NIPES

Journal of Energy Technology and Environment

Journal homepage: www.nipesjournals.org.ng

The Future of Cyber Security: Examining the Security Challenges and Trends in Smart Technology

Omosigho O. Moses and Ehizuenlen, E. Prudence
Department of Computer Engineering, Faculty of Engineering, University of Benin, Benin City, Edo State. Nigeria
*Corresponding Author Email: moses.omosigho@uniben.edu

Article information

Article History
Received: 8 February 2024
Revised: 18 February 2024
Accepted: 25 February 2024
Available online: 15 March 2024

Keywords:
Cyber security challenges, Smart technologies, Emerging trends, Vulnerabilities, Risk mitigation.

https://doi.org/10.5281/zenodo.10823176

https://nipesjournals.org.ng

Abstract

With the advent of smart technologies, the world is witnessing unprecedented growth in interconnected devices, autonomous systems, and digital infrastructures. However, this ubiquitous connectivity also raises major cybersecurity issues. This study provides an in-depth review of the cyber security threats posed by smart technologies and identifies emerging trends to mitigate these threats. Drawing on an in-depth literature review and case studies, the study aims to identify the key weaknesses of smart technologies and suggest proactive measures to mitigate them. The results of the study led to the proposed design of an architecture to address the identified cyber security challenges.

.
.

1. Introduction

Internet of things (IoT) devices, such as smartphones, smart homes, wearable tech, artificial intelligence (AI), edge computing, etc., have revolutionized many industries, including healthcare, transport, energy, infrastructure, etc. [1] These innovations have brought many advantages and made life easier and more connected, but they have also put society under unprecedented cyber risks [2]. Cloud Computing, Big Data, and Other New Edge Computing Technologies are also on the increase. As a result of the global information revolution, the world economy, social progress, and human life are now more reliant on information technology than ever before. [3] The open nature of the internet and the ease with which data can be exchanged have rendered it a global threat. As a result, information security has become a national security priority. [4][5]. The amount

and complexity of data storage is growing while the sharing of Big Data raises new questions about information security and privacy.[6], [7]. While the primary goals of cloud computing are data utility and data storage security [8], [9]. There are concerns about an all-inclusive approach to

securing smart technologies and users' privacy through cyber security [13]. Some important questions that come up while examining the security challenges and trends in smart technology are: What is cyber security? what are cyber security measures and roles in combating cyber-crimes? how do we protect our systems, networks, data stores, and programs from cyber-attacks? [10].

A cyber-attack is any malicious cyber activity intended to harm, disrupt, or interfere with a national cyber asset's services or information. An attack is a deliberate cyber activity using a cyber weapon to attack an information system and cause a cyber incident [45], [11], [12]. Cyber-attacks are on the rise, according to research and statistical reports. [13], [14], and people from all over the globe are attempting to gain access to vulnerable business systems. cyber-attacks are designed majorly to steal data, information and, money from organizations. This has been seen in the past few years when many computers have been hacked with malware that seeks to exploit financial systems in different countries [15]. In other cases, cyberattacks can be military in nature or political in nature. Some common types of cyberattacks include [16] [17], Ransomware Trojans, Phishing, DOS DDoS, SQL Injection DNS, Tunneling Zero day, exploits, and, Password attacks. XSS attacks, Rootkit attacks, DNS spying, or poisoning, Session hijacking URL manipulation, Crypto-jacking Inside threat, PC virus Knowledge breaks, DDS [11]. Cyber security has never been so challenging to implement because of the everincreasing number of devices, hackers, and the ever-changing nature of smart technologies [18]. Connected devices are one of the biggest threats to cybersecurity in smart technologies. [19].

In addition, the ever-increasing amount of information used by millions of devices is now stored in the cloud, which attracts attackers. [20]. In June 2012 DDoS attackers took advantage of vulnerabilities in mobile voicemail service AT&T and Google account recovery service Gmail to get into Cloud Flare's DDoS mitigation. [21]. With over 2 billion people using smartphones in the world by 2015, the number of mobile malware infections has grown exponentially. For example, in 2012 alone, Android malware unique detections around the world increased by 17 times compared to the year before.[22]. Physical attacks are also possible on hardware devices, as they are relatively easy to access and control. This is where physical security can provide attackers with a great deal of flexibility and the opportunity to conduct sophisticated security attacks on the hardware device [23], [24]. In addition, the reliance on industry-specific communication protocols and hardware can lead to interoperability problems and increase the vulnerability of the system. There are also issues with weak authentication, weak network security, and the potential for large-scale attacks on connected devices. [25]. Internal threats and data breaches as well as privacy issues also need to be addressed. [26]. Organizations need to implement cyber security regulations and standards such as GDPR, PCI, and DSS to ensure effective security controls and comply with data breach notification and privacy requirements. [27], [28], [29]. While the focus is on finding cost-effective solutions, advanced detection and response (ADR) systems are also required to mitigate the risk of a security breach on smart technologies.

This study is aimed at addressing the afore-mentioned cyber security challenges associated with smart technologies, as well as identify emerging trends in addressing those challenges and developing a proactive solution architecture response system against cyber-attacks.

[30] This study focused on existing threats in cybersecurity domain: such as security vulnerability analysis, critical analysis of current mitigation techniques, pros and cons of existing mitigation techniques, new attack patterns coming from emerging technologies, and the need to develop more advanced and effective malware defenses. It is considered the most exploitable weakness in today's hardware, software, and network layer which is the criticism of current mitigation technologies on

why they don't work on social media attacks, cloud computing attacks, smart devices attacks, and critical infrastructure attacks.

[19] The study addressed cybersecurity risks associated with IoT-enabled smart grid networks. the researchers also considered the security threats posed by online devices that made smart grid networks susceptible to large-scale attacks. The study highlighted the vastness of the attack surface on smart grid networks, with millions of nodes having the biggest attack surface. It also looked at the devastating consequences of a grid outage on widespread infrastructure, given the cascading effects of a power outage, as most of the things we rely on for our day-to-day lives, such as our homes and offices, as well as health centers and trains, need electricity to function. Once a smart device is breached, the whole grid is at risk of a full-scale outage, potentially causing significant economic and financial losses for whole cities. The study concluded that security should be a top priority for the large-scale roll-out of IoT smart grid networks.

[32] The researchers discussed the cyber security threats in an existing connected home ecosystem of the future. They considered the premise that, while these devices bring more features and capabilities to the table, they also bring new risks. They posited that, most researchers focused on corporate and national systems defenses, while they often overlook the vulnerabilities in the devices used in connected smart homes of today and tomorrow. The paper seeks to examine the impact and challenges that cybersecurity has on smart devices in connected homes. It also looks at some of the related backgrounds and motivations that we've seen around the growth and demand of seamless connectivity for smart devices to offer different functionality and capabilities for users.

[11] The objective of the study was to define and evaluate standard developments in the field of cyber security and to evaluate the challenges, limitations, and benefits of the suggested approaches based on peer-reviewed literature reviews. Different types of new descendant attacks were studied in detail including standard security frameworks, the history and first generation of cyber security techniques, trends and emerging trends as well as the threats and challenges of cyber security. the evaluations showed that there is a need for more proactive measures to be considered in the battle against cyber insecurity.

[31] This paper discussed the importance of cyber security and, the growing need to protect information in the modern world. It covers the current cybersecurity issues and the latest trends in the most recent technologies. It also covers the challenges related to cyber security on new technologies. These challenges include the inability to effectively protect private information, the increasing number of cyber-crimes, and the requirement of high-quality security for transparent, high-value transactions. The study found that the emergence of new technologies such as the cloud, mobile, electronic commerce, and network banking required increased security measures because they contain sensitive information about individuals. The paper also mentions that various government and corporate bodies are taking various steps to fight cybercrime. However, it does not specify what those steps are:

2.0 Methodology

The methodology employed in this study involves describing the emerging trends employed in addressing the challenges posed by cyber security threats, examine relevant case-datasets, and providing strategies for mitigating cyber security risk.

2.1 Emerging Trends to Address the Challenges Posed by Cyber Security Threats With the continuous development of cyber technologies, several cybersecurity solutions have emerged

over time [19] as illustrated in Figure 1. This section of the paper dwells on these emerging trends. These emerging solutions trend usually address various trends such as in threat detection intelligence, machine learning algorithms, anomaly detection, secure hardware development, blockchain applications, and AI for proactive defense mechanisms.

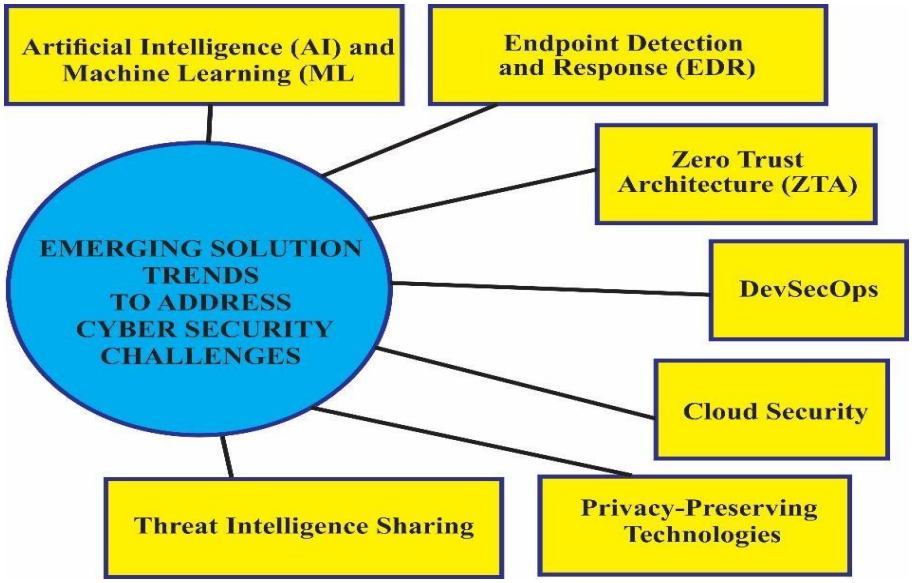

Figure 1: Emerging Solution Trends To Address Cyber Security Challenges

a. **Machine Learning (ML):** The use of AI and ML in cyber security is increasing to improve the detection and response to potential threats [33]. Machine learning uses large volumes of data to recognize patterns and anomalies that can be used to detect potential risks. AI-powered tools can automate threat response, making incident response more efficient and less prone to human error. AI algorithms can continually learn and evolve, making it easier for them to identify and respond to new threats.
b. **Endpoint attack Detection and Response (EDR):** In the past, perimeter defenses were the focus of cybersecurity strategies. However, with the rise of remote and mobile devices, the attack surface has expanded beyond the network's perimeter. [34] EDR systems provide realtime monitoring and protection of endpoints, including laptops, desktops, and mobile devices, to detect and address suspicious activity or threats.
c. **Node Zero Trust Architecture (ZTA):** ZTA is based on the premise that all users and devices at a node are at risk of compromise, so verification and strict access controls are required for every resource accessed. [35] Zero Trust Architecture ensures that no implicit trust is granted to any users, devices, or applications, regardless of where they are in the network. ZTA takes a more granular, granular approach to access control to reduce the risk of lateral movement within the network.
d. **Software Development and Security Operations (**DevSecOps**):** Integrating cybersecurity practices into DevSecOps makes security a part of the software development and deployment process. This means that security measures are applied across the entire software development lifecycle (from code development to deployment and beyond) [36]. Integrating security into DevSecOps early in the process reduces vulnerabilities, enhances collaboration between DevSecOps and Security teams, and accelerates response times to security issues.

e. **Cloud Access Security:** As cloud adoption continues to grow, the need for cloud security measures has never been greater. More and more cloud security solutions are popping up to secure data, manage access, and protect against cloud threats. [37] Cloud Access Security Brokers (CASBs), Encryption, and Identity and Access Management (IAM) solutions are some of the technologies being developed to secure cloud environments. Best practices include MFA, regular data backups, and robust disaster recovery plans.
f. **User Privacy-Preserving Technologies**: Privacy-friendly technologies help organizations safeguard user privacy while allowing data-driven analysis and insights. As data privacy regulations become more stringent, there is a growing focus on privacy-friendly technologies[38].Various privacy technologies, such as differential privacy techniques (DPPs), homomorphic encryption (HEMCs), and SMP (Secure Multi-User Computing), are designed to protect data privacy while enabling sensitive data analysis and sharing.
g. **Threat Intelligence Sharing**: Cybersecurity collaboration and information sharing are essential. Threat intelligence sharing is a way for organizations to proactively identify and mitigate threats. [39] Formal sharing platforms, sector-specific ISACs, or P2P partnerships can be used to share information on emerging threats.

2.2 Relevant Case datasets

To supplement the theoretical analysis, this section presents case datasets that illustrate real-world cyber security incidents in the context of smart technologies. These cases shed light on the scope and severity of cyber threats, their implications, and the lessons learned in terms of risk mitigation strategies.

a. Mirai Botnet Attack on Domain Name Service (DNS): In 2016, Mirai, a malicious botnet, targeted Dyn, which is one of the biggest DNS servers in the world. The attack caused a massive outage on popular websites such as Twitter, PayPal, and Netflix. [40]. Mirai took advantage of weak or common passwords on Internet of Things (IoT) devices, using them as zombie devices to overwhelm Dyn's servers with traffic and render them inoperable. The incident highlighted the need for more robust security measures in IoT devices, beginning at the manufacturing level and extending to regular software updates.
b. Stuxnet Worm On Nuclear Program: Stuxnet is a worm that was first discovered in 2010. It targeted industrial control systems (ICSs) that were specifically designed for SCADA (supervisory control & data acquisition). The Stuxnet worm was specifically designed to harm Iran's nuclear program, specifically targeting the centrifuges used to enrich the country's uranium. [41] The malicious software exploited weaknesses in Windows and SCADA software to cause physical damage. It spreads through USB drives as well as network shares. The Stuxnet case highlighted the physical damage that cyberattacks can inflict on critical infrastructure and how important it is to protect industrial IoT devices.
c. Jeep Cherokee Information System Hack: In 2015, a Jeep Cherokee's infotainment system was hacked remotely by two security researchers, allowing them to gain control over the vehicle's various functions, including the ability to brake and accelerate [42]. The flaw in the infotainment system's software was due to poor security practices. This incident raised questions about the potential risks of connected car technologies, as well as the need for strong security measures to protect passengers.
d. Ukraine Power Grid Cyber Attack: The Ukrainian power grid was affected by two major cyberattacks in 2015 and 2016. [43] Power outages affected thousands of customers as a result of the attacks. Black Energy malware and a variant known as "KillDisk" were used

by the attackers to access the control systems of the power grid and disrupt its operations. The events of 2015 and 2016 highlighted vulnerabilities in critical infrastructure systems as well as the need for improved cybersecurity measures to safeguard national power networks and other critical services.

e. Unauthorized Access Device Ring Camera Breaches: In 2019, several incidents occurred at Ring, a top smart doorbell and home security camera manufacturer [44]. Hackers gained unauthorized access to Ring's customer's devices, such as cameras, live streams, and even conversations with homeowners [45]. Many of these incidents occurred because customers used weak passwords or reused passwords. These incidents are a reminder of the importance of strong authentication mechanisms and the need to educate users on how to properly protect their devices. These case studies illustrate the real-life consequences of cybersecurity incidents within the smart technology space. They highlight the urgency of cybersecurity measures to be taken seriously by security professionals and manufacturers, as well as individuals.

3.0 Results and Discussion

The afore mentioned relevant case datasets, [40],[41],[42],[43],[44],[46],[47][48],[49],[50] were used to develop the proposed design architecture solution as a proactive strategy, to address cyberthreats and security challenges.

Case Datasets And Related Challenges

We proposed the following solutions to address the use cases and other future cyber security related challenges as identified in the different literature reviews.

I. **Network segmentation:** the study encourages the implementation of network segmentation to segregate the network into different segments or zones to limit the lateral movement of the malware. this can help contain the impact of an attack and prevent it from spreading to critical systems,

II. **Patch management:** regularly update and patch software and systems to address vulnerabilities. Many successful attacks exploit known vulnerabilities for which patches are available,

III. **Multi-Factor Authentication (MFA):** Implement MFA to add an extra layer of security, making it more difficult for unauthorized users or bots to gain access even if login credentials are compromised,

IV. **DNS Security Solutions:** Employ DNS security solutions, such as Domain Name System Security Extensions (DNSSEC), to enhance the integrity and authenticity of DNS data and prevent DNS spoofing attacks,

V. **Anomaly Detection and Intrusion Prevention Systems:** Utilize advanced threat detection systems to identify unusual or suspicious behavior on the network, triggering alerts and allowing for rapid response,

VI. **Use of Advanced Security Technologies**: Implementing advanced cybersecurity technologies such as intrusion detection systems, firewalls, and antivirus software can help identify and block malicious activities,

VII. **Encryption:** Utilizing strong encryption protocols for data transmitted between Ring Cameras and associated devices adds an additional layer of protection, making it more difficult for attackers to intercept and manipulate data.

Proactive Strategies For Cyber Security Risk Mitigation

I. **Education and Training:** Cybersecurity best practices are one of the most important proactive measures that can be taken. It requires that employees are well-informed and up-to-date on the latest security best practices. Schedule regular training sessions to help them understand the risks they may be exposed to and how to reduce them. For example, they should be aware of phishing scams and how to avoid them. They should also be taught about secure passwords, safe browsing, and how to be more cautious when using email or social media. By improving employees' cybersecurity awareness, organizations can significantly reduce their employees' risk of becoming victims of cyber threats.

II. **Regular Risk Assessments**: Risk assessments are essential for identifying and mitigating cyber threats and vulnerabilities within your organization's infrastructure. By performing comprehensive risk assessments, users can identify vulnerabilities in their systems, networks, and processes proactively. This allows them to implement controls and remedial measures to effectively mitigate these risks. Risk assessments should be performed regularly or whenever there are significant changes to their business processes. Doing so ensures ongoing proactive management of cyber risks.

III. **Robust Cybersecurity Policies and Procedures**: As the first line of defense against cyber threats, cybersecurity policies and procedures define acceptable technology usage. They also define password policies and email policies. They also define data classification policies and incident response policies. Developing and enforcing these policies creates a strong security culture within the organization and provides clear guidelines on how to respond to cyber threats.

IV. **Multi-Factor Authentication (MFA):** In MFA, users must provide more than just a username and password. For example, they must provide fingerprint scans or SMS codes, as well as tokenbased authentication. MFA takes the guesswork out of the authentication process by allowing users to provide more than just the username and password. This step-by-step approach significantly reduces the risk of an unauthorized user accessing your system, even after a password breach. Multi-factor authentication across applications and systems helps protect sensitive data and systems from easy access by cybercriminals.

V. **Regular Software Updates and Patch Management**: It is essential for all software, operating systems, and applications to be regularly updated to reduce cyber risks. Legacy systems are often susceptible to exploitation by cybercriminals seeking to gain unauthorized access or launch attacks. Software updates and patch management are two processes that help organizations reduce vulnerability exploitation risk in the first place. Software updates and patch management help organizations mitigate risks in the first place by prioritizing software updates.

VI. **Continuous Monitoring and Analysis:** Monitoring and analyzing network traffic and system logs, as well as security events, is an important proactive strategy for detecting unusual activity and threats in real time. By implementing an SIEM system, organizations can identify, correlate, and act on security incidents quickly. By monitoring their systems' health regularly, organizations can identify and respond to suspicious activity in real-time, minimizing the impact of cyber-attacks.

VII. **Incident Response Planning**: An incident response plan is a set of steps an organization takes in response to a security incident. It outlines who should be involved in the incident, escalation procedures, communications protocols, and how the incident should be contained and resolved. By developing an incident response plan and testing it regularly, organizations can minimize the disruption caused by cyber incidents. By preparing for

potential breaches ahead of time, organizations can respond more quickly and efficiently, reducing downtime and damage to their operations.

Proposed Design Architecture to Address Cyber Security Challenges

Figure 2 illustrates the implementation of layered security controls across the system. Below is a brief description of a design structure that can help resolve cybersecurity issues:

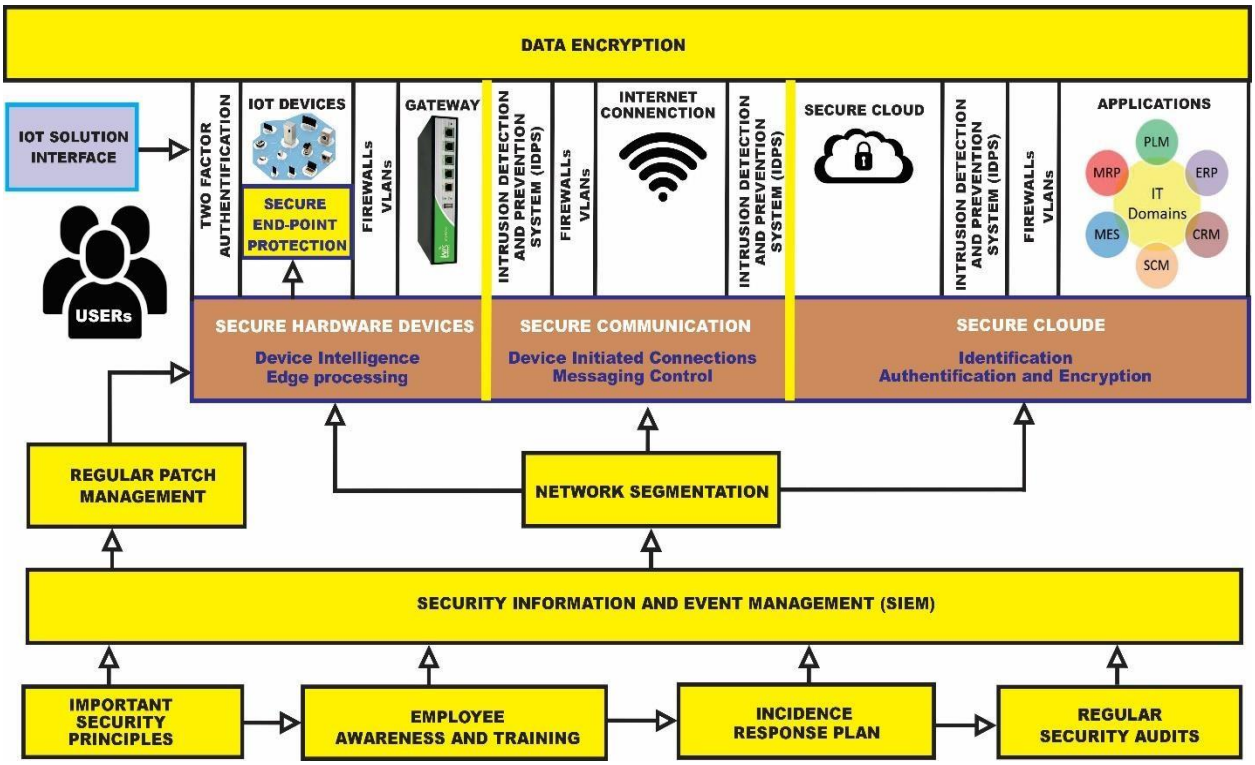

Figure 2: Multiple Layers Of The Security Architecture Of Iot Devices

In the end, a good cyber security architecture should combine several layers of protection, focus on preventing attacks, quickly identify and address incidents, and continually improve security defenses.

I. **Network Segmentation:** The most effective way to restrict lateral movement for an attacker is through a structured and segmented network architecture. Firewalls, VLANs, and access controls all work together to isolate different areas of the network and reduce the impact of a breach.

II. **Intrusion Detection and Prevention Systems (IDPS):** Identity and Access Protection (IDPS) is deployed at critical points of entry and exit within the network to provide real-time visibility and protection against known and potential threats. Identity and Access Protection can identify and prevent malicious activity, as well as anomalies, and prevent attacks before they can cause significant harm.

III. **Secure Endpoint Protection:** Endpoint protection solutions include anti-virus software, Host Interception Prevention Systems (HIPS), and endpoint encryption. These solutions protect individual devices against malware, viruses, and unauthorized access. Endpoint protection solutions need to be updated regularly to keep up with new threats.

IV. **Security Information and Event Management (SIEM):** SIEM allows the user to centralize, monitor, and correlate security incidents in real-time across their network. It also enables proactive threat detection, incident response, and enhances incident management capabilities.

V. **Two-Factor Authentication (2FA):** 2FA is another type of security measure. 2FA requires users to provide two different methods of authentication: a username and password, and a unique code sent to the user's device. This ensures that no one can gain access to the user's account, even if their password has been hacked.

VI. **Data Encryption**: Both in-transit and out-of-band encryption are essential to protect sensitive information from unauthorized access. By implementing encryption algorithms and protocols, the user reduces the chances of data breaches.

VII. **Regular Patch Management**: All software, operating systems, and applications need to be kept up to date with the most up-to-date security patches to address vulnerabilities and prevent known exploits. Implementing a consistent patch management process will ensure that all systems are kept up to date.

VIII. **Employee Awareness and Training**: Employees should be trained on how to identify cyber threats, best practices for safe computing, and the need to adhere to security policies. With regular training programs, the employees will understand their part in keeping the organization secure and will be able to identify phishing attacks, social engineering, and other attack methods. IX. **Incident Response Plan**: In the event of a security breach identified, it's essential to establish an incident response plan (ERP). The ERP should outline how an incident is identified, analyzed, contained, eradicated, and recovered. The users are required to test and improve their ERP regularly.

X. **Regular Security Audits**: Regular security audits conducted by independent assessors can help you identify weaknesses and areas for improvement. These audits look at system configurations, access control, policies, and procedures, and provide valuable insights to close security gaps. Cybersecurity threats and vulnerabilities are constantly changing, and the architecture needs to be regularly evaluated, updated, and enhanced to respond to emerging threats and vulnerabilities.

4.0 Conclusion

This study summarizes the key findings and provides an overview of the challenges smart technologies face when it comes to cyber security, as well as the emerging trends in risk mitigation. It highlights the need for organizations to take proactive steps to protect and mitigate the risks associated with smart technologies in an ever-changing threat environment. By investing in education, training, risk assessments, strong policies and procedures, MFA, software updates, constant monitoring, and incident response planning, organizations can significantly improve their cybersecurity posture and reduce the impact of cyber risks. It is essential to remain vigilant and continually adjust these strategies as cyber threats evolve. The recommendation for further studies is the physical implementation of the proposed architectural design.

References

[1] Kumar, S., Tiwari, P. & Zymbler, M. (2019). Internet of Things is a revolutionary approach for future technology enhancement: a review. *J Big Data* **6**, 111 https://doi.org/10.1186/s40537-019-0268-2

[2] Ioannis Agrafiotis, Jason R C Nurse, Michael Goldsmith, Sadie Creese, David Upton, (2018), A taxonomy of cyber-harms: Defining the impacts of cyber-attacks and understanding how they propagate, *Journal of Cybersecurity*, Volume 4, Issue 1, tyy006, https://doi.org/10.1093/cybsec/tyy006.

[3] J. Shi, C. Huang, H. E. Kai, and X. Shen, (2019)"ACS-HCA:An access control scheme under hierarchical cryptography architecture," *Chinese Journal of Electronics*, vol. 28, no. 1, pp. 56–65,.

[4] L. Fang, M. Li, L. Zhou, H. Zhang, and C. Ge, (2019) "A fine-grained user-divided privacy-preserving access control protocol in smart watch," *Sensors*, vol. 19, no. 9, Article ID 2109, 2019.

[5] R. Xu, C. Yu, E. Blasch, and G. Chen, (2019) "Exploration of blockchain-enabled decentralized capabilitybased access control strategy for space situation awareness," *Optical Engineering*, vol. 58, no. 4, p. 1,.

[6] Benjelloun, Fatima-Zahra & Ait Lahcen, Ayoub. (2015). Big Data Security: Challenges, Recommendations and Solutions. 10.4018/978-1-4666-8387-7.ch014.

[7] Abdullah Al-Shomrani, Fathy Eassa, Kamal Jambi. (2018)"Big Data Security and Privacy Challenges", International Journal of Engineering Development and Research (IJEDR), ISSN:2321-9939, Vol.6, Issue 1, pp.894-900, March URL :http://www.ijedr.org/papers/IJEDR1801155.pdf

[8] Sun Y, Zhang J, Xiong Y, Zhu G. (2014), Data Security and Privacy in Cloud Computing. International Journal of Distributed Sensor Networks. 10(7). doi:10.1155/190903

[9] Nesrine Kaaniche, Maryline Laurent, (2017), Data security and privacy preservation in cloud storage environments based on cryptographic mechanisms, Computer Communications, Volume 111, Pages 120-141, ISSN 0140-3664, https://doi.org/10.1016/j.comcom.2017.07.006.

[10] Perwej, Dr. Yusuf & Abbas, Qamar & Dixit, Jai & Akhtar, Nikhat & Jaiswal, Anurag. (2021). A Systematic Literature Review on the Cyber Security. International Journal of Scientific Research and Management. Volume 9. Pages 669 - 710. 10.18535/ijsrm/v9i12.ec04.

[11] Yuchong Li, Qinghui Liu, (2021), A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments, Energy Reports, Volume 7, Pages 8176-8186, ISSN 2352-4847, https://doi.org/10.1016/j.egyr.2021.08.126.

[12] Michael Robinson, Kevin Jones, Helge Janicke, (2015), Cyber warfare: Issues and challenges, computers & Security, Volume 49, Pages 70-94, ISSN 0167-4048, https://doi.org/10.1016/j.cose.2014.11.007.

[13] Gade, Nikhita Reddy & Reddy, Ugander. (2014). A Study Of Cyber Security Challenges And Its Emerging Trends On Latest Technologies.

[14] Internet live stats. [Internet] Available from: https://www.internetlivestats.com/ Accessed 3.14am 11/17/2023 [15] Sabillon R, Cavaller V, Cano J. (2016), National cyber security strategies: global trends in cyberspace. International Journal of Computer Science and Software Engineering. 5(5): 67.

[16] Fichtner L. (2018). What kind of cyber security? Theorising cyber security and mapping approaches. Internet Policy Review.; 7(2).

[17] Chowdhury (2016), A. Recent cyber security attacks and their mitigation approaches–an overview. In Applications and Techniques in Information Security: 6th International Conference, ATIS 2016, Cairns, QLD, Australia, October 26-28, 2016, Proceedings 7 (pp. 54-65)

[18] Amit Kumar Tyagi, N. Sreenath, (2021), Cyber Physical Systems: Analyses, challenges and possible solutions, Internet of Things and Cyber-Physical Systems, Volume 1, Pages 22-33, ISSN 2667-3452, https://doi.org/10.1016/j.iotcps.2021.12.002.

[19] Kenneth Kimani, Vitalice Oduol, Kibet Langat, (2019), Cyber security challenges for IoT-based smart grid networks, International Journal of Critical Infrastructure Protection, Volume 25, Pages 36-49, ISSN 18745482, https://doi.org/10.1016/j.ijcip.2019.01.001.

[20] Julian Jang-Jaccard, Surya Nepal, (2014), A survey of emerging threats in cybersecurity, Journal of Computer and System Sciences, Volume 80, Issue 5, , Pages 973-993, ISSN 0022-0000, https://doi.org/10.1016/j.jcss.2014.02.005.

[21] R.C. Newman (2009) Computer Security: Protecting Digital Resources (first edition), Jones & Bartlett Publishers (February 20,)

[22] http://www.welivesecurity.com/2012/12/11/trends-for-2013-astounding- growth-of-mobile-malware/ Accessed at 1.43pm 16, November 2023

[23] N. Potlapally, (2011), Hardware security in practice: Challenges and opportunities, in: HOST pp. 93–98.

[24] Q. Li, H. Gao, B. Xu, Z. Jiao, (2008), Hardware threat: The challenge of information security, in: ISCSCT, pp. 517–520.

[25] Himmat, Mubarak & Ibrahim, Mnahel & Hammam, Nazar & Eldirdiery, Hassan & Algazoli, Ghadah.(2023), The Current Trends, Techniques, and Challenges of Cybersecurity. European Journal of Information Technologies and Computer Science. 3. 1-5. 10.24018/compute.2023.3.4.93.

[26] Saxena, N.; Hayes, E.; Bertino, E.; Ojo, P.; Choo, K.-K.R.; Burnap, P.(2020), Impact and Key Challenges of Insider Threats on Organizations and Critical Businesses. *Electronics 9*, 1460. https://doi.org/10.3390/electronics9091460

[27] Abdullah Al-Shomrani , Fathy Eassa, Kamal Jambi (2018) Big Data Security and Privacy Challenges King AbdulAziz University, Jeddah, Saudi Arabia Computer Science IJEDR1801155 International Journal of Engineering Development and Research (www.ijedr.org) 894 IJEDR | Volume 6, Issue 1 |

ISSN: 2321-9939 https://www.linkedin.com/pulse/cybersecurity-compliance-regulations-you-should-know-sa Accessed at 3.43pm 18, November 2023

[28] https://www.isaca.org/resources/isaca-journal/issues/2020/volume-3/practical-data-security-and-privacy-forgdpr-and-ccpa feguarding/ Accessed at 5.43pm 18, November 2023.

[29] Julian Jang-Jaccard, Surya Nepal, (2014) A survey of emerging threats in cybersecurity, Journal of Computer and System Sciences, Volume 80, Issue 5, 2014, Pages 973-993, ISSN 0022-0000, https://doi.org/10.1016/j.jcss.02.005.

[30] Arabo, Abdullahi. (2015). Cyber Security Challenges within the Connected Home Ecosystem Futures. Procedia Computer Science. 61. 227-232. 10.1016/j.procs.2015.09.201.

[31] Rajasekharaiah, K. & Dule, Chhaya & Sudarshan, Dr. (2020). Cyber Security Challenges and its Emerging Trends on Latest Technologies. IOP Conference Series: Materials Science and Engineering. 981. 022062. 10.1088/1757-899X/981/2/022062.

[32] Mohamed, Nachaat. (2023). Current trends in AI and ML for cybersecurity: A state-of-the-art survey. Cogent Engineering. 10. 10.1080/23311916.2023.2272358.

[33] Fagbohunmi, Griffin & Uche, Okafor. (2023). An improved model for comparing different endpoint detection and response tools for mitigating insider threat. Indian Journal of Engineering. 20. 1-13. 10.54905/disssi/v20i53/e22ije1651.

[34] Wu, Kehe & Cheng, Rui & Xu, Huiyan & Tong, Jie. (2023). Design and Implementation of the Zero Trust Model in the Power Internet of Things. International Transactions on Electrical Energy Systems. 2023. 1-13. 10.1155/2023/6545323.

[35] Onome Christopher Edo, Theophilus Tenebe, Egbe-Etu Etu, Atamgbo Ayuwu, Joshua Emakhu, and Shakiru Adebiyi. (2022) "Zero Trust Architecture: Trend and Impacton Information Security" International Journal of Emerging Technology and Advan: 140-147. https://doi.org/10.46338/ijetae0722_15

[36] Ahmad, S., Mehfuz, S., Mebarek-Oudina, F. *et al.* (2022). RSM analysis based cloud access security broker: a systematic literature review. *Cluster Comput* **25**, 3733–3763 https://doi.org/10.1007/s10586-022-03598-z [38] Domingo-Ferrer, Josep & Blanco-Justicia, Alberto. (2020). Privacy-Preserving Technologies. 10.1007/9783-030-29053-5_14.

[39] Mtsweni, J., Mutemwa, M., & Mkhonto, N. (2016). Development of a Cyber-Threat Intelligence-Sharing Model from Big Data Sources. *Journal of Information Warfare*, *15*(3), 56–68. https://www.jstor.org/stable/26502744

[40] Xiaolu Zhang, Oren Upton, Nicole Lang Beebe, Kim-Kwang Raymond Choo, (2020). IoT Botnet Forensics: A Comprehensive Digital Forensic Case Study on Mirai Botnet Servers, Forensic Science International: Digital Investigation, Volume 32, Supplement, 300926, ISSN 2666-2817, https://doi.org/10.1016/j.fsidi.2020.300926.

[41] Baezner, Marie & Robin, Patrice. (2018). Stuxnet.

[42] C. Miller (2018), "Lessons learned from hacking a car," in *IEEE Design & Test*, vol. 36, no. 6, pp. 7-9, , doi: 10.1109/MDAT..2863106. keywords: {Automotive engineering;Computer security;Computer crime;Computer hacking},

[43] https://jsis.washington.edu/news/cyberattack-critical-infrastructure-russia-ukrainian-power-grid-attacks/ accessed on 18, November 2023 at 8:30pm.

[44] https://www.nytimes.com/2019/12/15/us/Hacked-ring-home-security-cameras.html accessed on 19, November 2023 at 8:35pm.

[45] Elmaghraby, Adel & Losavio, Michael. (2014). Cyber Security Challenges in Smart Cities: Safety, security and privacy. Journal of Advanced Research. 5. 10.1016/j.jare.2014.02.006.

[46] Cremer F, Sheehan B, Fortmann M, Kia AN, Mullins M, Murphy F, Materne S. (2022) Cyber risk and cybersecurity: a systematic review of data availability. Geneva Pap Risk Insur Issues Pract. 2022;47(3):698736. doi: 10.1057/s41288-022-00266-6. Epub 2022 Feb 17. PMID: 35194352; PMCID: PMC8853293.

[47] Ramanpreet Kaur, Dušan Gabrijelčič, Tomaž Klobučar, (2023). Artificial intelligence for cybersecurity: Literature review and future research directions, Information Fusion, Volume 97, 2023, 101804, ISSN 15662535, https://doi.org/10.1016/j.inffus.2023.101804.

[48] Kilincer, I.F., F. Ertam, and A. Sengur. 2021. Machine learning methods for cyber security intrusion detection: Datasets and comparative study. *Computer Networks* 188: 16. https://doi.org/10.1016/j.comnet.2021.107840.

[49] Stojanovic, B., K. Hofer-Schmitz, and U. Kleb. 2020. APT datasets and attack modeling for automated detection methods: A review. *Computers & Security* 92: 19. https://doi.org/10.1016/j.cose.2020.101734.

[50] Tan, Z., A. Jamdagni, X. He, P. Nanda, R.P. Liu, and J. Hu. 2015. Detection of denial-of-service attacks based on computer vision techniques. *IEEE Transactions on Computers* 64 (9): 2519–2533. https://doi.org/10.1109/TC.2014.2375218.