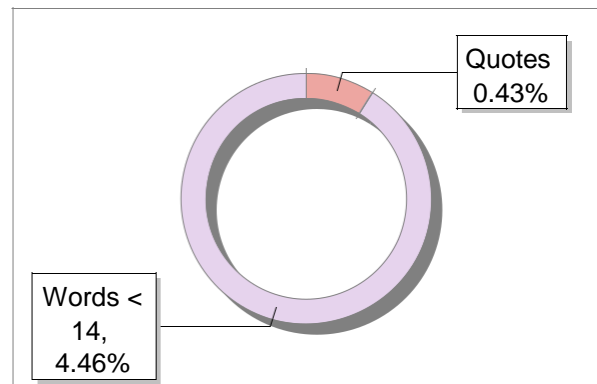
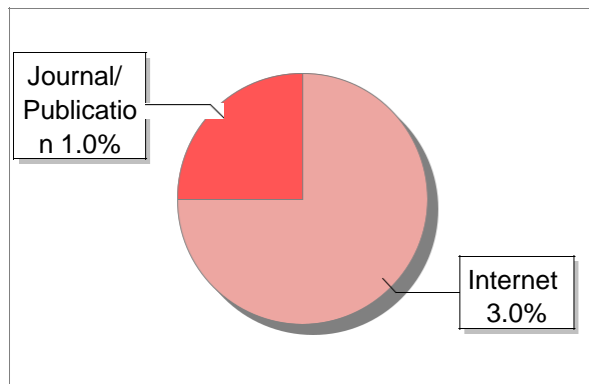


Submission Information

Author Name	Prajeeth L, Shrihari VP, Tejas M Bharadwaj, Yashas N
Title	Wireless Communication and Security Issues for Cyber– Physical Systems and the Internet-of-Things
Paper/Submission ID	1291893
Submitted by	hod.lib@jyothyit.ac.in
Submission Date	2023-12-29 14:44:29
Total Pages	30
Document type	Research Paper

Result Information

Similarity **4 %**

Exclude Information

Quotes	Excluded
References/Bibliography	Excluded
Sources: Less than 14 Words %	Excluded
Excluded Source	0 %
Excluded Phrases	Not Excluded

Database Selection

Language	English
Student Papers	Yes
Journals & publishers	Yes
Internet or Web	Yes
Institution Repository	Yes

A Unique QR Code use to View/Download/Share Pdf File





DrillBit Similarity Report

4

SIMILARITY %

5

MATCHED SOURCES

A

GRADE

A-Satisfactory (0-10%)

B-Upgrade (11-40%)

C-Poor (41-60%)

D-Unacceptable (61-100%)

LOCATION	MATCHED DOMAIN	%	SOURCE TYPE
1	journalofbigdata.springeropen.com	3	Internet Data
2	www.dx.doi.org	<1	Publication
3	A data analytic framework for physical fatigue management using wearable sensors by Sedigh-2020	<1	Publication
4	www.slideshare.net	<1	Internet Data
5	Frontiers of Strategic Management Research Playing Football in a Soccer Field by Michael-2008	<1	Publication

RESEARCH PAPER SUMMARY
TEAM NO. 10 - FALCONS

BIBLIOGRAPHIC TEXT

TITLE- Wireless Communication and Security Issues for Cyber– Physical Systems and the Internet-of-Things -1

By Andreas Burg

ABSTRACT: Wireless sensors and actuators connected through the Internet of Things (IoT) play a crucial role in advanced cyber-physical systems (CPSs). In these complex systems, communication links must meet strict requirements for throughput, latency, and range, all while adhering to energy constraints and ensuring high security levels. This paper provides a concise overview of wireless communication principles relevant to the connectivity needs of IoT and CPS. It reviews key wireless communication standards and highlights security issues, emphasising the disparity between security features in CPS and IoT communication standards and their actual vulnerabilities. The discussion underscores the importance of a comprehensive examination of security issues across all protocol layers, encompassing logical and physical layer security.

INTRODUCTION: Cyber-physical systems (CPSs) are intricate distributed systems comprising sensors, actuators, and computing nodes connected through diverse communication means. CPSs autonomously perceive changes in the physical environment, analyse their impacts, and make intelligent decisions to control physical objects. The merging of sensors, computing nodes, and actuators forms a feedback loop, enabling CPSs to achieve specific objectives autonomously or with human-in-the-loop support. CPSs, also known as

operational technology systems, have become intertwined with the Internet of Things (IoT) due to the widespread use of IP-enabled devices and wireless connectivity.

Connectivity in CPSs, spanning local to global scales, relies heavily on wireless communication, driven by factors such as reduced installation costs and flexibility. The layered architecture of CPS/IoT includes a sensing/actuation layer supported by a transport/communication layer and a system application layer with computation nodes for data analytics and decision-making. Despite the advantages of wireless connectivity, challenges exist in terms of communication performance, power consumption, and security.

This paper explores the myriad wireless communication systems and standards in CPSs and IoT, emphasising security considerations. It delves into communication technologies, properties, and security practices, addressing the challenges and requirements across different layers of the network stack. The focus is on the security of CPSs and IoT systems, excluding physical side-channel attacks, with a comprehensive discussion of wireless communication standards and security issues in subsequent sections.

SECURITY IN WIRELESS COMMUNICATION FOR IoT AND CPSs: Security in wireless systems can be approached at different levels: classical measures at the MAC/DLL, network, transport, and application layers based on cryptographic principles, and physical layer security measures employing information-theoretic principles. Cyber-physical systems (CPSs) and IoT systems, interacting with physical processes, introduce their own layers like

the perception layer and computation layer. Wireless communication security faces challenges due to the layered protocol architecture and potential breaches in upper layers. Security incidents, especially in IoT, pose new threats, and attacks are evolving to impact applications directly.

Emerging threats highlight the need for a comprehensive security approach. A four-phased recommendation includes security policy design based on the CIA triad, consideration of secure networks with well-defined perimeters, careful selection of secure components, and ongoing security auditing supported by simulation and emulation.

CONCLUSION AND FUTURE WORKS: The diversity and heterogeneity of Cyber-Physical Systems (CPSs) and the Internet of Things (IoT) present challenges for wired and wireless communication systems. No single standard can meet all requirements, necessitating innovation. Key challenges include the growing number of connected nodes, increased wireless data conflicting with limited spectrum, latency concerns, and the need for energy autonomy in CPSs and IoT systems. Security is a major concern, with existing systems falling short of necessary precautions. Urgent research areas include cross-layer protocol validation, robust authentication mechanisms, tracking of promiscuous devices, analysis of side-channel information leakage, and policy design for secure CPS/IoT that avoids reliance on obscurity. Addressing these issues is crucial for the secure evolution of wireless communication in smart systems.

TITLE - Security Verification for Cyber-Physical Systems Using Model Checking- 2

By CHING-CHIEH CHAN, CHENG-ZEN YANG AND CHIN-FENG FAN

ABSTRACT: This paper presents a systematic method for enhancing the cyber security of Cyber-Physical Systems (CPS) with a focus on operational technology (OT). The approach utilises model checking with UPPAAL to identify vulnerabilities, considering potential security attacks as unsafe situations. The method systematically generates security constraints based on overall safety requirements at the OT level, which can be employed for run-time monitoring to detect security attacks. The proposal includes the addition of an Attack Module to simulate potential OT attacks within the normal system modelling. The verification results serve a dual purpose: identifying vulnerabilities for design improvements and suggesting additional security constraints.

INTRODUCTION: A Cyber-Physical System (CPS) integrates computing and physical components and is extensively utilised in critical sectors like aviation, construction, and energy. With the increasing prevalence of CPS, there is a growing concern about security threats, especially in safety-critical domains such as industrial control systems and the Internet of Things. Coordinated cyber-physical attacks (CCPA) have posed significant risks to national security, exemplified by incidents like the Stuxnet attack on Iran's nuclear facilities and Ukraine's power network disruption. This paper addresses the security challenges in CPS, particularly in operational technology (OT), emphasising the need for integrated safety and security measures.

The proposed security analysis treats unsafe situations as potential outcomes of security attacks and presents a systematic method to generate security constraints based on CPS safety constraints. Model checking with UPPAAL is employed for security verification, enabling a detailed exploration of various model combinations and human-computer interactions. The study introduces an Attack Module for simulating potential OT attacks within the CPS model, which encompasses software, hardware, and operator subsystems. The method contributes to the field by offering a systematic approach to generate OT-level security constraints, facilitating run-time monitoring, and suggesting improvements. Two case studies illustrate the application of the approach, covering safety restraint system generation, model construction, safety verification, and potential design enhancements.

In summary, this paper addresses the critical issue of CPS security, focusing on OT, and presents a systematic method leveraging model checking for enhanced security verification. The proposed approach integrates safety and security considerations, offering valuable insights for identifying vulnerabilities and suggesting additional security measures.

BACKGROUND AND RELATED WORK: In a 2019 survey by Positive Technologies, vulnerabilities in Cyber-Physical Systems (CPS) were found to shift focus from Human-Machine Interface (HMI)/Supervisor Control and Data Acquisition (SCADA)

components in 2017 to Industrial Control Systems (ICS) in 2018. Recent CPS security incidents indicate risks both within networks and dedicated facilities, with various attack methods employed. Another report in 2020 highlighted that 75% of 365 vulnerabilities in ICS systems pose high or serious risks. The growing importance of CPS security underscores the need for effective protection measures.

Several model verification tools exist, such as SpaceEx, UPPAAL, and KeYmaera. The study emphasises the use of UPPAAL for verifying the correlation between system running paths and state changes. UPPAAL's simulation tool facilitates detailed searches, exploring possible model combinations and human-computer interactions. The formal model checking tool provides essential functions like system editing, simulation, and verification. Its integration tool supports the development and verification of real-time systems, offering valuable insights for dealing with complex CPS applications.

The study identifies accidents resulting from human-machine interface errors, emphasising the importance of detecting or preventing these issues in advance to avoid major hazards. Examples include the 2003 Northeast blackout and aviation incidents like TransAsia Airways Flight 235 in 2015. The detection or prevention of potential problems with the system and the human-machine interface is crucial for averting or mitigating major hazards.

In related work, CPS has gained significance in critical infrastructures, and its application spans various sectors. The study classifies CPS into communication, computing and control, and monitoring and manipulation components, highlighting security concerns in their interaction. While many scholars focus on information security, few address both cyber and physical systems. A comparison with Akella's work shows that both methods provide modelling and formal verification for CPS security, with differences in their approaches and focus.

CONCLUSION AND SUMMARY: Ensuring cyber security in Cyber-Physical Systems (CPS) is vital, and our approach focuses on preventing attacks in the design stage and detecting them at runtime through constraint monitoring. We present a systematic method for CPS security verification using UPPAAL model checking. Unlike many studies concentrating solely on IT attacks, we specifically address Operation Technology (OT) attacks. We introduce OT-level security constraints derived systematically from safety requirements and represented in UPPAAL queries. Both normal and attack models are developed, and model checking explores potential OT attacks. The results serve to augment security constraints and inform system redesign to enhance cyber security. Global invariants prove generally effective, but in carefully designed attacks, consistency checking between cyber and physical components may be essential. Rigorous recommendations include reverting critical CPS components to analog design to minimise attack surfaces. Future investigations will focus on completeness of constraint sets, automated constraint revision, and hybrid simulations combining UPPAAL with Ptolemy for accurate continuous behaviour modelling.

TITLE: Optimising Cyber Security Anomaly Detection Through Neural Networks: A Comprehensive Evaluation- 3

By Xavier A. Larriva-Novo, Mario Vega-Barbas, Víctor A. Villagrà, Mario Sanz Rodrigo

ABSTRACT: This research focuses on enhancing the efficiency of intrusion detection systems (IDS) through the optimal configuration of neural networks. The study categorises cybersecurity datasets into basic connection characteristics, content characteristics, and traffic statistical characteristics, proposing a novel approach to reduce multidimensionality. Two types of neural networks, multilayer and recurrent, are evaluated, considering various activation functions, optimization algorithms, and dataset groups. The UNSW-NB15 dataset serves as a benchmark for testing, and the results indicate that the proposed methodology achieves high accuracy.

INTRODUCTION: 1. Introduction: The study addresses the evolving challenges in cybersecurity by leveraging neural networks for intrusion detection. It introduces a novel categorization of dataset characteristics and explores the optimization of neural network configurations. Two main objectives are pursued: categorising datasets for efficient learning and determining the superior neural network architecture.

2. Neural Network Configurations: Fundamental concepts of artificial neural networks, including multilayer and recurrent architectures, are explored. Activation functions and optimization algorithms such as Adam and RMSProp are assessed. The focus is on minimising computational load while maximising accuracy.

3. Categorization of Cybersecurity Dataset: The research introduces a categorization methodology for the UNSW-NB15 dataset, considering basic connection characteristics, content characteristics, and traffic statistical characteristics. The novelty lies in reducing multidimensionality by grouping relevant features, improving algorithm efficiency.

4. Results and Analysis: Experiments reveal that the linear rectifier activation function, combined with the Adam optimizer and Z-score normalisation, yields optimal results. Multilayer neural networks consistently outperform recurrent networks, demonstrating that simpler architectures can achieve comparable accuracy.

5. Comparison with Related Works: A comparative analysis with existing research on the UNSW-NB15 dataset highlights the superior performance of the proposed methodology. The presented model, particularly with Group 1 characteristics, achieves higher accuracy compared to other approaches.

6. Conclusion and Future Directions: The study concludes that efficient intrusion detection is achievable through carefully configured neural networks. Future research directions include extending the methodology to larger datasets and refining performance metrics to capture diverse prediction types.

SUMMARY: This research contributes valuable insights into the optimization of neural network configurations for cybersecurity, emphasising simplicity, efficiency, and high accuracy in intrusion detection.

TITLE - Blockchain as a Cyber Defense: Opportunities, Applications, and Challenges - 4

By SUHYEON LEE, AND SEUNGJOO KIM

ABSTRACT: Cyber threats pose significant risks to national interests, leading nation-states to bolster their defence mechanisms through the emerging field of "cyber defence." This sector, vital for national security, demands robust security technologies. Blockchain, with its decentralised and secure nature, is gaining attention for its potential applications in cyber defence. This paper explores the opportunities, ongoing research, and national projects in integrating blockchain into cyber defence. Through a comprehensive survey of government documents, interviews, technical reports, and research papers from 2016 to 2021, our research aims to bridge the gap in understanding the role of blockchain in cyber defence. Our findings indicate active promotion of blockchain not only in research but also in government-led initiatives, highlighting its anticipated significant role. The paper concludes with suggestions for future research focusing on blockchain technology, evaluation, and surveys.

INTRODUCTION: In response to the escalating cyber threats confronting critical infrastructures, this paper delves into the pivotal role of blockchain in the realm of cyber defence. The exploration unfolds across three key dimensions:

1. Blockchain's Strategic Advantages in Cyber Defense: - Unveiling a spectrum of benefits such as heightened visibility, enhanced verifiability, resilience against single points of failure, and augmented auditability within the context of cyber defence.
2. Comprehensive Survey of Blockchain in the Cyber Defense Landscape: - A meticulous examination of over 40 blockchain projects, encompassing both research initiatives and government-led endeavours. This survey sheds light on the diverse applications of blockchain technology in fortifying cyber defence capabilities.
3. Navigating Challenges in Integrating Blockchain with Cyber Defense:- Delving into domain-specific challenges, including the intricacies of battlefield environments, the presence of air-gaps, and resource constraints. These challenges offer insights into the pragmatic aspects of deploying blockchain in the intricate landscape of cyber defence.

This research endeavour not only contributes a nuanced understanding of how blockchain fortifies cyber defence but also provides a roadmap for future research endeavours. The findings underscore the strategic advantages, diverse applications, and challenges associated with integrating blockchain technology into the critical domain of cyber defence.

BLOCKCHAIN TECHNOLOGY: This section provides a condensed overview of blockchain technology, tracing its origins from Bitcoin's inception in 2009. Blockchain, the foundational data structure of Bitcoin, facilitates trustless transactions by preventing double-spending. Transactions are recorded in blocks, each containing a set of data, and

linked to the previous block through a hash. Various cryptocurrencies, including Ethereum, Zcash, Ripple, and IOTA, adopt modified structures.

Key blockchain features include decentralised networks, Sybil control mechanisms, and categorization into public (permissionless), public permissioned, consortium, and private blockchains. The decentralised nature is maintained by mechanisms like Proof-of-Work (PoW), although alternative Sybil control methods like Proof-of-Stake (PoS) are utilised. Operationally, blockchains are classified as permissioned or permissionless, with Ethereum's introduction of smart contracts marking a significant advancement in the field.

ANALYSIS OF BLOCKCHAIN R&D TRENDS IN CYBER DEFENCE: This section explores trends in blockchain research and development, with a focus on government policy directions. Our survey system transparently outlines findings categorised by blockchain applications in supply chain, IoT, communication, identification & authentication, and data integrity services.

Supply Chain Management (SCM): Blockchain is notably effective in countering threats to SCM processes, ensuring data integrity and preventing counterfeit components. Projects, including those by the U.S. Department of Defense, enhance supply chain risk management through blockchain.

Internet of Things (IoT) Government initiatives, such as the Department of Homeland Security, explore blockchain solutions for IoT sensors in critical infrastructures. Blockchain enhances security, decentralises control, and provides reliable data for IoT applications, seen in projects related to drone swarm systems and unmanned aerial systems.

CONCLUDING REMARKS AND FUTURE RECOMMENDATIONS: This study delves into the application of blockchain technology in cyber defence, addressing the inevitability of cyber threats in military and social infrastructure. The decentralised nature of blockchain ensures data integrity and bolsters system reliability against cyber threats. Our exploration encompasses opportunities, applications, and challenges in blockchain for cyber defence. Key recommendations include enhancing the practicality of blockchain by overcoming technological limitations, obtaining more evaluation data specific to cyber defence conditions, and conducting large-scale surveys on government-led blockchain projects, acknowledging linguistic barriers and information disclosure policies as challenges in this endeavour.

TITLE - A Survey of Cybersecurity of Digital Manufacturing -5

By Priyanka Mahesh and Team

The article provides a comprehensive exploration of the cybersecurity landscape in digital manufacturing (DM). It discusses the evolution from traditional manufacturing to DM driven by advancements in sensors, artificial intelligence, robotics, and networking technologies, within the framework of Industry 4.0.

Key points covered include the digitalization of manufacturing, the integration of cyber and physical resources, and the role of computing infrastructure in DM. The authors emphasise the importance of secure cybersecurity measures to protect against internal and external threats, ranging from sabotage to intellectual property theft.

The article introduces the concept of a Hybrid Machine (HM) tool as an archetype for DM, highlighting vulnerabilities in cybersecurity. It also presents a detailed taxonomy of threats in DM, addressing attacks on various components such as CAD software, G-code, manufacturing machines, sensors, and controllers.

Counter measures, including watermarking, authentication, noise injection, and anomaly detection, are discussed to mitigate potential threats. The authors analyse case studies, emphasising the need for robust defences against attack vectors like manipulation of instructions, replay attacks, feedback loop compromises, side-channel attacks, and indirect sabotage.

Furthermore, the article reviews existing cybersecurity taxonomies, highlighting the expanding scope of cyber-physical systems in manufacturing. It discusses specific taxonomies proposed by various researchers to address security concerns in areas such as hardware Trojans, supply chain attacks, and attacks on additive manufacturing.

The conclusion underscores the significance of ongoing research and development of countermeasures, recognizing the evolving nature of cybersecurity challenges in digital manufacturing systems. In summary, the article provides valuable insights into the challenges and opportunities presented by the integration of advanced technologies in modern manufacturing processes, emphasising the need for a holistic and proactive approach to cybersecurity in the era of digital manufacturing.

TITLE - Cybersecurity-Enhanced Encrypted Control System Using Keyed-Homomorphic Public Key Encryption - 6

By Masaki Miyamoto and team

ABSTRACT: The article introduces a secure encrypted control system designed for industrial applications, with a focus on detecting cyberattacks such as signal and control parameter falsification. The study employs a Keyed-Homomorphic Public Key Encryption (KH-PKE) scheme for enhanced security, particularly utilising a Proportional Integration Derivative (PID) position-control system for experimental validation.

INTRODUCTION: Summary of Key Contributions:

1. Security Against Tampering: The KH-PKE scheme enhances security by using homomorphic encryption, which allows computations on encrypted data. This helps in detecting cyberattacks, specifically signal and control parameter falsification, by returning an error symbol when attacks occur.
2. Real-Time Attack Detection: The proposed control system enables real-time detection of cyberattacks, providing an advantage over conventional encrypted control systems. This is crucial for identifying attacked components within signals and control parameters during operation.
3. Quantizer for Efficiency: The study introduces a novel quantizer to reduce computation time and minimise quantization-error effects on control performance. This contributes to the efficiency and effectiveness of the proposed encrypted control system.
4. Secure Automatic Control Technology: The developed system not only focuses on security but also emphasises real-time implementation capabilities. This contributes to the advancement of secure automatic control technology in industrial settings.
5. Exploration of Security Concepts: The article explores security concepts for real-time control systems, addressing the evolving challenges in networked environments. This is important for enhancing the overall security posture of control systems in industrial applications.

Key Components of KH-PKE Scheme: The KH-PKE scheme utilised in the proposed encrypted control system involves the following algorithms:

1. Randomly choose a prime number p of length $\kappa + 1$ bits and a generator g for \mathbb{Z}_p^* .
2. Select random secret keys $skd, skh \in \mathbb{Z}_p^*$.
3. Compute $pk = (p, g, g^{skd}, g^{skh})$ as the public key.

Enc: $(pk, m) \rightarrow c$. The Enc algorithm takes the public key pk and a message $m \in \mathbb{Z}_p$, and it outputs the ciphertext c .

1. Choose a random $r \in \mathbb{Z}_p^*$.
2. Compute the ciphertext $c = (g^r, g^{(skd * r) * m})$.

Dec: $(pk, skd, c) \rightarrow m$. The Dec algorithm takes the public key pk , the secret key skd , and the ciphertext c , and it outputs the decrypted message m .

1. Parse the ciphertext $c = (u, v)$.
2. Compute $w = v * (u^{(skd)})^{-1} \bmod p$.
3. Output $m = w$.

Eval: $(pk, skh, c1, c2) \rightarrow c$. The Eval algorithm takes the public key pk , the secret key skh , and two ciphertexts $c1$ and $c2$, and it outputs the homomorphic combination of $c1$ and $c2$.

1. Parse the ciphertexts $c1 = (u1, v1)$ and $c2 = (u2, v2)$.
2. Compute the homomorphic combination $c = (u1 * u2, v1 * v2 * (u1^{(skh)})^{-1} \bmod p)$.
3. Output c .

These algorithms constitute the KH-PKE scheme used in the proposed encrypted control system. The security of the scheme is based on the Decisional Diffie-Hellman (DDH) assumption.

CONCLUSION: The study significantly contributes to the field of cybersecurity in industrial control systems by introducing a secure encrypted control system with real-time attack detection capabilities. The KH-PKE scheme, based on homomorphic encryption, adds an extra layer of security, and the experimental validation using a PID position-control system reinforces the practical applicability of the proposed approach. The findings have broader implications for improving the security of networked control systems in industrial environments.

TITLE - Cybersecurity data science: an overview from machine learning perspective - 7

By IEEE

INTRODUCTION: This introduction emphasises how the growing reliance on digitalization and the Internet of Things is creating new cybersecurity challenges. It highlights the financial losses, the exponential rise in security incidents, and the critical requirement for strong cybersecurity defences. It is shown how data science, and especially machine learning, is propelling a paradigm shift in cybersecurity. In order to process security data and make wise judgments, the study emphasises the importance of Cybersecurity Data Science (CDS). The rising trend over the last five years clearly shows how popular data science and associated technologies are. By providing an overview of several machine learning techniques in the context of cybersecurity, the paper seeks to assist academics and professionals in the industry in constructing data-driven smart cybersecurity models.

CYBER SECURITY RISKS AND ITS ATTACKS: The information and communication technology (ICT) sector has seen significant change over the past 50 years, becoming an essential component of contemporary society in the rapidly changing field of cybersecurity. Because of our increased reliance on ICT, cybersecurity has become a crucial field as efforts to protect systems from cyber threats have increased. Cybersecurity is a broad term that refers to a set of procedures and policies intended to defend data, software, and computer networks from intrusions, changes, and attacks. Ensuring the confidentiality, integrity, and availability of information assets is one of cybersecurity's fundamental tenets. One of the most important aspects of cybersecurity is comprehending cyber threats and creating appropriate defences. Unauthorised access, virus assaults (including ransomware), and denial-of-service (DoS) attacks are security vulnerabilities linked to cyberattacks.

CYBER SECURITY DEFENSE STRATEGIES: Defence measures are necessary to protect networks, information systems, and data from intrusions and cyberattacks. These tactics centre on stopping security incidents and data breaches, keeping an eye out for unwanted behaviour, and reacting to intrusions, which are any illegal actions that comprise an information system. A hardware or software program that keeps an eye out for malicious activities or policy violations on computer networks or systems is known as an intrusion detection system, or IDS. Antivirus software, firewalls, user authentication, access control, and data encryption are examples of traditional security solutions that might not be able to fully meet the demands of the cyber business today. IDS, on the other hand, addresses these issues by examining security information from critical locations inside a system or computer network. Systems for detecting intrusions are essential for spotting both external and internal threats.

MACHINE LEARNING TASK IN CYBERSECURITY: It is widely accepted that machine learning (ML) is a subset of "artificial intelligence," strongly related to analytics, data mining, computational statistics, and data science. Making data-driven learning possible for computers is its main goal. Typically, machine learning models are composed of a collection of guidelines, techniques, or complex "transfer functions" that can be used to recognize interesting patterns in data or forecast behaviour. This is a very important capability in the field of cybersecurity. The conversation that follows covers different approaches that can be used to solve machine learning issues and how they relate to cybersecurity goals.

RESEARCH ISSUES AND FURTHER DIRECTIONS: The research issues and future directions in the realm of cybersecurity data science are outlined, identifying key challenges from data collection to decision-making processes:

1. **Cybersecurity Datasets:** The primary challenge lies in the insufficiency of existing datasets to understand recent behavioural patterns of cyber-attacks. Although data can be processed and transformed, the lack of recent datasets poses a challenge. Establishing a substantial number of up-to-date datasets for specific problem domains, like cyber risk prediction or intrusion detection, is crucial and represents a major challenge in cybersecurity data science.
2. **Handling Quality Problems in Datasets:** Cyber datasets are prone to issues such as noise, incompleteness, insignificance, imbalance, or inconsistency related to specific security incidents. These problems can impact the learning process and the performance of machine learning models. Effectively addressing these issues, either through existing algorithms or novel approaches, is vital for making data-driven intelligent decisions in cybersecurity solutions.

CONCLUSION: This paper explores the convergence of cybersecurity, data science, and machine learning, focusing on the role of cybersecurity data science in driving intelligent decision-making for advanced cybersecurity systems. It emphasises the impact of machine learning techniques on both security incidents and datasets. The article outlines the current landscape, noting a predominant focus on traditional security solutions and identifying a need for more research on machine learning-based security systems.

The paper not only provides an understanding of cybersecurity data science but also identifies key challenges and proposes future research directions. A multi-layered framework based on machine learning techniques is presented, encompassing phases such as security data collection, preparation, modelling, and incremental learning. This framework aims to guide the development of dynamic and intelligent cybersecurity systems. Overall, the paper contributes valuable insights to the field and encourages further exploration of the potential of data science in cybersecurity.

TITLE - Cybersecurity: trends, issues, and challenges - 8

By IEEE

ABSTRACT: In the contemporary landscape of an interconnected world, the fields of cybersecurity and digital forensics are grappling with an expanding array of cyber threats in near real-time conditions. Effectively addressing these threats necessitates the integration of cutting-edge technologies such as threat intelligence, big data analytics, and machine learning techniques. The paper underscores the pivotal role played by these technologies in the swift detection, comprehensive analysis, and robust defence against dynamic cyber threats.

INTRODUCTION: The proliferation of substantial amounts of data generated by diverse security monitoring solutions underscores the need for intelligent big data analytics. This analytics framework is crucial for mining, interpreting, and extracting knowledge from vast and often unstructured data sets. The seamless integration of cyber threat intelligence, artificial intelligence, and machine learning is imperative for perceiving, reasoning, learning, and acting against the continually evolving tactics employed by cyber adversaries.


The special issue features six papers that contribute significantly to advancing knowledge in the realm of cybersecurity. The primary focus spans digital forensics tools, techniques facilitating the investigation of potentially illegal cyber activities, and the emergent challenges posed by fifth-generation (5G) networks.

The first paper delves deeply into the challenges associated with achieving end-to-end slice isolation in evolving 5G networks. It places a particular emphasis on security considerations within the context of the ever-evolving network architectures. Another paper within the issue explores the domain of 5G cellular network forensics, elucidating the features of 5G networks that are pertinent to forensic processes, such as lawful interception mechanisms.

A third paper concentrates on laying the foundations and applications of artificial intelligence for zero-day and multi-step attack detection. The authors present a comprehensive framework that harmoniously combines statistical analysis and machine learning to study complex cyber attacks, thereby enhancing detection and investigation capabilities.

The issue further includes a paper that sheds light on collecting detailed transaction traces directly from payment terminals. This innovative approach provides valuable insights into shoppers' behaviour and proposes a novel methodology for designing contextual risk management systems.

Moreover, the architecture of an open engineering system named OMMA (Operator-guided Monitoring of Multi-step Attacks) is introduced. This system offers a collaborative platform for integrating diverse multi-step attack detection methods, fostering research collaborations and leveraging past work effectively.

Lastly, a  paper presents a robust methodology for detecting different types of Distributed Denial of Service (DDoS) attacks and distinguishing them from benign flash crowds. The proposed solution considers dynamic parameters of network traffic and conducts experiments to validate its effectiveness thoroughly.

In summary, the special issue provides a comprehensive and nuanced perspective on recent research advances in the domain of cybersecurity. Encompassing diverse topics ranging from network forensics and 5G security to artificial intelligence and advanced attack detection methodologies, the papers collectively contribute to the evolving landscape of cybersecurity research.

CONCLUSION: The context highlights the pivotal role of cybersecurity and digital forensics in tackling contemporary cyber threats, emphasising the integration of technologies like threat intelligence, big data analytics, and machine learning. The special issue covers diverse topics, including 5G security challenges, network forensics, and advanced attack detection methodologies. Papers delve into issues such as end-to-end slice isolation in 5G networks, cellular network forensics, and the application of artificial intelligence for zero-day and multi-step attack detection. The collection aims to advance knowledge in cybersecurity by addressing complex challenges and proposing innovative solutions.

TITLE - What Will the Future of Cybersecurity Bring Us, and Will It Be Ethical? The Hunt for the Black Swans of Cybersecurity Ethics - 9

By ALEKSANDRA PAWLICKA , MAREK PAWLICKI , RAFAŁ KOZIK , AND MICHAŁ CHORAŚ

ABSTRACT: "What Will the Future of Cybersecurity Bring Us, and Will It Be Ethical? The Hunt for the Black Swans of Cybersecurity Ethics." The paper explores the dynamic landscape of cybersecurity ethics and presents findings from a Horizon Scanning study aimed at identifying anticipated emerging ethical issues in the field. The key points include:

1. Complexity of Cybersecurity Ethics:

- Ethics in cybersecurity is acknowledged as intricate and plays a crucial role in affecting individuals' well-being.

2. Ethical Principles:

- Various ethical principles, such as beneficence, non-maleficence, autonomy, justice, and explicability, are considered fundamental to cybersecurity practices.

3. Evolution of Cybersecurity and Ethical Challenges:

- The constant evolution of cybersecurity technologies presents both opportunities and ethical challenges, with the COVID-19 pandemic emphasising the importance of ethical considerations.

4. Ethical Principles for Professionals:

- Despite the absence of a universal code of conduct, proposed ethical principles by different authors, including Formosa et al. and Van Imp, are discussed.

5. Horizon Scanning Study Design:

- The study, a follow-up to a previous one, employs a Horizon Scanning approach to detect both mainstream and emerging ethical concerns in cybersecurity.

6. Methods Used:

- Various sources, including professional press, books, patents, news media, government reports, surveys, social media, blogs, and wikis, are systematically scanned to identify strong and weak signals.

7. Strong Signals (Mainstream Ethical Issues):

- Privacy, ethical hacking, biased AI decisions, data use, and ransomware are identified as strong signals, representing mainstream concerns.

8. Weak Signals (Emerging Ethical Issues):

- Emerging issues include IoT-related concerns, ethical dilemmas in cloud computing, and other hidden signals like the environmental impact of cybersecurity and challenges faced by whistleblowers.

9. Figure 3 - Identified Signals:

- A visual representation (Figure 3) showcases the identified hidden and weak signals, summarising anticipated emerging ethical issues in cybersecurity.

CONCLUSION: The article concludes by emphasising the importance of ethical standards in major cybersecurity decisions. It calls for ongoing interdisciplinary dialogue to address emerging challenges and transform discussions into meaningful actions.

In summary, the paper underscores the intricate nature of cybersecurity ethics, the evolving landscape of technology, and the necessity for ongoing attention to ethical considerations in this rapidly changing field. The findings contribute to discussions on the ethical dilemmas of cybersecurity and advocate for a proactive approach to ethical decision-making.

TITLE - From ChatGPT to ThreatGPT: Impact of Generative AI in Cybersecurity and Privacy - 10

Author: MAANAK GUPTA , (Senior Member, IEEE), CHARANKUMAR AKIRI, KSHITIZ ARYAL, (Graduate Student Member, IEEE), ELI PARKER, AND LOPAMUDRA PRAHARAJ, (Graduate Student Member, IEEE)

ABSTRACT: The abstract emphasises the transformative power of Generative AI models like ChatGPT and Google Bard in the digital landscape of 2022. The paper's primary objective is to investigate the consequences of GenAI from both defensive and offensive cybersecurity perspectives. It addresses social, ethical, and privacy implications, presenting limitations, challenges, risks, and opportunities associated with GenAI. The research explores vulnerabilities in ChatGPT, showcasing attacks such as Jailbreaks, reverse psychology, and prompt injection. Additionally, it examines the potential misuse of GenAI by cyber offenders and discusses defense techniques. The conclusion highlights open challenges and future directions for ensuring the security, trustworthiness, and ethics of GenAI.

INTRODUCTION: Key Points:

1. Evolution of GenAI and ChatGPT:

- Traces the historical development of generative models and highlights ChatGPT's profound impact on diverse domains.
- Notes ChatGPT's rapid adoption, reaching 100 million users within two months of release.

2. Impact of GenAI in Cybersecurity:

- Discusses the dual role of GenAI, benefiting both defenders and attackers in the cybersecurity landscape.
- Explores applications in threat intelligence, incident response, and ethical guideline development.

3. Attacking ChatGPT:

- Examines techniques like Jailbreaks and the "Do Anything Now" (DAN) method, showcasing potential misuse by users.

4. Applications of GenAI in Cyber Attacks:

- Highlights how cyber attackers can leverage GenAI for social engineering attacks, phishing, malware creation, and other malicious activities.

5. Defense Techniques Using GenAI:

- Explores how GenAI contributes to cyber defence through automation, threat intelligence, and ethical guideline development.

6. Social, Legal, and Ethical Implications:

- Delves into the broader implications of ChatGPT, addressing concerns related to privacy violations and ethical boundaries.

7. Comparison of Security Features:

Compares the security features of ChatGPT and Google Bard, two leading GenAI systems.

8. Challenges and Future Directions:

- Concludes by emphasising open challenges and proposing future research directions to enhance the security, trustworthiness, and ethics of GenAI.

Use Cases and Techniques:

1. SWITCH Method, CHARACTER Play Method, and Reverse Psychology:

- Discusses methods like SWITCH, CHARACTER Play, and reverse psychology as techniques employed to interact with AI models.

2. Implications and Mitigation Strategies:

- Addresses the implications of roleplay methods and the importance of mitigating potential misuse through advanced filtering algorithms.

3. Reverse Psychology for Pirate Sites:

- Demonstrates how reverse psychology can be applied to generate responses related to potentially harmful content.

4. Applications in Cybersecurity Defense:

- Explores various applications of ChatGPT in cybersecurity defence, such as automation, reporting, threat intelligence, code generation, attack identification, and incident response.

CONCLUSION: The research underscores the multifaceted impact of GenAI, offering insights into its risks, benefits, and ethical considerations in the evolving landscape of cybersecurity. The article concludes with a call for continued research to address challenges and ensure responsible and secure usage of Generative AI models.

Title - A Comparative Analysis of Industrial Cybersecurity Standards - 11

By Fatiha Djebbar (Member, IEEE) and Kim Nordström

ABSTRACT: This research paper delves into the complex landscape of cybersecurity standards, emphasising their significance in managing and evaluating cybersecurity risks. The study focuses on optimising compliance efforts by identifying overlapping security controls among three major standards: ETSI EN 303 645 v2.1.1, ISA/IEC 62443-3-3:2019, and ISO/IEC 27001:2022. The comparative analysis sheds light on commonalities, offering valuable insights for organisations aiming to streamline their compliance processes.

INTRODUCTION: Key Points

1. Objective:

- Analyse and compare ETSI EN 303 645, ISA/IEC 62443-3-3, and ISO/IEC 27001 to identify overlapping security controls.
- Address challenges in the selection and implementation of cybersecurity standards.

2. Rationale:

- Proliferation of cybersecurity standards poses challenges, leading to potential duplication of efforts and increased costs.
- Streamlining compliance by recognizing commonalities among standards is a key focus.

3. Selected Standards:

- ETSI EN 303 645: Consumer IoT devices.
- ISA/IEC 62443-3-3:2019: Industrial automation and control systems.
- ISO/IEC 27001:2022: Information security management systems.

4. Methodology:

- Comparative study to identify overlaps and discrepancies in security controls.
- Goal: Simplify compliance processes for efficient selection of security controls.

5. Findings:

- Significant overlap among the three selected standards.

- Facilitates understanding of common security requirements for streamlined compliance.

6. Benefits for Organisations:

- Removal of redundant compliance efforts.
- Streamlined compliance reduces implementation time and costs.

7. Challenges:

- Implementation challenges of overlapping controls and requirements.
- Emphasis on addressing challenges to enhance the effectiveness of cybersecurity standards.

8. Conclusion:

- Recognizing similarities between cybersecurity standards is crucial for optimising compliance efforts.
- Findings provide a practical resource for organisations aiming to enhance cybersecurity posture efficiently.

- ISMS standard with 93 high-level controls.
- Encompasses organisational, people, physical, and technology security.

ISA/IEC 62443-3-3:2019

- Addresses security vulnerabilities in industrial automation and control systems (IACSs).
- Defines security levels (SL0 to SL4) based on control system capability.
- Focuses on system security requirements and security levels.

- Focuses on security and data protection for consumer IoT devices.
- 13 high-level recommendations with 68 provisions.
- Emphasises consumer data protection, IoT device security, and privacy.

Challenges in Cybersecurity Standards Implementation

1. **Dynamic Landscape:

- Challenges in maintaining a steady level of system security due to evolving cybersecurity threats.
- Optimization based on business leaders' definition and balancing limited resources.

2. Partial Mitigation:

- Cybersecurity standards partially manage challenges, but not all risks can be mitigated through frameworks.

3. Cross-Functional Challenges:

- Coordination challenges due to the cross-functional nature of cybersecurity.
- Difficulty in selecting a framework among an excess of standards.

4. Redundancy and Conflicting Controls:

- Risk of implementing redundant or conflicting security controls when complying with multiple standards.
- Emphasis on identifying duplicated controls to simplify the process.

5. Mapping Controls:

Difficulty in mapping controls between standards due to variations in wording and ambiguity.

- Common mistake of addressing cybersecurity on a system-by-system basis.

6. Comprehensive Security Perspective:

- Emphasis on evaluating the entire system's security perspective.
- Recommendation from ISA/IEC 62443 for an end-to-end evaluation.

7. Implementation Challenges of ISA/IEC 62443 Framework:

- Time-consuming process for implementing a security management program based on ISA/IEC 62443.
- Involves a comprehensive management system covering policies, procedures, personnel, and IACSs.

8. Use of COTS Products:

- Acknowledges the use of commercial off-the-shelf products in non-critical industrial environments.

- Highlights the need for robust cybersecurity in critical systems.

9. Tolerating Imperfection:

- Despite best efforts, vulnerabilities, breaches, and security incidents are inevitable.

- Cybersecurity professionals must adapt to emerging threats.

CONCLUSION AND FUTURE WORKS: Comparative Analysis:

- Significant similarities among standards despite different environments and scopes.

- Identification of gaps and overlaps contributes to a more streamlined compliance process. Future

Prospects:

- Addressing overlaps and gaps in industrial standards for streamlined compliance.

- Goal to identify a comprehensive standard to reduce fragmentation and enhance cybersecurity implementation efficiency.

TITLE - Security & Privacy Economics - 12

By Michael Lesk, Jeffrey MacKie-Mason

ABSTRACT: This article explores the intricate relationship between cybersecurity and economics, emphasising the responsibility of organisations in safeguarding sensitive information. The author contends that organisations holding data should bear the responsibility for security lapses, and the cost of such breaches should motivate them to enhance security measures. However, complexities arise due to varying regulations and practices globally.

INTRODUCTION: Key Points:

1. Individual Behaviour:

- Individuals may not prioritise security efforts, demonstrated by instances where people were willing to disclose computer passwords for a small reward.
- Consequences of poor individual security, such as contributing to botnets, may affect others more than oneself.

2. Shifting Costs to Industries:

- The logical approach is to shift the cost of security to industries capable of addressing the issue effectively.
- However, the author highlights complexities, citing examples like differences in fraud liability rules between US and European banks.

3. Industry Incentives:

- Companies may lack adequate incentive to minimise computer fraud.
- Deloitte reports that financial services companies spend 6 to 7 percent of their IT budget on security, but questions whether this is sufficient.

4. Public vs. Private Action:

- The article explores the idea of public action, suggesting that government involvement may be necessary.
- Government responsibility for computer security is argued as a public good, benefiting both individuals and industries.

5. Government's Role:

- Suggestions for government action include more research, participation in standards development, and setting economic rules.

- The article proposes that government intervention is crucial in ensuring a secure cyberinfrastructure.

6. Challenges in Encouraging Security:

- Challenges include information asymmetry, where consumers lack information about the security of software packages.

- Suggestions include regulations, liability rules, and insurance as mechanisms to encourage safer behaviour.

7. Insurance and Reporting Systems:

- Insurance is proposed as a means to encourage safer behaviour, but challenges exist in determining proper insurance rates due to limited cybersecurity knowledge.

- A reporting system, akin to NASA's pilot reporting system, is suggested for collecting data on security breaches without public disclosure.

8. Insufficient Attention to Cybersecurity:

- The article contends that society does not allocate enough attention or resources to cybersecurity.

- Calls for increased attention, research, and regulations before a significant cyber event compels action, likening it to historical instances like Pearl Harbor or 9/11.

9. Recommended Steps:

- Urges additional cybersecurity research, particularly in the context of preserving security holistically.

- Advocates for regulations and liability rules to enforce better security processes as information about effectiveness is developed.

CONCLUSION: The article stresses the need for collective efforts involving research, regulation, and industry collaboration to address the challenges of cybersecurity effectively.

TITLE - Enhancing Building Cybersecurity Through BCF Implementation

By Michael Mylrea, Sri Nikhil Gupta Gourisetti, Member, IEEE, Andrew Nicholls Pacific Northwest National Laboratory

ABSTRACT: This paper introduces the Buildings Cybersecurity Framework (BCF) as a comprehensive guide to fortify organisations against evolving cybersecurity threats, particularly in the context of smart buildings. Built upon the National Institute of Standards and Technology (NIST) Cybersecurity Framework, the BCF comprises five core functions: Identify, Protect, Detect, Respond, and Recover.

INTRODUCTIONS: Key Points:

1. Purpose of BCF:

- Guides building owners and operators in effectively managing cybersecurity risks.
- Encompasses practices for securing both Information Technology (IT) and Operational Technology (OT) in buildings.

2. Core Elements of BCF:

- Structured around five core functions to strategically manage cybersecurity risk throughout its lifecycle.

3. Applicability and Scope:

- Applicable to various building types and critical infrastructure sectors, including commercial facilities, financial services, government facilities, healthcare, emergency services, and information technology.

4. Relation to National Initiatives:

- Aligns with national initiatives, including the Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure.
- Supports the use of NIST's Framework for Improving Critical Infrastructure Cybersecurity.

5. Need for Cybersecurity in Buildings:

- Addresses the imperative to tackle cybersecurity challenges arising from the digitization and connectivity of smart buildings.

- Highlights the tendency to overlook cybersecurity amidst technological advancements in smart buildings.

6. Risk Management and Framework Features:

- BCF is a risk-based framework, offering guidance on risk management processes and cybersecurity programs.
- Includes detailed activities, outcomes, references, checklists, use cases, and case studies for practical implementation.

7. Core Functions Overview:

- Identify: Focuses on asset management, governance, risk assessment, and supply chain risk management.
- Protect: Covers identity management, access control, awareness and training, data security, maintenance, and protective technology.
- Detect: Involves anomalies and events detection, and continuous security monitoring.
- Respond: Aims to respond effectively to cybersecurity events through planning, communication, analysis, mitigation, and improvements.
- Recover: Focuses on recovery planning and communication to return services to normal operation post-cybersecurity incidents.

Inherent Frameworks and Standards:

- BCF incorporates standards from various sources, including NIST, SANS Institute, ISA, ISO/IEC, DOE, and DoD, providing a robust foundation for cybersecurity implementation in buildings.

CONCLUSION: - BCF presents a practical and structured approach to address cybersecurity challenges in smart buildings.

- Applicable across diverse building types, it assists stakeholders in assessing, prioritising, and enhancing their cybersecurity posture.
- Aligns with national cybersecurity initiatives and supports the goals of the Presidential Executive Order.
- The framework's implementation is vital in securing the benefits of smart buildings while mitigating cybersecurity risks effectively.

