Journal of Frontiers in Multidisciplinary Research

Security Challenges in Embedded Systems: A Review of USA and African Perspectives

Ojong Felix Enow [1*], Ebimor Yinka Gbabo [2], Andrew Tochukwu Ofoedu [3], Possible Emeka Chima [4]
[1] Independent Researcher, Buea, Cameroon
[2] National Grid, UK
[3] Shell Nigeria Exploration and Production Company Lagos, Nigeria
[4] Independent Researcher, Nigeria

* Corresponding Author: **Ojong Felix Enow**

Article Info

E-ISSN: 3050-9726
P-ISSN: 3050-9718
Volume: 04
Issue: 01
January-June 2023
Received: 22-03-2023
Accepted: 25-04-2023
Published: 06-06-2023
Page No: 458-464

Abstract
This Review provides a glimpse into the security challenges faced by embedded systems, with a focus on the divergent perspectives of the United States (USA) and Africa. Embedded systems, integral to diverse applications from industrial automation to IoT devices, are susceptible to an array of security threats. In the USA, a developed technological landscape presents challenges like sophisticated cyberattacks, potential espionage, and the growing risk of supply chain vulnerabilities. The review delves into the advanced cybersecurity measures implemented in the USA and explores ongoing efforts to mitigate emerging threats. Contrastingly, the African perspective introduces unique challenges stemming from the digital divide, varying technological infrastructures, and a growing dependence on embedded systems for critical services. The review sheds light on the prevalence of cyber threats in African nations, including malware attacks, data breaches, and the exploitation of vulnerabilities in embedded systems. Additionally, it explores the socioeconomic implications of inadequate security measures, emphasizing the need for region-specific strategies to bolster embedded system security. The Review underscores the importance of a comprehensive approach to address security challenges in embedded systems, encompassing robust cybersecurity frameworks, international collaboration, and tailored solutions to meet the distinct needs of both the USA and Africa. As technological landscapes continue to evolve, understanding the nuanced perspectives on security challenges becomes imperative for fostering a secure and resilient global embedded systems ecosystem.

DOI: https://doi.org/10.54660/.JFMR.2023.4.1.458-464

Keywords: Security, Challenges, Embedded System, Perspectives, Digital

1. Introduction

Embedded systems, the silent backbone of modern technological infrastructures, play a pivotal and often unnoticed role in powering diverse sectors globally (Biygautane *et al*., 2020). From industrial automation and healthcare to smart devices and critical infrastructure, these compact computing devices are embedded into the fabric of our daily lives (Munirathinam,2020). Their ability to execute dedicated functions with precision has revolutionized how tasks are automated, monitored, and controlled, contributing to unprecedented advancements across industries.

As embedded systems become increasingly intertwined with critical operations, their vulnerability to cyber threats becomes a growing concern (Yaacoub *et al*., 2020). Cybersecurity, once a secondary consideration, has now become paramount in safeguarding these systems from malicious actors seeking unauthorized access, data breaches, and potential disruptions (Safitra *et al*., 2023). The interconnectedness of embedded systems with the broader digital landscape accentuates the need for robust cybersecurity measures to ensure the integrity, confidentiality, and availability of the services they underpin.

This review aims to undertake a comprehensive examination of the security challenges faced by embedded systems, casting a comparative lens on the distinct perspectives of two contrasting regions—the United States (USA) and African nations. By exploring the intricacies of cybersecurity in both the technologically advanced landscape of the USA and the emerging digital ecosystems of African nations, this analysis seeks to unearth commonalities, differences, and potential collaborative strategies

to fortify embedded systems on a global scale. As technology becomes an increasingly integral part of societal progress, the insights derived from this comparative analysis will contribute to the formulation of nuanced and effective cybersecurity approaches tailored to the specific needs of these diverse regions (Zhangand Kim,2023).

2. Security Challenges in Embedded Systems: USA

In the rapidly advancing landscape of technology, embedded systems serve as the backbone of critical infrastructure, industrial operations, and national security (Mishraand Singh,2023). However, with their pervasive integration, these systems become lucrative targets for cyber adversaries, posing significant security challenges. This comprehensive analysis delves into the security challenges faced by embedded systems in the United States (USA), examining advanced cyber threats, vulnerabilities within the supply chain, and the profound implications for national security.

Embedded systems, due to their ubiquity, have become prime targets for sophisticated cyberattacks. Notable examples include: Widely recognized as the first digital weapon, Stuxnet specifically targeted supervisory control and data acquisition (SCADA) systems, which often incorporate embedded systems (Pliatsios *et al*., 2020). It disrupted Iran's nuclear program, highlighting the potential for cyber threats to manipulate physical processes. While not directly targeting embedded systems, Mirai infected and exploited vulnerable IoT devices, many of which incorporate embedded systems (Jiang *et al*., 2020). The attack resulted in widespread disruption of internet services through massive distributed denial-of-service (DDoS) attacks.

Cyberattacks on embedded systems can have severe consequences, particularly when integrated into critical infrastructure (Lehto,2022). The impact extends to: Attacks on embedded systems within power grids can lead to service disruptions, affecting millions and posing a threat to national energy security. Embedded systems in control systems of transportation networks are vulnerable, potentially resulting in accidents or disruptions with cascading effects on national mobility (Vivek and Conner, 2022). Compromised embedded systems in communication infrastructure can be exploited to disrupt vital communication channels, impacting emergency services and national defense operations (Mazzolin and Samueli, 2020). The interconnected nature of global supply chains introduces vulnerabilities that can be exploited by malicious actors. Key aspects include:

Many embedded systems rely on components from various suppliers, creating potential points of compromise. Malicious actors may infiltrate the supply chain at any stage, from manufacturing to distribution (Martínez and Durán, 2021). The use of counterfeit or compromised components in the supply chain can introduce vulnerabilities into embedded systems. These components may contain malicious firmware or backdoors, enabling unauthorized access. While not directly impacting embedded systems, the SolarWinds attack demonstrated the vulnerability of the software supply chain (Johnson *et al*., 2023). A compromised software update allowed adversaries access to numerous networks, including those controlling critical infrastructure. Instances of hardware trojans—malicious alterations to hardware during manufacturing—highlight the potential for supply chain manipulation (Halak, 2021; Ukoba and Jen, 2023). Detecting such trojans in embedded systems poses a significant challenge.

Embedded systems are integral to military technologies, including weapon systems, communication networks, and reconnaissance (Lukong *et al*., 2021). A breach in these systems can compromise the effectiveness of national defense strategies. Embedded systems control essential government functions, from emergency services to intelligence operations (Khan *et al*., 2021). Breaches can jeopardize the confidentiality, integrity, and availability of critical information. Recognizing the gravity of national security risks, the USA has implemented various strategies and initiatives: NIST Cybersecurity Framework provides a set of guidelines and best practices to enhance the cybersecurity posture of organizations, including those managing embedded systems (Möller, 2023.). The government collaborates with private entities to strengthen cybersecurity defenses. Initiatives like the National Cybersecurity Center of Excellence (NCCoE) bring together government, industry, and academia to address cybersecurity challenges. The USA has enacted legislation and regulations aimed at enhancing cybersecurity in critical infrastructure (Atkinsand Lawson,2021). For instance, the Cybersecurity and Infrastructure Security Agency (CISA) plays a pivotal role in securing critical infrastructure from cyber threats.

In conclusion, the security challenges in embedded systems within the USA present complex and multifaceted issues with far-reaching implications. The constant evolution of cyber threats demands a proactive approach, involving collaboration between government entities, private sectors, and international stakeholders (Safitra *et al*., 2023). As the reliance on embedded systems continues to grow, securing these technologies is not just a technological imperative but a crucial element in safeguarding national security and the resilience of critical infrastructure.

2.1 Security Challenges in Embedded Systems: Africa

Embedded systems, vital components of technological infrastructures, are experiencing heightened security challenges in the African context (Ukwandu *et al*., 2022). This analysis explores the multifaceted landscape, addressing the digital divide, prevalent cyber threats, and the consequential socioeconomic implications. The unique characteristics of African nations, including the digital divide and diverse technological infrastructures, shape the security challenges faced by embedded systems in the region (Shukla *et al*., 2023). The digital divide refers to the gap between those with and without access to modern information and communication technologies (ICTs). In Africa, this divide is manifested in disparities such as:

A significant portion of the African population lacks reliable access to the internet, hindering the widespread adoption of advanced technologies and increasing the vulnerability of embedded systems (Abiodun *et al*., 2021). Disparities between urban and rural areas contribute to varying levels of technological adoption. Urban centers often have better access to technology, while rural areas may lack basic infrastructure. The diversity of technological infrastructures across African nations contributes to the complexity of cybersecurity challenges: Many African countries rely on legacy systems with outdated software and limited security features, making them susceptible to cyber threats. Limited connectivity in some regions impedes the implementation of robust cybersecurity measures, creating vulnerabilities in the interconnected systems (Djenna *et al*., 2021). Financial constraints often limit investments in cybersecurity

infrastructure, leaving systems inadequately protected against evolving threats.

Malicious software poses a significant threat, targeting embedded systems in sectors such as healthcare, finance, and energy (Aloseel *et al*., 2020). Notable malware includes ransomware and trojans. The compromise of sensitive data is a prevalent concern, affecting industries that rely on embedded systems for data storage and processing. The proliferation of IoT devices, often incorporating embedded systems, introduces vulnerabilities. Inadequate security measures in these devices make them susceptible to exploitation (Eceiza *et al*., 2021).

Real-world examples highlight the impact of cyber threats on embedded systems in Africa: The "Emotet" malware targeted banks in South Africa, compromising financial data and illustrating the vulnerability of critical infrastructure. A healthcare data breach in Nigeria exposed sensitive patient information, emphasizing the need for enhanced security measures in the healthcare sector (Kasten *et al*., 2023). Several African nations have experienced DDoS attacks, disrupting online services and exposing weaknesses in cybersecurity infrastructure.

Inadequate security measures in embedded systems carry significant socioeconomic repercussions: Cyberattacks on critical infrastructure can result in economic losses, affecting industries, businesses, and national economies. Embedded systems control essential public services, and their compromise can lead to disruptions in healthcare, transportation, and utilities, negatively impacting citizens' daily lives (Adeniyi *et al*., 2020).Embedded systems are integral to the functioning of critical services, and their compromised security can threaten socioeconomic stability: Inadequate security in healthcare embedded systems jeopardizes patient data privacy and the integrity of medical services, potentially eroding public trust. Embedded systems in banking and finance are at risk, with potential consequences including fraud, financial instability, and loss of investor confidence (Cheng *et al*., 2021). Embedded systems control energy distribution and production. Cyber threats to these systems can lead to power outages, disrupting industrial operations and daily life.

In conclusion, the security challenges faced by embedded systems in Africa are deeply entwined with the region's unique digital landscape, technological disparities, and socioeconomic considerations. Addressing these challenges requires a holistic approach, encompassing improvements in digital infrastructure, cybersecurity education, and international collaboration (Shillair *et al*., 2022). As African nations strive for technological advancement and economic growth, fortifying the security of embedded systems becomes imperative to ensure sustainable development and safeguard against evolving cyber threats (Gikunda,2023).

2.2 Comparative Analysis

The security challenges confronting embedded systems in the United States (USA) and Africa reflect the complexities of their respective technological, economic, and geopolitical landscapes (Lazardand Youngs,2021). This comparative analysis aims to dissect the nature and intensity of cybersecurity challenges, identify commonalities in shared vulnerabilities, and evaluate the current strategies and countermeasures adopted by these distinct regions. In the USA, a technologically mature landscape with advanced infrastructure and widespread digital adoption contrasts sharply with Africa's diverse technological maturity levels (Roca *et al*., 2021). The USA faces sophisticated threats due to its reliance on cutting-edge technologies, while Africa grapples with a broader range of challenges stemming from a digital divide and varying technological infrastructures (O'Brien *et al*., 2023).

The USA's robust financial capabilities enable substantial investments in cybersecurity infrastructure, research, and development (Kafi and Adnan, 2022). Conversely, many African nations face resource constraints, impacting their ability to implement comprehensive cybersecurity measures. This divergence accentuates the disparities in the intensity of cyber threats faced by each region. The USA boasts well-established and stringent regulatory frameworks governing cybersecurity, fostering a culture of compliance and accountability (Yulianto *et al*., 2023). African nations, however, exhibit a more varied regulatory landscape, with disparities in the enforcement and effectiveness of cybersecurity regulations. This diversity contributes to differences in the nature of security challenges.

Both the USA and Africa grapple with supply chain vulnerabilities, albeit in different contexts. The USA faces risks associated with globalized supply chains, including the potential compromise of critical components. In Africa, supply chain challenges may stem from reliance on international suppliers and vulnerabilities in the delivery process, exacerbating the risks of compromised embedded systems (Hassija *et al*., 20220). Both regions experience challenges related to legacy systems and outdated infrastructure. The USA may encounter security issues due to aging critical infrastructure, while Africa contends with the persistence of outdated technologies and limited resources for upgrading systems. These shared vulnerabilities underscore the universal struggle to secure older technologies in the face of evolving threats. The proliferation of Internet of Things (IoT) devices introduces common security challenges. In both the USA and Africa, the growing interconnectedness of devices, often incorporating embedded systems, amplifies the attack surface (Ukwandu *et al*., 2022). Inadequate security measures in IoT devices create opportunities for cyber adversaries to exploit vulnerabilities, emphasizing the shared challenges in securing the expanding network of embedded systems (Malhotra *et al*., 2021).

The USA employs a comprehensive National Cybersecurity Strategy, emphasizing risk management, innovation, and collaboration. Government agencies collaborate with the private sector through initiatives like the National Cybersecurity Center of Excellence (NCCoE) to develop and implement best practices (Aulianisaand Indirwan,2020). Robust legislation, such as the Cybersecurity and Infrastructure Security Agency (CISA) Act, empowers agencies like CISA to secure critical infrastructure. Regulations, including the NIST Cybersecurity Framework, provide guidelines for organizations to enhance their cybersecurity posture. The USA actively collaborates with international partners to address global cyber threats. Participation in international forums, sharing threat intelligence, and engaging in joint initiatives contribute to a collective defense against cyber adversaries (Brilingaitė *et al*., 2022).

Many African nations focus on capacity building initiatives to enhance cybersecurity skills and knowledge. Training programs, workshops, and partnerships with international organizations aim to strengthen the expertise of cybersecurity

professionals (Trim and Lee, 2021). Efforts are underway to develop and enforce robust regulatory frameworks across Africa. Initiatives like the African Union Convention on Cyber Security and Data Protection aim to harmonize cybersecurity regulations and promote a cohesive approach (Boshe *et al*., 2022). Governments in Africa collaborate with the private sector to enhance cybersecurity capabilities. Public-private partnerships facilitate knowledge sharing, technology transfer, and joint initiatives to address evolving threats.

The comparative analysis of security challenges in embedded systems in the USA and Africa reveals a nuanced landscape shaped by technological disparities, economic factors, and regional dynamics (de Oliveira *et al*., 2023). While the USA grapples with sophisticated threats stemming from its technological maturity, Africa faces a diverse range of challenges influenced by the digital divide and resource constraints. Shared vulnerabilities, including supply chain risks, legacy systems, and the proliferation of IoT devices, underscore the universal nature of the cybersecurity struggle (Abdulkadir *et al*., 2022). The evaluation of current strategies highlights the USA's emphasis on comprehensive frameworks, legislation, and international collaboration, contrasted with Africa's focus on capacity building, regulatory development, and partnerships with the private sector. As both regions strive to fortify the security of embedded systems, the imperative lies in leveraging strengths, addressing common challenges collaboratively, and tailoring strategies to suit the unique characteristics of each environment (Ahmedand Khan,2023). A global approach to cybersecurity, recognizing the interconnectedness of digital systems, is essential for fostering a resilient and secure landscape for embedded systems in an increasingly interconnected world (Victor and Great, 2021).

Embedded systems play a pivotal role in numerous contemporary applications, ranging from consumer electronics and automotive systems to critical infrastructure and medical devices (Jahromi and Kundur,2020). As these systems become increasingly integrated into our daily lives, ensuring their security becomes paramount.

One significant security concern in embedded systems is their resource constraints. Unlike traditional computing systems, embedded devices often operate with limited processing power, memory, and storage (Safari *et al*., 2022). This constraint poses challenges in implementing robust security measures, making it crucial to strike a balance between efficiency and security.

Another critical aspect addressed in the analysis is the lifespan of embedded systems. Unlike general-purpose computers that undergo frequent updates and patches, many embedded devices operate for extended periods without regular maintenance (Khan *et al*., 2023). This longevity poses a challenge in terms of adapting to evolving security threats.

In conclusion, this comparative analysis provides a comprehensive overview of the unique security challenges faced by embedded systems. By understanding the nuances of resource constraints, communication protocols, lifespan considerations, and third-party integrations, stakeholders can develop informed strategies to enhance the security posture of embedded systems across diverse applications (Alliouiand Mourdi,2023).

2.3 Recommendations and Future Considerations

As the world navigates the evolving landscape of security challenges in embedded systems, it becomes imperative to outline recommendations and future considerations that transcend geographical boundaries. This analysis focuses on fostering international collaboration, tailoring strategies to specific regional needs, and harnessing the power of technology and education for enhanced cybersecurity. With a particular lens on the USA and African perspectives, these recommendations aim to create a resilient global framework for securing embedded systems. Advocate for the creation of a collaborative platform or consortium involving governments, international organizations, industry leaders, and academia. This consortium would facilitate the exchange of threat intelligence, best practices, and coordinated responses to emerging security challenges in embedded systems.

Encourage the development of unified global standards for embedded system security. Establishing common benchmarks and protocols can streamline international cooperation, ensuring seamless integration of embedded systems across diverse regions while adhering to shared security standards. Promote the creation of secure information-sharing platforms where nations and organizations can voluntarily contribute threat intelligence. This collective approach enables a more comprehensive understanding of evolving threats, fostering a proactive defense against global cyber adversaries. Support collaborative research and development initiatives on a global scale. Joint projects can lead to the creation of innovative cybersecurity solutions, threat mitigation strategies, and advancements in secure embedded system designs that benefit all participating nations.

Given the USA's technological maturity, continued investment in research and development (R&D) is crucial. Foster public-private partnerships to accelerate innovations in cybersecurity technologies, including artificial intelligence (AI), machine learning (ML), and advanced encryption algorithms. Strengthen supply chain resilience through increased scrutiny and verification mechanisms. Encourage domestic manufacturing of critical components and promote transparency in supply chain processes to mitigate the risks associated with compromised components. Implement adaptive and ongoing cybersecurity training programs to ensure that professionals stay ahead of evolving threats. Collaboration between academic institutions and industry can facilitate the development of specialized courses aligned with industry needs.

Intensify efforts in capacity building through partnerships with international organizations and industry stakeholders. Provide training programs, workshops, and certifications to equip cybersecurity professionals with the skills needed to address the diverse challenges in securing embedded systems. Strengthen and enforce regulatory frameworks related to cybersecurity. Develop region-specific standards that consider the unique challenges of each African nation while promoting compliance and accountability in the implementation of security measures. Establish localized threat intelligence networks that cater to the specific cyber landscape of each African region. Collaborate with neighboring nations to share information, insights, and strategies, fostering a collective defense against region-specific cyber threats.

Embrace the integration of artificial intelligence and machine

learning in cybersecurity measures. Advanced analytics can enhance threat detection capabilities, automate responses, and provide predictive insights, bolstering the defense against sophisticated cyber threats. Advocate for the incorporation of secure-by-design principles in the development lifecycle of embedded systems. Encourage industries to invest in technologies that prioritize security from the outset, reducing vulnerabilities and the need for extensive post-implementation security measures. Embed cybersecurity education at all levels of academic curricula. Introduce age-appropriate cybersecurity concepts in schools, colleges, and universities to cultivate a cybersecurity-aware culture. Educational initiatives should extend beyond formal institutions, reaching professionals and the general public through awareness campaigns. Foster public-private partnerships to bridge the cybersecurity skills gap. Collaborate with industry leaders to develop specialized training programs, workshops, and certification courses that align with the evolving needs of the cybersecurity landscape. The recommendations and future considerations presented here aim to transcend geographical boundaries, recognizing that the security challenges in embedded systems demand a global response. International collaboration, tailored strategies for diverse perspectives, and the integration of technology and education form the pillars of a holistic approach. As the world becomes more interconnected, the security of embedded systems requires a concerted effort from nations, organizations, and individuals. By advocating for global cooperation, tailoring strategies to regional needs, and investing in technology and education, the international community can navigate the complex landscape of embedded system security challenges, fostering a secure and resilient digital future for all.

3. Conclusion

In dissecting the security challenges in embedded systems from the perspectives of the United States (USA) and African nations, a nuanced landscape emerges, shaped by technological maturity, economic variations, and regional dynamics. As we recapitulate the key findings from this comparative analysis, it is evident that the security of embedded systems transcends borders, demanding a collaborative and global response. The USA, with its technological maturity, faces sophisticated threats, while Africa grapples with a diverse range of challenges, including a digital divide and resource disparities. Both regions encounter common challenges such as supply chain vulnerabilities, legacy systems, and the proliferation of Internet of Things (IoT) devices, underlining the universal nature of the cybersecurity struggle. While the USA emphasizes comprehensive frameworks, legislation, and international collaboration, Africa focuses on capacity building, regulatory development, and partnerships with the private sector.

As we confront the complex security landscape of embedded systems, a resounding call to action echoes – one that transcends geographical boundaries. The interconnectedness of our digital ecosystems necessitates a global perspective in addressing security challenges. A collaborative approach that involves governments, industry leaders, international organizations, and academia is imperative. The need for a global cybersecurity consortium becomes apparent – a platform where nations can unite to exchange threat intelligence, establish unified standards, and engage in joint research and development initiatives. The shared understanding of threats and vulnerabilities will foster a proactive defense against global cyber adversaries.

The establishment of common benchmarks and protocols for embedded system security is crucial. A unified approach ensures seamless integration across regions, fostering a global environment where cybersecurity standards transcend geopolitical borders. Secure information-sharing platforms should be promoted, facilitating voluntary contributions of threat intelligence. This collective approach enables a comprehensive understanding of evolving threats, empowering nations to mount a unified defense against cyber adversaries.

Looking to the future, the trajectory of advancements and developments in mitigating security risks in embedded systems holds promise. Consideration of potential advancements on a global scale involves embracing technological innovations and educational initiatives. The integration of artificial intelligence and machine learning stands as a beacon for the future. Advanced analytics and automation will redefine the landscape, enhancing threat detection, response capabilities, and predictive insights. The shift towards secure-by-design principles in the development lifecycle of embedded systems is imperative. Investing in technologies that prioritize security from the outset reduces vulnerabilities and fortifies the overall security posture. The continuous integration of cybersecurity education at all levels is vital. As we foster a culture of cybersecurity awareness, initiatives in schools, colleges, and professional settings will cultivate a workforce adept at navigating the evolving cybersecurity landscape.

In conclusion, the security challenges in embedded systems demand a unified vision that recognizes the interconnected nature of our digital world. The USA and Africa, despite their diverse perspectives, share a common goal – to fortify the foundations of cybersecurity in embedded systems. As we navigate the future, a collaborative and global approach, grounded in shared standards, knowledge exchange, and collective defense, will pave the way for a secure and resilient digital ecosystem on a global scale.

4. Reference

1. Abdulkadir M, Abdulahi A, Abdulkareem LA, Alor OE, Ngozichukwu B, Al-Sarkhi A, *et al*. The effect of gas injection geometry and an insight into the entrainment and coalescence processes concerned with a stationary Taylor bubble in a downward two-phase flow. Exp Therm Fluid Sci. 2022;130:110491.
2. Abiodun OI, Abiodun EO, Alawida M, Alkhawaldeh RS, Arshad H. A review on the security of the internet of things: Challenges and solutions. Wirel Pers Commun. 2021;119:2603-37.
3. Adeniyi OD, Ngozichukwu B, Adeniyi MI, Olutoye MA, Musa U, Ibrahim MA. Power generation from melon seed husk biochar using fuel cell. Ghana J Sci. 2020;61(2):38-44.
4. Ahmed S, Khan M. Securing the Internet of Things (IoT): A Comprehensive Study on the Intersection of Cybersecurity, Privacy, and Connectivity in the IoT Ecosystem. AI IoT 4th Ind Revolut Rev. 2023;13(9):1-17.
5. Allioui H, Mourdi Y. Exploring the full potentials of IoT for better financial growth and stability: A comprehensive survey. Sensors. 2023;23(19):8015.

6. Aloseel A, He H, Shaw C, Khan MA. Analytical review of cybersecurity for embedded systems. IEEE Access. 2020;9:961-82.
7. Atkins S, Lawson C. An improvised patchwork: success and failure in cybersecurity policy for critical infrastructure. Public Adm Rev. 2021;81(5):847-61.
8. Aulianisa SS, Indirwan I. Critical Review of the Urgency of Strengthening the Implementation of Cyber Security and Resilience in Indonesia. Lex Sci Law Rev. 2020;4(1):31-45.
9. Biygautane M, Clegg S, Al-Yahya K. Institutional work and infrastructure public-private partnerships (PPPs): the roles of religious symbolic work and power in implementing PPP projects. Account Audit Account J. 2020;33(5):1077-112.
10. Boshe P, Hennemann M, von Meding R. African Data Protection Laws: Current Regulatory Approaches, Policy Initiatives, and the Way Forward. Glob Priv Law Rev. 2022;3(2).
11. Brilingaitė A, Bukauskas L, Juozapavičius A, Kutka E. Overcoming information-sharing challenges in cyber defence exercises. J Cybersecur. 2022;8(1):tyac001.
12. Cheng X, Liu S, Sun X, Wang Z, Zhou H, Shao Y, *et al*. Combating emerging financial risks in the big data era: A perspective review. Fundam Res. 2021;1(5):595-606.
13. de Oliveira RT, Ghobakhloo M, Figueira S. Industry 4.0 towards social and environmental sustainability in multinationals: Enabling circular economy, organizational social practices, and corporate purpose. J Clean Prod. 2023:139712.
14. Djenna A, Harous S, Saidouni DE. Internet of things meet internet of threats: New concern cyber security issues of critical cyber infrastructure. Appl Sci. 2021;11(10):4580.
15. Eceiza M, Flores JL, Iturbe M. Fuzzing the internet of things: A review on the techniques and challenges for efficient vulnerability discovery in embedded systems. IEEE Internet Things J. 2021;8(13):10390-411.
16. Gikunda K. Empowering Africa: An In-depth Exploration of the Adoption of Artificial Intelligence Across the Continent. arXiv [preprint]. 2023:arXiv:2401.09457.
17. Halak B. Cist: A threat modelling approach for hardware supply chain security. In: Hardware Supply Chain Security: Threat Modelling, Emerging Attacks and Countermeasures. 2021. p. 3-65.
18. Hassija V, Chamola V, Gupta V, Jain S, Guizani N. A survey on supply chain security: Application areas, security threats, and solution architectures. IEEE Internet Things J. 2020;8(8):6222-46.
19. Jahromi AA, Kundur D. Fundamentals of cyber-physical systems. In: Cyber-Physical Systems in the Built Environment. 2020. p. 1-13.
20. Jiang X, Lora M, Chattopadhyay S. An experimental analysis of security vulnerabilities in industrial IoT devices. ACM Trans Internet Technol. 2020;20(2):1-24.
21. Johnson D, Pranada E, Yoo R, Uwadiunor E, Ngozichukwu B, Djire A. Review and Perspective on Transition Metal Electrocatalysts Toward Carbon-neutral Energy. Energy Fuels. 2023;37(3):1545-76.
22. Kafi MA, Adnan T. Empowering Organizations through IT and IoT in the Pursuit of Business Process Reengineering: The Scenario from the USA and Bangladesh. Asian Bus Rev. 2022;12(3):67-80.
23. Kasten J, Hsiao CC, Ngozichukwu B, Yoo R, Johnson D, Lee S, *et al*. High Performing pH-Universal Electrochemical Energy Storage Using 2D Titanium Nitride Mxene. In: 2023 AIChE Annual Meeting. AIChE; 2023.
24. Khan A, Xu D, Tian DJ. Low-cost privilege separation with compile time compartmentalization for embedded systems. In: 2023 IEEE Symposium on Security and Privacy (SP). IEEE; 2023. p. 3008-25.
25. Khan F, Kumar RL, Kadry S, Nam Y, Meqdad MN. Cyber physical systems: A smart city perspective. Int J Electr Comput Eng. 2021;11(4):3609.
26. Lazard O, Youngs R. The EU and climate security: toward ecological diplomacy. Carnegie Europe. 2021;12.
27. Lehto M. Cyber-attacks against critical infrastructure. In: Cyber Security: Critical Infrastructure Protection. Cham: Springer; 2022. p. 3-42.
28. Lukong VT, Ukoba KO, Jen TC. Analysis of sol aging effects on self-cleaning properties of TiO2 thin film. Mater Res Express. 2021;8(10):105502.
29. Malhotra P, Singh Y, Anand P, Bangotra DK, Singh PK, Hong WC. Internet of things: Evolution, concerns and security challenges. Sensors. 2021;21(5):1809.
30. Martínez J, Durán JM. Software supply chain attacks, a threat to global cybersecurity: SolarWinds' case study. Int J Saf Secur Eng. 2021;11(5):537-45.
31. Mazzolin R, Samueli AM. A Survey of Contemporary Cyber Security Vulnerabilities and Potential Approaches to Automated Defence. In: 2020 IEEE International Systems Conference (SysCon). IEEE; 2020. p. 1-7.
32. Mishra P, Singh G. Energy management systems in sustainable smart cities based on the internet of energy: A technical review. Energies. 2023;16(19):6903.
33. Möller DP. NIST Cybersecurity Framework and MITRE Cybersecurity Criteria. In: Guide to Cybersecurity in Digital Transformation: Trends, Methods, Technologies, Applications and Best Practices. Cham: Springer; 2023. p. 231-71.
34. Munirathinam S. Industry 4.0: Industrial internet of things (IIOT). Adv Comput. 2020;117(1):129-64.
35. O'Brien N, Li E, Chaibva CN, Bravo RG, Kovacevic L, Ayisi-Boateng NK, *et al*. Strengths, Weaknesses, Opportunities, and Threats Analysis of the Use of Digital Health Technologies in Primary Health Care in the Sub-Saharan African Region: Qualitative Study. J Med Internet Res. 2023;25(1):e45224.
36. Pliatsios D, Sarigiannidis P, Lagkas T, Sarigiannidis AG. A survey on SCADA systems: secure protocols, incidents, threats and tactics. IEEE Commun Surv Tutor. 2020;22(3):1942-76.
37. Roca JB, Vaishnav P, Morgan GM, Fuchs E, Mendonça J. Technology Forgiveness: Why emerging technologies differ in their resilience to institutional instability. Technol Forecast Soc Change. 2021;166:120599.
38. Safari S, Ansari M, Khdr H, Gohari-Nazari P, Yari-Karin S, Yeganeh-Khaksar A, *et al*. A survey of fault-tolerance techniques for embedded systems from the perspective of power, energy, and thermal issues. IEEE Access. 2022;10:12229-51.
39. Bitragunta SLV. Enhanced System of Load Management for Low-Voltage. Int J Innov Res Eng Multidiscip Phys Sci. 2022;10(3).
40. Safitra MF, Lubis M, Fakhrurroja H. Counterattacking

cyber threats: A framework for the future of cybersecurity. Sustainability. 2023;15(18):13369.
41. Shillair R, Esteve-González P, Dutton WH, Creese S, Nagyfejeo E, von Solms B. Cybersecurity education, awareness raising, and training initiatives: National level evidence-based results, challenges, and promise. Comput Secur. 2022;119:102756.
42. Shukla S, Bisht K, Tiwari K, Bashir S. Comparative Study of the Global Data Economy. In: Data Economy in the Digital Age. Singapore: Springer; 2023. p. 63-86.
43. Trim PR, Lee YI. The global cyber security model: counteracting cyber attacks through a resilient partnership arrangement. Big Data Cogn Comput. 2021;5(3):32.
44. Ukoba K, Jen TC. Thin films, atomic layer deposition, and 3D Printing: demystifying the concepts and their relevance in industry 4.0. CRC Press; 2023.
45. Ukwandu E, Ben-Farah MA, Hindy H, Bures M, Atkinson R, Tachtatzis C, *et al*. Cyber-security challenges in aviation industry: A review of current and future trends. Information. 2022;13(3):146.
46. Victor E, Great CU. The Role of Alkaline/alkaline Earth Metal Oxides in CO2 Capture: A Concise Review. J Energy Res Rev. 2021;9(3):46-64.
47. Vivek S, Conner H. Urban road network vulnerability and resilience to large-scale attacks. Saf Sci. 2022;147:105575.
48. Yaacoub JPA, Salman O, Noura HN, Kaaniche N, Chehab A, Malli M. Cyber-physical systems security: Limitations, issues and future trends. Microprocess Microsyst. 2020;77:103201.
49. Yulianto S, Gaol FL, Supangkat SH, Ranti B. A Comprehensive Model for Enhancing Cybersecurity Resilience and IT Governance Through Red Teaming Exercises. In: 2023 29th International Conference on Telecommunications (ICT). IEEE; 2023. p. 1-7.
50. Zhang L, Kim C. Chromatics in urban landscapes: Integrating interactive genetic algorithms for sustainable color design in marine cities. Appl Sci. 2023;13(18):10306.