in cybersecurity has a bright future in terms of enhancing defenses against online attacks. In terms of ethics, laws, and the growing nature of cyberattacks, it also poses fresh difficulties. To keep ahead of the continuously evolving threat landscape, organizations will need to invest in AI-driven security solutions and modify their policies.

Cybersecurity Best Practices to Avoid Attackers

As technology evolves cyber security teams, organizations, IT departments all other IT based peoples, teams, organizations should aware about these latest tools and technologies. Implementing the appropriate security measures is crucial for organizations if they want to defend themselves and keep up with criminals.

1. Use Multi-Factor Authentication

A second layer of authentication can be added to help prevent unauthorized access. In order to get access, users must first submit two or more different kinds of identification, such as a password and a one-time code sent via text message or email. Even if threat actors are successful in guessing the password, it will be considerably tougher for them to get access as a result.

2. Use Strong Passwords

Malicious actors can readily access accounts and systems thanks to weak passwords, which are simple for them to guess. In order to avoid this, businesses should never reuse passwords across different accounts or services and instead use strong passwords of at least 8 characters made up of letters, digits, and symbols.

A password manager like LastPass or 1Password, which can create secure passwords automatically and store them securely in an encrypted database, is also advised for usage by organizations. Or you can easily use google suggested password for logins.

3. Monitor Network Traffic

Organizations should keep a close eye on network traffic for any odd activity that would point to a breach, such as uncommon logins, huge file transfers, or unencrypted data exchanges. IT staff should look into any suspicious behavior right away and take action to remedy any potential problems as soon as possible to prevent future harm to the network or systems.

4. Update devices and software

Every device in an organization needs to be running the most recent operating system version with all security updates installed as soon as they are available. This will assist in repairing any holes that attackers might use to access networks or systems.

5. Use VPN’s

A VPN is an important tool for maintaining your online safety. It improves your overall internet experience while enhancing your security and privacy. Let's examine a VPN's advantages and disadvantages as well as its value.

VPN can secure connection in the internet while securing your data and privacy. Also, VPN can avoid getting hacked your device. Because VPN hide your real location and real IP address similar to proxy servers.

Conclusion

AI is quickly becoming a necessary tool for improving the effectiveness of IT security teams. AI provides the critical analysis and threat identification that security professionals need to reduce breach risk and improve security posture because humans can no longer scale to adequately secure an enterprise-level attack surface.

Additionally, AI can direct incident response, find and priorities hazards, and detect malware assaults before they happen. Therefore, despite any potential drawbacks, AI will advance cybersecurity and assist organizations in developing stronger security postures.

References

Webpages

[1] "Best Antivirus Programs," [Online]. Available: https://www.pcmag.com/picks/the-best-antivirus-protection.

[2] "chaosGPT," [Online]. Available: https://poe.com/universal_link_page?handle=ChaosGPT.

[3] "AI-based Brute Force Attack," [Online]. Available: https://aisel.aisnet.org/mwais2018/39/.

[4] "www.ionos.com," [Online]. Available: https://www.ionos.com/digitalguide/online-marketing/social-media/social-bots/.

[5] "www.independent.co.uk," [Online]. Available: https://www.independent.co.uk/tech/brexit-twitter-bots-pro-leave-eu-referendum-result-oxford-university-study-a7800786.html.

[6] "www.nytimes.com," [Online]. Available: https://www.nytimes.com/2016/11/18/technology/automated-pro-trump-bots-overwhelmed-pro-clinton-messages-researchers-say.html.

[7] "www.reuters.com," [Online]. Available: https://www.reuters.com/article/us-germany-election-fake/german-election-campaign-largely-unaffected-by-fake-news-or-bots-idUSKCN1BX258.