World Journal of Advanced Engineering Technology and Sciences
eISSN: 2582-8266
Cross Ref DOI: 10.30574/wjaets
Journal homepage: https://wjaets.com/

(REVIEW ARTICLE)

Check for updates

Organizational information security threats: Status and challenges

Bernard Oloo Akello *

Jaramogi Oginga Odinga University of Science and Technology, Kisumu, Kenya.

World Journal of Advanced Engineering Technology and Sciences, 2024, 11(01), 148–162

Publication history: Received on 19 May 2023; revised on 04 February 2024; accepted on 07 February 2024

Article DOI: https://doi.org/10.30574/wjaets.2024.11.1.0152

Abstract

Organizational information security is a critical concern in today's interconnected and data-driven world. With the increasing frequency and sophistication of cyber threats, organizations face significant risks to the confidentiality, integrity, and availability of their sensitive information. This paper provides an overview of the key aspects and challenges related to organizational information security. It highlights the importance of implementing robust security measures, such as firewalls, intrusion detection systems, encryption technologies, and secure coding practices, to protect against external threats. It also demonstrates the need for continuous monitoring, threat intelligence sharing, and incident response capabilities to detect and respond to security incidents effectively. This survey shows importance of user awareness, training, and adherence to security policies and procedures. In addition, the significance of establishing a security-centric culture within organizations to mitigate the risk of insider threats and promote a strong security posture is discussed. The evolving threat landscape, including challenges associated with advanced persistent threats, zero-day vulnerabilities, and the security of emerging technologies such as IoT and AI are highlighted, together with the need for ongoing research and innovation to address these challenges and enhance the effectiveness of preventive measures.

Keywords: Attacks; Threats; Privacy; Organizations; Information security

1. Introduction

As technology advances and we become more interconnected, organizations find themselves in a constant battle to protect their valuable data, systems, and networks from an array of malicious actors [1]-[4]. The evolving threat landscape demands utmost attention and collective efforts to ensure the security and resilience of organizations. In recent years, there has been a significant shift in the nature and sophistication of information security threats [5], [6]. Attackers have become increasingly adept at exploiting vulnerabilities, leveraging new technologies, and employing innovative attack vectors. As a result, organizations across industries face a multitude of challenges that require proactive measures and comprehensive strategies to mitigate risks [7]. One of the most prominent threats organizations face today is the rise of sophisticated cyber attacks. Cybercriminals, hacktivists, and state-sponsored actors have honed their skills, deploying complex malware, ransomware, and phishing campaigns to infiltrate systems and compromise sensitive information [8]-[10]. These attacks not only cause financial losses but also damage reputations and erode customer trust. According to [11] and[12], the advent of the Internet of Things (IoT) has brought about a new wave of security concerns. As we embrace interconnected devices in our workplaces, homes, and public spaces, the attack surface expands exponentially. Vulnerabilities in IoT devices, coupled with lax security practices, can lead to devastating consequences, including unauthorized access, data breaches, and even physical harm [13].

Another emerging threat is the proliferation of social engineering attacks, which exploit human vulnerabilities rather than technical ones [14]-[17]. Social engineering techniques such as pre-texting, phishing, and baiting manipulate individuals into divulging sensitive information or performing actions that can compromise organizational security. The

* Corresponding author: Bernard Oloo Akello

sophistication of these attacks, combined with the increasing amount of personal information available online, makes them a significant concern for organizations today. The rapid adoption of cloud computing services has been noted in [18] to present both opportunities and challenges for organizations. While cloud technology offers flexibility, scalability, and cost-efficiency, it also introduces new risks. Inadequate access controls, data breaches in cloud storage, and insecure Application Programming Interfaces (APIs) are among the vulnerabilities that organizations must address to safeguard their sensitive data in the cloud [19], [20]. In addition, the ever-expanding threat landscape is exacerbated by the emergence of emerging technologies such as artificial intelligence, blockchain, and quantum computing [21]-[23]. While these technologies hold immense promise, they also introduce unique security implications. Organizations must carefully navigate the risks associated with these emerging technologies to ensure their benefits are realized without compromising security.

Based on the above discussion, it is clear that the information security landscape facing organizations today is evolving at an unprecedented pace. To protect against emerging threats, organizations must adopt a proactive and holistic approach to cyber security. This involves investing in robust defense mechanisms, implementing effective security awareness programs, fostering a culture of security throughout the organization, and collaborating with industry partners and government entities to share threat intelligence and best practices. In this paper, a review of the organizational security threats, major security incidences, technologies to protect against these information security threats as well as the challenges of these current technologies is provided.

2. Major organizational information security threats

Organizations face numerous information security threats that can compromise the confidentiality, integrity, and availability of their sensitive data. Table 1 describes some of the major organizational information security threats.

Table 1 Major organizational information security threats

Security threat	Explanation
Phishing and Social Engineering	Phishing involves tricking individuals into revealing sensitive information or performing actions that can compromise security [24], [25]. Social engineering techniques exploit human vulnerabilities to manipulate people into divulging confidential information or granting unauthorized access
Advanced Persistent Threats (APTs)	APTs are sophisticated and targeted attacks usually perpetrated by well-funded and organized groups. They involve long-term infiltration, espionage, and data exfiltration, with the aim of gaining unauthorized access to sensitive information [26]-[28].
Distributed Denial of Service (DDoS) Attacks	DDoS attacks overwhelm a network, system, or application with a flood of traffic, rendering it inaccessible to legitimate users [29]. These attacks disrupt services, leading to financial loss and reputational damage [30].
Physical Security Breaches	Physical breaches involve unauthorized access to physical spaces, such as data centers or offices, where sensitive information is stored [31]. Theft or tampering with physical assets, such as servers or storage devices, can lead to significant data breaches.
Mobile Device and BYOD Risks	The use of personal mobile devices or “bring your own device” (BYOD) policies can introduce security vulnerabilities [31]-[34]. Lost or stolen devices, unsecured Wi-Fi connections, and vulnerable mobile apps can lead to data breaches and unauthorized access.
Malware Attacks	Malicious software, such as viruses, worms, Trojans, ransomware, and spyware, can infiltrate systems and networks, infecting computers and stealing or damaging data [35].
Cloud Computing Risks	Organizations leveraging cloud services face risks such as data breaches, insecure APIs, mis-configurations, insider threats at the cloud provider, and lack of control over data security [36]-[38].
Unpatched Software and Vulnerabilities	Organizations that fail to apply necessary software updates and security patches are vulnerable to known vulnerabilities that attackers can exploit to gain unauthorized access or disrupt systems [39], [40].
Insider Threats	Insiders with authorized access to an organization's systems and data can intentionally or inadvertently cause harm [41]. This includes employees, contractors, or business partners

	who misuse their privileges, steal data, or accidentally expose sensitive information [42], [43].
Data Breaches	Data breaches occur when unauthorized individuals gain access to sensitive information, such as customer data, intellectual property, or trade secrets [44], [45]. Breached data can be exploited for financial gain, identity theft, or other malicious purposes.
Third-Party Risks	Organizations often rely on third-party vendors, suppliers, or partners who may have access to their systems or data [46]. If these third parties have weak security measures or suffer a breach, it can impact the organization's security posture.

To mitigate these threats, organizations should implement a comprehensive information security program, including robust policies and procedures, employee education and awareness, regular security assessments, strong access controls, encryption, and incident response plans.

3. Prominent organizational security incidences

One prominent organizational security incident that shook the world was the data breach at Equifax in 2017. Equifax is one of the largest credit reporting agencies in the United States. In this incident, hackers gained unauthorized access to the personal information of approximately 147 million people, including their names, social security numbers, birth dates, addresses, and in some cases, driver's license numbers. The Equifax breach had far-reaching consequences as it exposed sensitive personal information of a significant portion of the American population [47]. The stolen data could be used for identity theft, fraud, and other malicious activities. The incident highlighted the vulnerability of organizations that handle vast amounts of personal data and raised concerns about the security practices and measures implemented [48] by such entities. The breach not only had severe implications for the affected individuals but also resulted in a significant loss of trust in Equifax and the credit reporting industry as a whole. The company faced widespread criticism for its handling of the incident, including delays in reporting the breach and inadequate security measures. The incident also led to numerous lawsuits, investigations by regulatory authorities, and congressional hearings.

Another notable organizational security incident was the ransomware attack on Colonial Pipeline in May 2021 [49]. Colonial Pipeline operates one of the largest fuel pipeline networks in the United States, transporting gasoline, diesel, and jet fuel from Texas to the East Coast. The attack involved a criminal group called DarkSide, which exploited a vulnerability in the company's IT systems to gain control over its networks. As a result of the attack, Colonial Pipeline was forced to shut down its operations, leading to widespread fuel shortages, panic buying, and disruptions in the fuel supply across several states. The incident highlighted the vulnerability of critical infrastructure systems to cyber attacks and the potential impact on everyday life [50]. The Colonial Pipeline attack drew attention to the growing threat of ransomware attacks, where hackers encrypt an organization's data and demand a ransom in exchange for its release [51]. It also underscored the importance of robust cyber-security measures, incident response planning, and coordination between the private sector and government agencies in dealing with such attacks.

The 2013 data breach of Target, a major U.S.-based retail corporation is yet another notable organizational security incident [52]. Hackers gained access to Target's network and stole the personal and financial information of approximately 110 million customers. The breach occurred during the holiday shopping season, making it particularly impactful. It exposed weaknesses in Target's security infrastructure and raised concerns about the security of payment systems used by retailers [53]. The Target breach served as a wake-up call for organizations worldwide, highlighting the importance of implementing robust security measures [54] to protect customer data. It led to increased awareness of the need for improved cyber-security practices, including better network monitoring, threat detection, and incident response protocols.

In 2020, SolarWinds, a leading provider of network management software, experienced a sophisticated supply chain attack that impacted numerous organizations worldwide [55]. Hackers compromised SolarWinds' software updates and used them to distribute a backdoor known as "Sunburst" to the company's customers. This allowed the attackers to gain unauthorized access to the networks of various government agencies and private companies, including Microsoft [56], [57]. The SolarWinds breach exposed the vulnerabilities associated with supply chain attacks and the potential for devastating consequences when trusted software updates are compromised. It highlighted the need for organizations to enhance their security practices and adopt robust mechanisms for verifying the integrity of software and third-party components.

In 2014, Sony Pictures Entertainment experienced a major cyber attack that resulted in the leakage of a vast amount of sensitive information [58]. The attack, attributed to North Korean hackers, led to the exposure of confidential emails, employee personal information, unreleased films, and other internal documents [59]. The incident not only had financial implications for Sony but also raised concerns about the vulnerability [60] of critical infrastructure and the potential for geopolitical cyber conflicts.

The Cambridge Analytica scandal, which emerged in 2018, involved the unauthorized access and exploitation of personal data from millions of Facebook users. Cambridge Analytica, a political consulting firm, used data obtained from a third-party app on Facebook to profile and target users with personalized political advertisements [61]-[63]. The incident sparked debates about data privacy, ethics, and the role of social media platforms in handling user data. It also led to increased scrutiny of how organizations handle and protect user information.

Stuxnet is another incidence and perhaps one of the most infamous and sophisticated computer worms ever discovered [64]. It was first identified in 2010 and specifically targeted industrial control systems (ICS) that are commonly used in critical infrastructure [65], such as power plants and factories. It exploited multiple zero-day vulnerabilities and used various propagation methods, including USB drives, to spread and infect systems. What made this worm particularly remarkable was its ability to target and manipulate programmable logic controllers (PLCs) that manage machinery and industrial processes [66]. It specifically targeted Siemens' PLCs that were used in Iran's uranium enrichment facilities, causing significant damage to their centrifuges. The worm was designed to manipulate the rotational speeds of the centrifuges, causing them to spin too fast or too slow, which ultimately disrupted the enrichment process. By doing so, Stuxnet aimed to delay Iran's nuclear program and hinder its ability to develop nuclear weapons [67]. It demonstrated the potential of cyber attacks to physically damage or disrupt critical infrastructure, highlighting the convergence of cyber warfare and traditional military tactics. It also revealed the level of sophistication and resources that nation-states were willing to dedicate to covert cyber operations.

The discovery and analysis of Stuxnet brought attention to the importance of cyber-security for industrial control systems [68]. It prompted discussions about the vulnerabilities of critical infrastructure and the need for enhanced security measures to protect against similar attacks in the future [69]. The impact of this worm extended beyond its intended target as it spread beyond Iran's nuclear facilities and infected systems globally, inadvertently exposing the world to its advanced capabilities. It served as a wake-up call for governments, organizations, and security experts, highlighting the need for improved defenses against advanced cyber threats [70]. Overall, Stuxnet represents a landmark event in the history of cyber-security, demonstrating the potential for cyber attacks to physically disrupt critical infrastructure and showcasing the level of sophistication and covert operations employed by nation-states in the realm of cyber warfare [71].

These incidences have had significant impacts on individuals, businesses, and even global discussions on cyber-security, data privacy, and the responsibilities of organizations in safeguarding customer information. They serve as reminders of the ongoing challenges faced by organizations in safeguarding their systems and data in an increasingly interconnected and digitally-dependent world. They also demonstrate the critical importance of organizational security and the potential consequences of failing to adequately protect sensitive data.

4. Technologies to protect against information security threats

To protect against information security threats, organizations employ various technologies that work together to create a robust defense posture. Table 2 presents some of the key technologies commonly used in information security.

Table 2 Key technologies for information security

Technology	Discussion
Intrusion Detection and Prevention Systems (IDPS)	IDPS technologies monitor network traffic and system activities, looking for suspicious patterns or behaviors that may indicate an intrusion [72]-[74]. They can alert security personnel or automatically take action to block or mitigate potential threats.
Data Encryption	Encryption technologies transform sensitive data into unreadable formats [75], ensuring that even if intercepted, the information remains protected [76]-[79]. It is commonly used for data at rest (stored data) and data in transit (communication channels).

Antivirus and Anti-malware Software	These technologies scan systems for known viruses, malware, and other malicious software. They help detect and remove or quarantine threats, protecting against a wide range of malicious code and exploits [80-[82].
Virtual Private Networks (VPNs)	VPNs establish secure connections over untrusted networks, such as the internet [83]-[85]. They create encrypted tunnels for data transmission, enabling remote users to access corporate networks securely.
Secure Sockets Layer/Transport Layer Security (SSL/TLS)	SSL/TLS protocols provide secure communication over networks, encrypting data transmitted between systems and ensuring its integrity and confidentiality [86]-[89]. They are widely used for secure web browsing (HTTPS) and secure email communications.
Security Information and Event Management (SIEM)	SIEM solutions aggregate and analyze logs and event data from various sources to detect and respond to security incidents [90]. They provide real-time monitoring, threat detection [91], and incident response capabilities.
Secure Coding Practices	Technologies alone are not enough; secure coding practices play a vital role in preventing vulnerabilities and reducing the risk of exploits. Secure coding frameworks, guidelines, and training programs help developers write secure software [92]-[95].
Firewalls	Act as a first line of defense by monitoring and controlling incoming and outgoing network traffic based on predetermined security rules [96]. They help prevent unauthorized access and protect against external threats [97]-[100].
Multi-factor Authentication (MFA)	MFA adds an extra layer of security by requiring users to provide multiple forms of identification (e.g., passwords, biometrics, security tokens) to verify their identities [101], [102], [103]. This mitigates the risk of unauthorized access due to compromised passwords.
Patch Management Systems	Regularly updating software and operating systems with security patches is crucial for protecting against known vulnerabilities [104]-[106]. Patch management systems automate the process of identifying, deploying, and verifying the installation of necessary patches.

It's important to note that technology is just one aspect of a comprehensive information security strategy. Effective security also requires well-defined policies and procedures, regular security assessments, user awareness training, incident response plans, and ongoing monitoring and improvement efforts.

5. Challenges of the current technologies for information security threats prevention

While technologies play a crucial role in preventing information security threats, they also face several challenges that can limit their effectiveness. Some common challenges associated with current information security technologies include rapidly evolving threat landscape, zero-day vulnerabilities, complexity and integration issues, false positives and negatives, insider threats [107], resource limitations, user awareness and training, as well as privacy concerns.

According to [108] and [109], the threat landscape is constantly evolving, with new attack vectors, techniques, and malware emerging regularly. Therefore, information security technologies need to keep pace with these developments to effectively detect and mitigate new and sophisticated threats. As explained in [110] and [111], zero-day vulnerabilities are unknown software vulnerabilities that can be exploited by attackers before a patch is available. As such, information security technologies may not be able to protect against such vulnerabilities until a patch or update is released, leaving systems exposed to targeted attacks [112]. To offer enhanced security, many organizations employ a variety of security technologies from different vendors, leading to complex environments that require integration and interoperability between different systems. Lack of compatibility and integration challenges can result in gaps in security coverage and difficulties in managing and maintaining the technologies. The authors in [113] and [114] explain that information security technologies, such as intrusion detection systems and antivirus software, can generate false positives (incorrectly identifying benign activity as malicious) or false negatives (failing to detect actual threats). These inaccuracies can impact the efficiency and trustworthiness of security measures and may require additional time and resources for investigation.

While technologies can help protect against external threats, insider threats pose unique challenges [115], [116]. Authorized users with privileged access may intentionally or unintentionally misuse their privileges, leading to data breaches or other security incidents. Detecting and mitigating insider threats often requires a combination of technology, employee monitoring, and awareness programs. On the other hand, implementing and managing information security technologies [117] can be resource-intensive, both in terms of budget and skilled personnel. For instance, organizations may face challenges in allocating sufficient resources for the acquisition, implementation, monitoring, and maintenance of security technologies. As explained in [118], information security technologies are only as effective as the users who interact with them. Therefore, lack of user awareness and adherence to security best practices can undermine the effectiveness of security technologies [119]-[121] As such, adequate user education and training programs are essential to ensure that employees understand security risks and follow proper security protocols [122]. Regarding privacy, some security technologies, such as monitoring systems or data collection tools, may raise privacy concerns among users. Striking a balance between security and privacy is essential to maintain trust and compliance with privacy regulations [123]-[126].

Addressing these challenges requires a holistic approach that combines technology, policies, processes, and education. Organizations need to continually evaluate and update their security technologies, monitor emerging threats [127], invest in skilled personnel, and foster a culture of security awareness throughout the organization.

6. Research gaps

While significant advancements have been made in the prevention of organizational information security threats, there are still several research gaps that need to be addressed. Some key areas where further research is needed include the following:

Advanced Threat Detection: As cyber threats become increasingly sophisticated, there is a need for improved techniques to detect and mitigate advanced persistent threats (APTs) and zero-day attacks [128]-[132]. Therefore, research is required to develop more effective approaches for identifying and responding to emerging threats in real-time.

Insider Threat Detection: Insider threats continue to be a significant concern for organizations. Further research is needed to develop robust techniques for detecting and mitigating insider threats, including the use of behavioral analytics, anomaly detection, and privileged user monitoring [133]-[137].

Security of Internet of Things (IoT) Devices: The proliferation of IoT devices in various sectors introduces new security challenges [138]-[142]. More research work is needed to address vulnerabilities in IoT devices, develop secure communication protocols, and design effective security architectures to protect against IoT-related threats.

Artificial Intelligence (AI) and Machine Learning (ML) Security: AI and ML technologies are being increasingly integrated into security systems [143]-[146]. However, there is a need to study the potential vulnerabilities and adversarial attacks that can exploit AI/ML algorithms [147], as well as develop techniques to secure and defend against such attacks.

Privacy-Preserving Technologies: With the growing concerns over data privacy, there is a need for research on privacy-preserving technologies [148]-[152]. This includes developing methods for secure data sharing, privacy-enhancing data analysis techniques, and secure computation protocols that protect sensitive information while still enabling valuable insights to be derived [153]- [157].

Human Factors in Security: Human behavior remains a critical factor in organizational security. There is need for research directed towards better understanding human vulnerabilities, motivations, and decision-making processes that can lead to security breaches [158]-[160]. This includes studying user awareness, training effectiveness, and designing user-centric security interfaces and systems.

Cyber Threat Intelligence and Information Sharing: Enhancing collaboration and information sharing among organizations and security professionals is crucial in combating evolving threats [161]. A need arises to develop frameworks, protocols, and platforms that facilitate the sharing of timely and actionable threat intelligence while addressing privacy and trust concerns [162]-[167].

Resilience and Incident Response: According to [168] and [169], there is need for research that focuses on improving organizational resilience [170] to cyber incidents, including strategies for rapid incident response, effective recovery, and minimizing the impact of attacks. This includes studying incident response processes, incident management frameworks, and approaches for managing complex and coordinated attacks [171]-[173].

Addressing these research gaps will help advance the field of organizational information security and enable the development of more robust and effective prevention strategies. This calls for collaboration between academia, industry, and government entities to drive research and innovation in these critical areas.

7. Conclusion

Organizational information security is a complex and ever-evolving landscape. While significant progress has been made in recent years, numerous challenges persist, requiring continuous efforts to enhance security practices and technologies. It has been shown that organizations face a multitude of threats, ranging from sophisticated cyber-attacks to insider threats and vulnerabilities associated with emerging technologies like IoT and AI. The rapid pace of technological advancements and the increasing connectivity of systems further amplify the complexity of securing organizational information. To navigate this landscape effectively, organizations need to adopt a comprehensive and proactive approach to information security. This includes implementing a combination of robust technologies, well-defined policies and procedures, regular training and awareness programs, and incident response capabilities. Collaboration with external partners, such as threat intelligence providers and industry peers, is also crucial for staying ahead of evolving threats. While technological solutions are essential, it is equally important to recognize the role of human factors in information security. User awareness, training, and a culture of security play a vital role in preventing incidents and minimizing the impact of security breaches. Organizations must prioritize not only technical defenses but also the education and empowerment of their workforce. Furthermore, compliance with regulatory requirements and privacy laws is a growing concern. Organizations must stay abreast of legal and regulatory developments to ensure their security practices align with the necessary standards and protect customer data and privacy. There is therefore need for ongoing vigilance, investment, and collaboration. This calls for a multidimensional approach that combines technological advancements, research and innovation, user education, policy frameworks, and strong incident response capabilities. By addressing the challenges, filling research gaps, and adopting a proactive security mindset, organizations can enhance their defenses and protect sensitive information from ever-evolving threats.

Compliance with ethical standards

Disclosure of conflict of interest

The author has no any conflict of interest.

References

[1] Tounsi W, Rais H. A survey on technical threat intelligence in the age of sophisticated cyber attacks. Computers & security. 2018 Jan 1, 72:212-33.

[2] Skopik F, Settanni G, Fiedler R. A problem shared is a problem halved: A survey on the dimensions of collective cyber defense through security information sharing. Computers & Security. 2016 Jul 1, 60:154-76.

[3] Whyte C, Mazanec BM. Understanding Cyber-Warfare: Politics, Policy and Strategy. Taylor & Francis, 2023 Apr 18.

[4] Jimo S, Abdullah T, Jamal A. IoE Security Risk Analysis in a Modern Hospital Ecosystem. InCybersecurity in the Age of Smart Societies: Proceedings of the 14th International Conference on Global Security, Safety and Sustainability, London, September 2022 2023 Jan 3 (pp. 451-467). Cham: Springer International Publishing.

[5] Renaud K, Flowerday S, Warkentin M, Cockshott P, Orgeron C. Is the responsibilization of the cyber security risk reasonable and judicious?. Computers & Security. 2018 Sep 1, 78:198-211.

[6] Abduljabbar ZA, Abduljaleel IQ, Ma J, Al Sibahee MA, Nyangaresi VO, Honi DG, Abdulsada AI, Jiao X. Provably secure and fast color image encryption algorithm based on s-boxes and hyperchaotic map. IEEE Access. 2022 Feb 11, 10:26257-70.

[7] Datta P. Supply network resilience: a systematic literature review and future research. The International Journal of Logistics Management. 2017 Nov 13.

[8] DiMaggio J. The Art of Cyberwarfare: An Investigator's Guide to Espionage, Ransomware, and Organized Cybercrime. No Starch Press, 2022 Apr 26.

[9] Ryan M. Ransomware Revolution: The Rise of a Prodigious Cyber Threat. Berlin/Heidelberg, Germany: Springer, 2021 Feb 24.

[10] Russo L, Binaschi F, De Angelis A, Armando A, Henauer M, Rigoni A. Cybersecurity exercises: wargaming and red teaming. Next Generation CERTs. 2019 Sep 25, 54:44.

[11] Mawgoud AA, Taha MH, Khalifa NE. Security threats of social internet of things in the higher education environment. Toward Social Internet of Things (SIoT): Enabling Technologies, Architectures and Applications: Emerging Technologies for Connected and Smart Social Objects. 2020:151-71.

[12] Tucker K, Bulim J, Koch G, North MM. Internet industry: A perspective review through internet of things and internet of everything. International Management Review. 2018, 14(2):26.

[13] Nyangaresi VO. Extended Chebyshev Chaotic Map Based Message Verification Protocol for Wireless Surveillance Systems. InComputer Vision and Robotics: Proceedings of CVR 2022 2023 Apr 28 (pp. 503-516). Singapore: Springer Nature Singapore.

[14] Klimburg-Witjes N, Wentland A. Hacking humans? Social Engineering and the construction of the "deficient user" in cybersecurity discourses. Science, Technology, & Human Values. 2021 Nov, 46(6):1316-39.

[15] Schaab P, Beckers K, Pape S. Social engineering defence mechanisms and counteracting training strategies. Information & Computer Security. 2017 Jun 12.

[16] Salahdine F, Kaabouch N. Social engineering attacks: A survey. Future Internet. 2019 Apr 2, 11(4):89.

[17] Siddiqi MA, Pak W, Siddiqi MA. A study on the psychology of social engineering-based cyberattacks and existing countermeasures. Applied Sciences. 2022 Jun 14, 12(12):6042.

[18] Hussien ZA, Abdulmalik HA, Hussain MA, Nyangaresi VO, Ma J, Abduljabbar ZA, Abduljaleel IQ. Lightweight Integrity Preserving Scheme for Secure Data Exchange in Cloud-Based IoT Systems. Applied Sciences. 2023 Jan, 13(2):691.

[19] Suryateja PS. Threats and vulnerabilities of cloud computing: a review. International Journal of Computer Sciences and Engineering. 2018 Mar, 6(3):297-302.

[20] Qazi FA. Insecure Application Programming Interfaces (APIs) in Zero-Trust Networks (Doctoral dissertation, Capitol Technology University).

[21] Girasa R, Scalabrini GJ. Regulation of Innovative Technologies: Blockchain, Artificial Intelligence and Quantum Computing. Springer Nature, 2022 Jul 19.

[22] Abuarqoub A, Abuarqoub S, Alzu'bi A, Muthanna A. The Impact of Quantum Computing on Security in Emerging Technologies. InThe 5th International Conference on Future Networks & Distributed Systems 2021 Dec 15 (pp. 171-176).

[23] Al Sibahee MA, Ma J, Nyangaresi VO, Abduljabbar ZA. Efficient Extreme Gradient Boosting Based Algorithm for QoS Optimization in Inter-Radio Access Technology Handoffs. In2022 International Congress on Human-Computer Interaction, Optimization and Robotic Applications (HORA) 2022 Jun 9 (pp. 1-6). IEEE.

[24] Pethers B, Bello A. Role of Attention and Design Cues for Influencing Cyber-Sextortion Using Social Engineering and Phishing Attacks. Future Internet. 2023 Jan, 15(1):29.

[25] Al-Khateeb M, Al-Mousa M, Al-Sherideh A, Almajali D, Asassfeha M, Khafajeh H. Awareness model for minimizing the effects of social engineering attacks in web applications. International Journal of Data and Network Science. 2023, 7(2):791-800.

[26] Sharma A, Gupta BB, Singh AK, Saraswat VK. Advanced Persistent Threats (APT): evolution, anatomy, attribution and countermeasures. Journal of Ambient Intelligence and Humanized Computing. 2023 May 6:1-27.

[27] Khalid MN, Al-Kadhimi AA, Singh MM. Recent Developments in Game-Theory Approaches for the Detection and Defense against Advanced Persistent Threats (APTs): A Systematic Review. Mathematics. 2023 Mar 10, 11(6):1353.

[28] Myneni S, Jha K, Sabur A, Agrawal G, Deng Y, Chowdhary A, Huang D. Unraveled—A semi-synthetic dataset for Advanced Persistent Threats. Computer Networks. 2023 May 1, 227:109688.

[29] Said D. Quantum Computing and Machine Learning for Cybersecurity: Distributed Denial of Service (DDoS) Attack Detection on Smart Micro-Grid. Energies. 2023 Apr 20, 16(8):3572.

[30] Nyangaresi VO. Target Tracking Area Selection and Handover Security in Cellular Networks: A Machine Learning Approach. InProceedings of Third International Conference on Sustainable Expert Systems: ICSES 2022 2023 Feb 23 (pp. 797-816). Singapore: Springer Nature Singapore.

[31] Li G, Ren L, Fu Y, Yang Z, Adetola V, Wen J, Zhu Q, Wu T, Candan KS, O'Neill Z. A critical review of cyber-physical security for building automation systems. Annual Reviews in Control. 2023 Mar 9.

[32] Eke CI, Norman AA, Mulenga M. Machine learning approach for detecting and combating bring your own device (BYOD) security threats and attacks: a systematic mapping review. Artificial Intelligence Review. 2023 Jan 17:1-44.

[33] Almarhabi K, Bahaddad A, Alghamdi AM. Security management of BYOD and cloud environment in Saudi Arabia. Alexandria Engineering Journal. 2023 Feb 1, 63:103-14.

[34] Shihepo E, Bhunu-Shava F, Chitauro M. Designing A Real-Time Bring your Own Device Security Awareness Model for Mobile Device Users within Namibian Enterprises. In2023 6th International Conference on Information Systems and Computer Networks (ISCON) 2023 Mar 3 (pp. 1-4). IEEE.

[35] Hu W, Tan Y. Generating adversarial malware examples for black-box attacks based on GAN. InData Mining and Big Data: 7th International Conference, DMBD 2022, Beijing, China, November 21–24, 2022, Proceedings, Part II 2023 Jan 19 (pp. 409-423). Singapore: Springer Nature Singapore.

[36] Abood EW, Abdullah AM, Al Sibahe MA, Abduljabbar ZA, Nyangaresi VO, Kalafy SA, Ghrabta MJ. Audio steganography with enhanced LSB method for securing encrypted text with bit cycling. Bulletin of Electrical Engineering and Informatics. 2022 Feb 1, 11(1):185-94.

[37] Guo J, Guo H. Real-Time Risk Detection Method and Protection Strategy for Intelligent Ship Network Security Based on Cloud Computing. Symmetry. 2023 Apr 27, 15(5):988.

[38] Guo R, Tafti A, Subramanyam R. Internal IT modularity, firm size, and adoption of cloud computing. Electronic Commerce Research. 2023 Apr 14:1-30.

[39] Anjum M, Singhal S, Kapur PK, Khatri SK, Panwar S. Analysis of vulnerability fixing process in the presence of incorrect patches. Journal of Systems and Software. 2023 Jan 1, 195:111525.

[40] Riegler M, Sametinger J, Vierhauser M, Wimmer M. A model-based mode-switching framework based on security vulnerability scores. Journal of Systems and Software. 2023 Jun 1, 200:111633.

[41] Pal P, Chattopadhyay P, Swarnkar M. Temporal feature aggregation with attention for insider threat detection from activity logs. Expert Systems with Applications. 2023 Aug 15, 224:119925.

[42] Nyangaresi VO, Moundounga AR. Secure data exchange scheme for smart grids. In2021 IEEE 6th International Forum on Research and Technology for Society and Industry (RTSI) 2021 Sep 6 (pp. 312-316). IEEE.

[43] Singh M, Mehtre BM, Sangeetha S, Govindaraju V. User Behaviour based Insider Threat Detection using a Hybrid Learning Approach. Journal of Ambient Intelligence and Humanized Computing. 2023 Mar 5:1-21.

[44] Ayaburi EW. Understanding online information disclosure: examination of data breach victimization experience effect. Information Technology & People. 2023 Jan 13, 36(1):95-114.

[45] Mayer P, Zou Y, Lowens BM, Dyer HA, Le K, Schaub F, Aviv AJ. Awareness, Intention,(In) Action: Individuals' Reactions to Data Breaches. ACM Transactions on Computer-Human Interaction. 2023.

[46] Sohail S, Low KH, Che Man MH, Sivakumar AK. Preliminary Empirical Estimation of Crash Area for Quad-rotor Unmanned Aerial Vehicles (UAV) Crash on Ground Contributing to Third-Party Risks (TPR). InAIAA SCITECH 2023 Forum 2023 (p. 1680).

[47] Cole T. How are financial institutions enabling online fraud? A developmental online financial fraud policy review. Journal of Financial Crime. 2023 Jan 17(ahead-of-print).

[48] Hussain MA, Hussien ZA, Abduljabbar ZA, Ma J, Al Sibahee MA, Hussain SA, Nyangaresi VO, Jiao X. Provably throttling SQLI using an enciphering query and secure matching. Egyptian Informatics Journal. 2022 Dec 1, 23(4):145-62.

[49] Goodell JW, Corbet S. Commodity market exposure to energy-firm distress: Evidence from the Colonial Pipeline ransomware attack. Finance Research Letters. 2023 Jan 1, 51:103329.

[50] Dudley R, Golden D. The colonial pipeline ransomware hackers had a secret weapon: self-promoting cybersecurity firms. MIT Technology Review and ProPublica. 2021 May.

[51] Brewer R. Ransomware attacks: detection, prevention and cure. Network Security. 2016 Sep 1, 2016(9):5-9.

[52] Shu X, Tian K, Ciambrone A, Yao D. Breaking the target: An analysis of target data breach and lessons learned. arXiv preprint arXiv:1701.04940. 2017 Jan 18.

[53] Manworren N, Letwat J, Daily O. Why you should care about the Target data breach. Business Horizons. 2016 May 1, 59(3):257-66.

[54] Nyangaresi VO. Masked Symmetric Key Encrypted Verification Codes for Secure Authentication in Smart Grid Networks. In2022 4th Global Power, Energy and Communication Conference (GPECOM) 2022 Jun 14 (pp. 427-432). IEEE.

[55] Kshetri N. Economics of supply chain cyberattacks. IT professional. 2022 Jun 30, 24(3):96-100.

[56] Huddleston J, Ji P, Bhunia S, Cogan J. How VMware Exploits Contributed to SolarWinds Supply-chain Attack. In2021 International Conference on Computational Science and Computational Intelligence (CSCI) 2021 Dec 15 (pp. 760-765). IEEE.

[57] Martínez J, Durán JM. Software supply chain attacks, a threat to global cybersecurity: SolarWinds' case study. International Journal of Safety and Security Engineering, vol. 2021 Oct, 11(5):537-45.

[58] Shulkitas K. The Sony Pictures Hack: The Government's Role, National Security, and the Way Ahead. Naval War College Newport United States, 2018 May 3.

[59] Horton N, DeSimone A. Sony's Nightmare before Christmas: The 2014 North Korean Cyber Attack on Sony and Lessons for US Government Actions in Cyberspace. JHUAPL Laurel United States, 2018 Feb 1.

[60] Alsamhi SH, Shvetsov AV, Kumar S, Shvetsova SV, Alhartomi MA, Hawbani A, Rajput NS, Srivastava S, Saif A, Nyangaresi VO. UAV computing-assisted search and rescue mission framework for disaster and harsh environment mitigation. Drones. 2022 Jun 22, 6(7):154.

[61] Hinds J, Williams EJ, Joinson AN. "It wouldn't happen to me": Privacy concerns and perspectives following the Cambridge Analytica scandal. International Journal of Human-Computer Studies. 2020 Nov 1, 143:102498.

[62] Heawood J. Pseudo-public political speech: Democratic implications of the Cambridge Analytica scandal. Information polity. 2018 Jan 1, 23(4):429-34.

[63] González F, Yu Y, Figueroa A, López C, Aragon C. Global reactions to the cambridge analytica scandal: A cross-language social media study. InCompanion Proceedings of the 2019 world wide web conference 2019 May 13 (pp. 799-806).

[64] Kumar P, Govindaraj V, Erturk VS, Nisar KS, Inc M. Fractional mathematical modeling of the Stuxnet virus along with an optimal control problem. Ain Shams Engineering Journal. 2023 Jul 1, 14(7):102004.

[65] Nyangaresi VO, Ogundoyin SO. Certificate based authentication scheme for smart homes. In2021 3rd Global Power, Energy and Communication Conference (GPECOM) 2021 Oct 5 (pp. 202-207). IEEE.

[66] Pavlović ZG. Innovative Model Of E-Business Increasing Safety On High-Speed Railways. In2023 22nd International Symposium INFOTEH-JAHORINA (INFOTEH) 2023 Mar 15 (pp. 1-6). IEEE.

[67] Alsabbagh W, Amogbonjaye S, Urrego D, Langendörfer P. A Stealthy False Command Injection Attack on Modbus based SCADA Systems. In2023 IEEE 20th Consumer Communications & Networking Conference (CCNC) 2023 Jan 8 (pp. 1-9). IEEE.

[68] Graham J, Hieb J, Naber J. Improving cybersecurity for industrial control systems. In2016 ieee 25th international symposium on industrial electronics (isie) 2016 Jun 8 (pp. 618-623). IEEE.

[69] Miller T, Staves A, Maesschalck S, Sturdee M, Green B. Looking back to look forward: Lessons learnt from cyber-attacks on industrial control systems. International Journal of Critical Infrastructure Protection. 2021 Dec 1, 35:100464.

[70] Al Sibahee MA, Nyangaresi VO, Ma J, Abduljabbar ZA. Stochastic Security Ephemeral Generation Protocol for 5G Enabled Internet of Things. InIoT as a Service: 7th EAI International Conference, IoTaaS 2021, Sydney, Australia, December 13–14, 2021, Proceedings 2022 Jul 8 (pp. 3-18). Cham: Springer International Publishing.

[71] Hemsley KE, Fisher E. History of industrial control system cyber incidents. Idaho National Lab.(INL), Idaho Falls, ID (United States), 2018 Dec 31.

[72] Möller DP. Intrusion detection and prevention. InGuide to Cybersecurity in Digital Transformation: Trends, Methods, Technologies, Applications and Best Practices 2023 Apr 19 (pp. 131-179). Cham: Springer Nature Switzerland.

[73] Javadpour A, Pinto P, Ja'fari F, Zhang W. DMAIDPS: a distributed multi-agent intrusion detection and prevention system for cloud IoT environments. Cluster Computing. 2023 Feb, 26(1):367-84.

[74] Lima M, Lima R, Lins F, Bonfim M. Beholder–A CEP-based intrusion detection and prevention systems for IoT environments. Computers & Security. 2022 Sep 1, 120:102824.

[75] Nyangaresi VO, Morsy MA. Towards privacy preservation in internet of drones. In2021 IEEE 6th International Forum on Research and Technology for Society and Industry (RTSI) 2021 Sep 6 (pp. 306-311). IEEE.

[76] Li D, Wu JM, Liang ZH, Li LY, Dong X, Chen SK, Fu T, Wang XL, Wang YZ, Song F. Sophisticated yet Convenient Information Encryption/Decryption Based on Synergistically Time-/Temperature-Resolved Photonic Inks. Advanced Science. 2023 Feb, 10(5):2206290.

[77] Fu J, Feng J, Shi B, Zhou Y, Xue C, Zhang M, Qi Y, Wen W, Wu J. Grading patterning perovskite nanocrystal-polymer composite films for robust multilevel information encryption and decryption. Chemical Engineering Journal. 2023 Jan 1, 451:138240.

[78] Gao S, Wu R, Wang X, Wang J, Li Q, Wang C, Tang X. A 3D model encryption scheme based on a cascaded chaotic system. Signal Processing. 2023 Jan 1, 202:108745.

[79] Wang WT, Sun JY, Wang G, Zhang H. Fisher-Yates scrambling algorithm combined with S-box color image encryption technology based on 3D-SCCM chaotic system. Multimedia Tools and Applications. 2023 Apr 28:1-26.

[80] Nyakomitta SP, Omollo V. Biometric-Based Authentication Model for E-Card Payment Technology. IOSR Journal of Computer Engineering (IOSRJCE). 2014, 16(5):137-44.

[81] Muhammad Z, Amjad F, Iqbal Z, Javed AR, Gadekallu TR. Circumventing Google Play vetting policies: A stealthy cyberattack that uses incremental updates to breach privacy. Journal of Ambient Intelligence and Humanized Computing. 2023 Jan 28:1-0.

[82] Rahali A, Akhloufi MA. MalBERTv2: Code Aware BERT-Based Model for Malware Identification. Big Data and Cognitive Computing. 2023 Mar 24, 7(2):60.

[83] Trabelsi R, Fersi G, Jmaiel M. Virtual Private Network Blockchain-based Dynamic Access Control Solution for Inter-organisational Large Scale IoT Networks. InRisks and Security of Internet and Systems: 17th International Conference, CRiSIS 2022, Sousse, Tunisia, December 7-9, 2022, Revised Selected Papers 2023 May 14 (pp. 207-222). Cham: Springer Nature Switzerland.

[84] Naas M, Fesl J. A novel dataset for encrypted virtual private network traffic analysis. Data in Brief. 2023 Apr 1, 47:108945.

[85] Nyangaresi VO. Privacy Preserving Three-factor Authentication Protocol for Secure Message Forwarding in Wireless Body Area Networks. Ad Hoc Networks. 2023 Apr 1, 142:103117.

[86] Liu A, Alqazzaz A, Ming H, Dharmalingam B. Iotverif: Automatic verification of SSL/TLS certificate for IoT applications. IEEE Access. 2019 Dec 24, 9:27038-50.

[87] Zarate M. Technology Acceptance for Protecting Healthcare Data in the Presence of Rising Secure Sockets Layer/Transport Layer Security Communications: A Generic Qualitative Inquiry (Doctoral dissertation, Capella University).

[88] Dastres R, Soori M. Secure socket layer (SSL) in the network and web security. International Journal of Computer and Information Engineering. 2020 Nov 5, 14(10):330-3.

[89] Kong L, Zhou Y, Huang G, Wang H. Fine-grained Identification for SSL/TLS Packets. International Journal of Network Security. 2020 Nov 1, 22(6):975-80.

[90] González-Granadillo G, González-Zarzosa S, Diaz R. Security information and event management (SIEM): analysis, trends, and usage in critical infrastructures. Sensors. 2021 Jul 12, 21(14):4759.

[91] Omollo VN, Musyoki S. Blue bugging Java Enabled Phones via Bluetooth Protocol Stack Flaws. International Journal of Computer and Communication System Engineering. 2015 Jun 9, 2 (4):608-613.

[92] Humayun M, Niazi M, Jhanjhi NZ, Mahmood S, Alshayeb M. Toward a readiness model for secure software coding. Software: Practice and Experience. 2023 Apr, 53(4):1013-35.

[93] Georgiou T, Baillie L, Chatzifoti O, Chan SC. Future forums: A methodology for exploring, gamifying, and raising security awareness of code-citizens. International Journal of Human-Computer Studies. 2023 Jan 1, 169:102930.

[94] Larios-Vargas E, Elazhary O, Yousefi S, Lowlind D, Vliek ML, Storey MA. DASP: A Framework for Driving the Adoption of Software Security Practices. IEEE Transactions on Software Engineering. 2023 Jan 10.

[95] Collins J, Ford V. Teaching by Practice: Shaping Secure Coding Mentalities through Cybersecurity CTFs. Journal of Cybersecurity Education, Research and Practice. 2023, 2022(2):9.

[96] Bauböck R, Permoser JM. Sanctuary, firewalls, regularisation: three inclusive responses to the presence of irregular migrants. Journal of Ethnic and Migration Studies. 2023 Apr 12:1-8.

[97] Nyangaresi VO. A Formally Verified Authentication Scheme for mmWave Heterogeneous Networks. Inthe 6th International Conference on Combinatorics, Cryptography, Computer Science and Computation (605-612) 2021.

[98] Liang H, Li X, Xiao D, Liu J, Zhou Y, Wang A, Li J. Generative Pre-trained Transformer-Based Reinforcement Learning for Testing Web Application Firewalls. IEEE Transactions on Dependable and Secure Computing. 2023 Mar 6.

[99] Zhao Y, Pang Y, Ke X, Wang B, Zhu G, Cao M. A metaverse-oriented CP-ABE scheme with cryptographic reverse firewall. Future Generation Computer Systems. 2023 Apr 29.

[100] Hussein MA. A Proposed Multi-Layer Firewall to Improve the Security of Software Defined Networks. International Journal of Interactive Mobile Technologies. 2023 Jan 15, 17(2).

[101] Ometov A, Bezzateev S, Mäkitalo N, Andreev S, Mikkonen T, Koucheryavy Y. Multi-factor authentication: A survey. Cryptography. 2018 Jan 5, 2(1):1.

[102] Abduljabbar ZA, Omollo Nyangaresi V, Al Sibahee MA, Ghrabat MJ, Ma J, Qays Abduljaleel I, Aldarwish AJ. Session-Dependent Token-Based Payload Enciphering Scheme for Integrity Enhancements in Wireless Networks. Journal of Sensor and Actuator Networks. 2022 Sep 19, 11(3):55.

[103] Wahab AA, Hou D, Schuckers S. A User Study of Keystroke Dynamics as Second Factor in Web MFA. InProceedings of the Thirteenth ACM Conference on Data and Application Security and Privacy 2023 Apr 24 (pp. 61-72).

[104] Zheng J, Okamura H, Dohi T. Pull-Type Security Patch Management in Intrusion Tolerant Systems: Modeling and Analysis. InMaintenance Management-Current Challenges, New Developments, and Future Directions 2023 Apr 5. IntechOpen.

[105] Alabi OM. The Hyperautomation of Software Security Patch Management in Enterprise Networks: A Case Study at the Central Bank of Ireland (Doctoral dissertation, Dublin, National College of Ireland).

[106] Mori K, Yamazaki K, Takei C, Oshizaka T, Takeuchi I, Miyaji K, Todo H, Itakura S, Sugibayashi K. Remote-controllable dosage management through a wearable iontophoretic patch utilizing a cell phone. Journal of Controlled Release. 2023 Mar 1, 355:1-6.

[107] Nyangaresi VO, Petrovic N. Efficient PUF based authentication protocol for internet of drones. In2021 International Telecommunications Conference (ITC-Egypt) 2021 Jul 13 (pp. 1-4). IEEE.

[108] Kaloudi N, Li J. The ai-based cyber threat landscape: A survey. ACM Computing Surveys (CSUR). 2020 Feb 5, 53(1):1-34.

[109] Achar S. Cloud Computing Security for Multi-Cloud Service Providers: Controls and Techniques in our Modern Threat Landscape. International Journal of Computer and Systems Engineering. 2022 Sep 13, 16(9):379-84.

[110] Singh UK, Joshi C, Kanellopoulos D. A framework for zero-day vulnerabilities detection and prioritization. Journal of Information Security and Applications. 2019 Jun 1, 46:164-72.

[111] Al-Rushdan H, Shurman M, Alnabelsi SH, Althebyan Q. Zero-day attack detection and prevention in software-defined networks. In2019 international arab conference on information technology (acit) 2019 Dec 3 (pp. 278-282). IEEE.

[112] Nyakomitta PS, Nyangaresi VO, Ogara SO. Efficient authentication algorithm for secure remote access in wireless sensor networks. Journal of Computer Science Research. 2021 Aug, 3(4):43-50.

[113] Vij C, Saini H. Intrusion Detection Systems: Conceptual Study and Review. In2021 6th International Conference on Signal Processing, Computing and Control (ISPCC) 2021 Oct 7 (pp. 694-700). IEEE.

[114] Yi L, Yin M, Darbandi M. A deep and systematic review of the intrusion detection systems in the fog environment. Transactions on Emerging Telecommunications Technologies. 2023 Jan, 34(1):e4632.

[115] Mehmood M, Amin R, Muslam MM, Xie J, Aldabbas H. Privilege Escalation Attack Detection and Mitigation in Cloud using Machine Learning. IEEE Access. 2023 May 8.

[116] Okeke RI, Eiza MH. The Application of role-based framework in preventing internal identity theft related crimes: A qualitative case study of UK retail companies. Information Systems Frontiers. 2023 Apr, 25(2):451-72.

[117] Qiu Z, Ma J, Zhang H, Al Sibahee MA, Abduljabbar ZA, Nyangaresi VO. Concurrent pipeline rendering scheme based on GPU multi-queue and partitioning images. InInternational Conference on Optics and Machine Vision (ICOMV 2023) 2023 Apr 14 (Vol. 12634, pp. 143-149). SPIE.

[118] Chen H, Zhang Y, Zhang S, Lyu T. Exploring the role of gamified information security education systems on information security awareness and protection behavioral intention. Education and Information Technologies. 2023 May 3:1-34.

[119] Lowry PB, Dinev T, Willison R. Why security and privacy research lies at the centre of the information systems (IS) artefact: Proposing a bold research agenda. European Journal of Information Systems. 2017 Nov, 26:546-63.

[120] Wong LW, Lee VH, Tan GW, Ooi KB, Sohal A. The role of cybersecurity and policy awareness in shifting employee compliance attitudes: Building supply chain capabilities. International Journal of Information Management. 2022 Oct 1, 66:102520.

[121] Silic M, Lowry PB. Using design-science based gamification to improve organizational security training and compliance. Journal of management information systems. 2020 Jan 2, 37(1):129-61.

[122] Mohammad Z, Nyangaresi V, Abusukhon A. On the Security of the Standardized MQV Protocol and Its Based Evolution Protocols. In2021 International Conference on Information Technology (ICIT) 2021 Jul 14 (pp. 320-325). IEEE.

[123] Van Zoonen L. Privacy concerns in smart cities. Government Information Quarterly. 2016 Jul 1, 33(3):472-80.

[124] Yao Y, Basdeo JR, Kaushik S, Wang Y. Defending my castle: A co-design study of privacy mechanisms for smart homes. InProceedings of the 2019 chi conference on human factors in computing systems 2019 May 2 (pp. 1-12).

[125] Cilliers L. Wearable devices in healthcare: Privacy and information security issues. Health information management journal. 2020 May, 49(2-3):150-6.

[126] Tyagi AK, Rekha G, Sreenath N. Beyond the hype: Internet of things concepts, security and privacy concerns. InAdvances in Decision Sciences, Image Processing, Security and Computer Vision: International Conference on Emerging Trends in Engineering (ICETE), Vol. 1 2020 (pp. 393-407). Springer International Publishing.

[127] Nyangaresi VO, Alsamhi SH. Towards secure traffic signaling in smart grids. In2021 3rd Global Power, Energy and Communication Conference (GPECOM) 2021 Oct 5 (pp. 196-201). IEEE.

[128] Stellios I, Kotzanikolaou P, Psarakis M. Advanced persistent threats and zero-day exploits in industrial Internet of Things. Security and Privacy Trends in the Industrial Internet of Things. 2019:47-68.

[129] Quintero-Bonilla S, Martín del Rey A. A new proposal on the advanced persistent threat: A survey. Applied Sciences. 2020 Jun 3, 10(11):3874.

[130] Alshamrani A, Myneni S, Chowdhary A, Huang D. A survey on advanced persistent threats: Techniques, solutions, challenges, and research opportunities. IEEE Communications Surveys & Tutorials. 2019 Jan 9, 21(2):1851-77.

[131] Chen J, Su C, Yeh KH, Yung M. Special issue on advanced persistent threat. Future Generation Computer Systems. 2018 Feb 1, 79:243-6.

[132] Honi DG, Ali AH, Abduljabbar ZA, Ma J, Nyangaresi VO, Mutlaq KA, Umran SM. Towards Fast Edge Detection Approach for Industrial Products. In2022 IEEE 21st International Conference on Ubiquitous Computing and Communications (IUCC/CIT/DSCI/SmartCNS) 2022 Dec 19 (pp. 239-244). IEEE.

[133] Saxena N, Hayes E, Bertino E, Ojo P, Choo KK, Burnap P. Impact and key challenges of insider threats on organizations and critical businesses. Electronics. 2020 Sep 7, 9(9):1460.

[134] Raval MS, Gandhi R, Chaudhary S. Insider threat detection: machine learning way. Versatile Cybersecurity. 2018:19-53.

[135] Alsowail RA, Al-Shehari T. Empirical detection techniques of insider threat incidents. IEEE Access. 2020 Apr 23, 8:78385-402.

[136] Walker-Roberts S, Hammoudeh M, Dehghantanha A. A systematic review of the availability and efficacy of countermeasures to internal threats in healthcare critical infrastructure. IEEE Access. 2018 Mar 20, 6:25167-77.

[137] Nyangaresi VO, Mohammad Z. Session Key Agreement Protocol for Secure D2D Communication. InThe Fifth International Conference on Safety and Security with IoT: SaSeIoT 2021 2022 Jun 12 (pp. 81-99). Cham: Springer International Publishing.

[138] Rekha S, Thirupathi L, Renikunta S, Gangula R. Study of security issues and solutions in Internet of Things (IoT). Materials Today: Proceedings. 2023 Jan 1, 80:3554-9.

[139] Sadique KM, Rahmani R, Johannesson P. DIdM-EIoTD: Distributed Identity Management for Edge Internet of Things (IoT) Devices. Sensors. 2023 Apr 17, 23(8):4046.

[140] Mukati N, Namdev N, Dilip R, Hemalatha N, Dhiman V, Sahu B. Healthcare assistance to COVID-19 patient using internet of things (IoT) enabled technologies. Materials today: proceedings. 2023 Jan 1, 80:3777-81.

[141] Gupta M, Singh VP, Gupta KK, Shukla PK. An efficient image encryption technique based on two-level security for internet of things. Multimedia Tools and Applications. 2023 Feb, 82(4):5091-111.

[142] Abduljabbar ZA, Nyangaresi VO, Ma J, Al Sibahee MA, Khalefa MS, Honi DG. MAC-Based Symmetric Key Protocol for Secure Traffic Forwarding in Drones. InFuture Access Enablers for Ubiquitous and Intelligent Infrastructures: 6th EAI International Conference, FABULOUS 2022, Virtual Event, May 4, 2022, Proceedings 2022 Sep 18 (pp. 16-36). Cham: Springer International Publishing.

[143] Stewart J, Sprivulis P, Dwivedi G. Artificial intelligence and machine learning in emergency medicine. Emergency Medicine Australasia. 2018 Dec, 30(6):870-4.

[144] Ahmad T, Zhang D, Huang C, Zhang H, Dai N, Song Y, Chen H. Artificial intelligence in sustainable energy industry: Status Quo, challenges and opportunities. Journal of Cleaner Production. 2021 Mar 20, 289:125834.

[145] M. Bublitz F, Oetomo A, S. Sahu K, Kuang A, X. Fadrique L, E. Velmovitsky P, M. Nobrega R, P. Morita P. Disruptive technologies for environment and health research: an overview of artificial intelligence, blockchain, and internet of things. International journal of environmental research and public health. 2019 Oct, 16(20):3847.

[146] Krishnam NP, Ashraf MS, Rajagopal BR, Vats P, Chakravarthy DS, Rafi SM. Analysis Of Current Trends, Advances And Challenges Of Machine Learning (Ml) And Knowledge Extraction: From Ml To Explainable AI. Industry Qualifications The Institute of Administrative Management UK. 2022 May, 58:54-62.

[147] Ghrabat MJ, Hussien ZA, Khalefa MS, Abduljabba ZA, Nyangaresi VO, Al Sibahee MA, Abood EW. Fully automated model on breast cancer classification using deep learning classifiers. Indonesian Journal of Electrical Engineering and Computer Science. 2022 Oct, 28(1):183-91.

[148] Pramod D. Privacy-preserving techniques in recommender systems: state-of-the-art review and future research agenda. Data Technologies and Applications. 2023 Mar 17, 57(1):32-55.

[149] Liu M, Zhang Z, Chai W, Wang B. Privacy-preserving COVID-19 contact tracing solution based on blockchain. Computer Standards & Interfaces. 2023 Jan 1, 83:103643.

[150] Sousa S, Kern R. How to keep text private? A systematic review of deep learning methods for privacy-preserving natural language processing. Artificial Intelligence Review. 2023 Feb, 56(2):1427-92.

[151] Hiwale M, Walambe R, Potdar V, Kotecha K. A systematic review of privacy-preserving methods deployed with blockchain and federated learning for the telemedicine. Healthcare Analytics. 2023 May 5:100192.

[152] Nyangaresi VO, Ma J. A Formally Verified Message Validation Protocol for Intelligent IoT E-Health Systems. In2022 IEEE World Conference on Applied Intelligence and Computing (AIC) 2022 Jun 17 (pp. 416-422). IEEE.

[153] Sharma S, Chen K, Sheth A. Toward practical privacy-preserving analytics for IoT and cloud-based healthcare systems. IEEE Internet Computing. 2018 Jan 16, 22(2):42-51.

[154] Burkhalter L, Küchler N, Viand A, Shafagh H, Hithnawi A. Zeph: Cryptographic Enforcement of End-to-End Data Privacy. InOSDI 2021 Jul 14 (pp. 387-404).

[155] Mukherjee S, Gupta S, Rawlley O, Jain S. Leveraging big data analytics in 5G-enabled IoT and industrial IoT for the development of sustainable smart cities. Transactions on Emerging Telecommunications Technologies. 2022 Dec, 33(12):e4618.

[156] Leng J, Zhou M, Zhao JL, Huang Y, Bian Y. Blockchain security: A survey of techniques and research directions. IEEE Transactions on Services Computing. 2020 Nov 25, 15(4):2490-510.

[157] Abood EW, Hussien ZA, Kawi HA, Abduljabbar ZA, Nyangaresi VO, Ma J, Al Sibahee MA, Kalafy A, Ahmad S. Provably secure and efficient audio compression based on compressive sensing. International Journal of Electrical & Computer Engineering (2088-8708). 2023 Feb 1, 13(1).

[158] Shaikh FA, Siponen M. Information security risk assessments following cybersecurity breaches: The mediating role of top management attention to cybersecurity. Computers & Security. 2023 Jan 1, 124:102974.

[159] Chowdhury NH, Adam MT, Teubner T. Time pressure in human cybersecurity behavior: Theoretical framework and countermeasures. Computers & Security. 2020 Oct 1, 97:101931.

[160] Hopcraft R, Tam K, Misas JD, Moara-Nkwe K, Jones K. Developing a Maritime Cyber Safety Culture: Improving Safety of Operations. Maritime Technology and Research. 2023, 5(1).

[161] Guarascio M, Cassavia N, Pisani FS, Manco G. Boosting cyber-threat intelligence via collaborative intrusion detection. Future Generation Computer Systems. 2022 Oct 1, 135:30-43.

[162] Nyangaresi VO. Provably Secure Pseudonyms based Authentication Protocol for Wearable Ubiquitous Computing Environment. In2022 International Conference on Inventive Computation Technologies (ICICT) 2022 Jul 20 (pp. 1-6). IEEE.

[163] Jasper SE. US cyber threat intelligence sharing frameworks. International Journal of Intelligence and CounterIntelligence. 2017 Jan 2, 30(1):53-65.

[164] Tounsi W, Rais H. A survey on technical threat intelligence in the age of sophisticated cyber attacks. Computers & security. 2018 Jan 1, 72:212-33.

[165] Wagner TD, Mahbub K, Palomar E, Abdallah AE. Cyber threat intelligence sharing: Survey and research directions. Computers & Security. 2019 Nov 1, 87:101589.

[166] Homan D, Shiel I, Thorpe C. A new network model for cyber threat intelligence sharing using blockchain technology. In2019 10th IFIP International Conference on New Technologies, Mobility and Security (NTMS) 2019 Jun 24 (pp. 1-6). IEEE.

[167] Abduljaleel IQ, Abduljabbar ZA, Al Sibahee MA, Ghrabat MJ, Ma J, Nyangaresi VO. A Lightweight Hybrid Scheme for Hiding Text Messages in Colour Images Using LSB, Lah Transform and Chaotic Techniques. Journal of Sensor and Actuator Networks. 2022 Dec, 11(4):66.

[168] Kraus VL. Adaptive Incident Response Plans for Cyber Resilience in Small and Medium Enterprises: Analysis and Increase of Cyber Security for a Small Enterprise by Designing an Incident Response Pl. InHandbook of Research on Cybersecurity Risk in Contemporary Business Systems 2023 (pp. 1-32). IGI Global.

[169] Bitzer M, Häckel B, Leuthe D, Ott J, Stahl B, Strobel J. Managing the Inevitable–A Maturity Model to Establish Incident Response Management Capabilities. Computers & Security. 2023 Feb 1, 125:103050.

[170] Zaki Rashed AN, Ahammad SH, Daher MG, Sorathiya V, Siddique A, Asaduzzaman S, Rehana H, Dutta N, Patel SK, Nyangaresi VO, Jibon RH. Signal propagation parameters estimation through designed multi layer fibre with higher dominant modes using OptiFibre simulation. Journal of Optical Communications. 2022 Jun 23(0).

[171] Batmetan JR, Mamonto J, Muyu R, Poluakan C. Evaluation of Incident Management in University using IT Infrastructure Library Framework. International Journal of Information Technology and Education. 2022 Mar 24, 1(2):103-8.

[172] Darko J, Park H. A Proactive Dynamic-Distributed Constraint Optimization Framework for Unmanned Aerial and Ground Vehicles in Traffic Incident Management. In2021 6th International Conference on Intelligent Transportation Engineering (ICITE 2021) 2022 Jun 1 (pp. 708-721). Singapore: Springer Nature Singapore.

[173] van der Kleij R, Schraagen JM, Cadet B, Young H. Developing decision support for cybersecurity threat and incident managers. Computers & Security. 2022 Feb 1, 113:102535.