International Journal of Research in Engineering and Innovation (IJREI)
journal home page: http://www.ijrei.com
ISSN (Online): 2456-6934

REVIEW ARTICLE

Securing the internet of things: challenges, strategies, and emerging trends in IoT Security Systems

Mohammed M. Sultan

Tikrit University, Iraq

Article Information

Received: 12 November 2023
Revised: 06 December 2023
Accepted: 17 December 2023
Available online: 27 December 2023

Keywords:

IoT Security
Data Confidentiality
Decentralized Identity Management
Interconnected Ecosystem

Abstract

The Internet of Things (IoT) has revolutionized how we interact with technology, enabling seamless connectivity among various devices. However, this interconnected ecosystem also presents significant security challenges that demand comprehensive solutions. This paper explores IoT security systems, focusing on understanding the unique challenges and devising effective strategies to mitigate risks. By analyzing the diverse landscape of IoT networks and protocols, we identify potential vulnerabilities and threats that could compromise integrity and data confidentiality. Additionally, we delve into emerging technologies and trends, such as blockchain-based solutions and decentralized identity management, which hold promise for enhancing IoT security.
Throughout the paper, we emphasize the importance of ongoing monitoring, prompt firmware updates, and efficient incident response strategies. Organizations can ensure compliance and create a more secure IoT environment by adhering to established regulatory frameworks and standards. This research paper serves as a comprehensive guide for practitioners and researchers, offering valuable insights into IoT security systems' challenges, best practices, and future directions.

1. Introduction

The rapid proliferation of interconnected devices in the Internet of Things (IoT) has transformed the way we interact with technology, enabling seamless connectivity and unprecedented convenience in various domains [1-5]. However, the pervasive nature of IoT introduces significant security challenges that demand immediate attention. As billions of devices become interconnected, the attack surface expands, and the potential risks associated with IoT vulnerabilities increase [6]. This paper focuses on understanding the unique security challenges faced by the IoT ecosystem and exploring effective strategies and emerging trends in IoT security systems. The diverse landscape of IoT networks and protocols presents potential vulnerabilities and threats that can compromise device integrity, data confidentiality, and user privacy. Unauthorized access, data interception, device spoofing, and denial-of-service attacks are some of the common security risks that need to be addressed. The consequences of IoT security breaches can be severe, including data breaches leading to financial losses, privacy violations, and disruption of critical services [7]. To address these challenges, an effective IoT security architecture is essential. It should encompass multiple layers, including device authentication, secure communication protocols, access control mechanisms, and robust data encryption [8]. Robust device authentication ensures that only authorized devices can access the network, mitigating the risk of unauthorized access and device spoofing. Secure communication protocols, such as Transport Layer Security (TLS) and Datagram Transport

Corresponding author: Mohammed M. Sultan
Email Address: mmsultan@tu.edu.iq
https://doi.org/10.36037/IJREI.2023.7607

Layer Security (DTLS), provide end-to-end encryption and integrity checks to protect data in transit [9] [10]. Access control mechanisms enable fine-grained control over device permissions and restrict unauthorized actions. Data encryption techniques, such as Advanced Encryption Standard (AES), protect sensitive information stored on IoT devices and in transit [11].

Furthermore, emerging technologies and trends hold promise for enhancing IoT security. Blockchain-based solutions offer decentralized and tamper-resistant mechanisms for secure transactions, identity management, and data integrity. Decentralized identity management systems provide enhanced control over user identities and reduce reliance on centralized authorities [12]. Additionally, the integration of artificial intelligence and machine learning techniques enables proactive threat detection and intelligent decision-making in real-time [13]. By addressing the unique challenges, implementing effective security measures, and staying abreast of emerging trends, organizations can mitigate risks and create a secure IoT environment. This research paper aims to provide valuable insights into the challenges, best practices, and future directions of IoT security systems, serving as a comprehensive guide for practitioners and researchers in this rapidly evolving field.

2. Challenges in IoT security systems

The security of IoT systems faces numerous challenges that arise from several aspects such as device heterogeneity, Resource Constraints, Scalability, Privacy Concerns, Network Vulnerabilities, Interoperability, Supply Chain Security, and Human Factors [14-17]. In the following, we discuss each challenge and solutions proposed to handle with the best practice to overcome it.

2.1 Device Heterogeneity

Device Heterogeneity is one of the significant challenges in IoT security systems, which refers to the wide variety of IoT devices with diverse capabilities, operating systems, and communication protocols. This heterogeneity poses challenges for implementing standardized security mechanisms and ensuring consistent security practices across different devices [18, 19]. Securing these heterogeneous devices requires tailored security approaches that can address their specific characteristics and limitations. For example, the authors of [20, 21] highlight the importance of secure firmware updates and secure boot processes to mitigate security risks in IoT devices. These processes ensure that devices have up-to-date and trusted software, reducing the likelihood of vulnerabilities being exploited. In addition, the implementation of standardized security protocols and frameworks is crucial to accommodate the diverse communication protocols used by IoT devices [22]. By adopting protocols such as Transport Layer Security (TLS) or Datagram Transport Layer Security (DTLS), device communication can be secured, regardless of the specific communication protocol employed. Moreover, device authentication mechanisms play a vital role in addressing the challenge of device heterogeneity. While the authors of [23] propose a blockchain-based IoT identity management system that can handle the authentication of heterogeneous devices in a distributed and interoperable manner. This approach ensures that only authorized devices can access the IoT network, mitigating the risk of unauthorized access. By considering the specific characteristics and requirements of heterogeneous IoT devices, including their varying capabilities, operating systems, and communication protocols, tailored security measures can be developed to effectively address the challenge of device heterogeneity in IoT security systems.

2.2 Resource Constraints

IoT devices often operate with limited computational power, memory, and energy resources [2]. These constraints pose challenges in implementing robust security measures while ensuring optimal device performance and energy efficiency. To address resource constraints, researchers have focused on developing lightweight security mechanisms and energy-aware security solutions [24]. For instance, Ali et al. [25] propose lightweight cryptographic algorithms that require fewer computational resources, enabling efficient encryption and decryption operations on resource-constrained devices. In addition, the design and implementation of lightweight security protocols are crucial to minimize memory usage and processing overhead on IoT devices. A various lightweight security protocols that provide essential security functionalities while optimizing resource consumption are discussed in [26] [27]. Furthermore, energy-aware security mechanisms aim to strike a balance between security requirements and energy efficiency. The research in [28] present a lightweight and privacy-preserving data aggregation scheme for fog-based IoT, which reduces communication overhead and energy consumption during data transmission and aggregation processes. Efficient management of security keys and credentials is another aspect to consider in resource-constrained IoT devices. Scalable key management schemes, such as those proposed by Dorri et al. [29], enable secure and efficient key distribution and revocation processes, considering the limitations of IoT devices. By considering the resource constraints of IoT devices and leveraging lightweight security mechanisms, energy-aware solutions, and scalable key management schemes, it is possible to address the challenge of resource constraints while ensuring effective security in IoT systems.

2.3 Scalability

The scalability challenge in IoT security systems refers to the ability to maintain effective security measures as the number of connected devices and the scale of IoT deployments increase. As IoT networks expand, the management of security credentials, access control policies, and security configurations become more complex and resource-intensive. To address the

scalability challenge, standardized security mechanisms and scalable key management schemes have been proposed. Abdmeziem et al. [30] discuss the importance of scalable and efficient key management protocols to establish secure communication between many IoT devices. These protocols enable the secure distribution and revocation of cryptographic keys, ensuring the confidentiality and integrity of data transmissions. Additionally, the adoption of cloud-based security solutions can provide scalability in managing security policies and configurations. Cloud-based security platforms, as discussed by Rehman et al. [31], offer centralized management and control of security functions, making it easier to update security policies and distribute security patches across many IoT devices. Furthermore, the utilization of blockchain technology has shown promise in addressing scalability concerns in IoT security. Khashan et al [32] propose a secure, distributed, and blockchain-based IoT identity management system that can handle authentication and access control for a large number of heterogeneous IoT devices in a scalable manner. By leveraging scalable key management protocols, cloud-based security platforms, and blockchain-based solutions, it is possible to overcome the scalability challenge in IoT security systems while ensuring the effective management of security credentials and configurations.

2.4 Privacy Concerns

Privacy is a critical aspect of IoT security systems as the widespread deployment of interconnected devices leads to the continuous collection, processing, and sharing of personal and sensitive data. This data includes personal identifiers, location information, health records, and behavioral patterns, raising concerns about unauthorized access, data breaches, and privacy violations. The unique characteristics of IoT, such as ubiquitous sensing and data aggregation, amplify the potential impact of privacy breaches. Consequently, addressing privacy concerns is crucial to foster trust and encourage widespread adoption of IoT technologies. To tackle privacy challenges in IoT, researchers have proposed various approaches. One notable solution is the utilization of blockchain technology, which offers decentralized and tamper-resistant data storage and access control mechanisms. Fernández-Caramés et al. [33] discuss the potential of blockchain in enhancing privacy in IoT systems. By leveraging distributed ledgers, data can be securely stored and accessed, ensuring transparency and reducing the reliance on centralized authorities. Blockchain-based systems can empower users to have control over their personal data, enabling them to define access permissions and monitor data usage. Additionally, user-centric privacy protection methods have been investigated to address privacy concerns in IoT deployments. Authors of [34] present a user-centric privacy protection framework that emphasizes empowering users with control over their personal data. The framework advocates for transparent privacy controls, informed consent mechanisms, and user-friendly interfaces to provide users with visibility and choice over the data collected by IoT devices. By placing individuals at the center of privacy protection, this approach promotes privacy-aware practices and enhances user trust in IoT systems. Furthermore, privacy-enhancing technologies, such as differential privacy and secure multi-party computation, have been explored to mitigate privacy risks in IoT environments [35] [36]. These techniques aim to preserve data privacy while allowing meaningful analysis and data sharing among authorized parties. Researchers have proposed integrating these privacy-preserving mechanisms into IoT systems to strike a balance between data utility and privacy protection. By combining blockchain technology, user-centric privacy protection frameworks, and privacy-enhancing technologies, privacy concerns in IoT security systems can be effectively addressed. These approaches contribute to building a privacy-aware IoT ecosystem that respects individuals' privacy rights and ensures secure and responsible data handling practices.

2.5 Network Vulnerabilities

Network vulnerabilities pose a significant challenge in IoT security systems, considering the vast number of interconnected devices and the diverse communication infrastructure involved. The interconnected nature of IoT devices and the transmission of sensitive data across networks make them susceptible to various types of attacks, including unauthorized access, eavesdropping, data tampering, and denial-of-service attacks [37]. To address network vulnerabilities, researchers have proposed several approaches. One key aspect is the implementation of robust authentication and access control mechanisms. Efficient authentication protocols, such as lightweight mutual authentication schemes, can validate the identity of IoT devices and ensure that only authorized devices gain access to the network [38]. Access control mechanisms, such as role-based access control and attribute-based access control, help enforce fine-grained authorization policies, limiting device access to specific resources. Securing data transmission is another critical aspect of addressing network vulnerabilities. Utilizing secure communication protocols, such as Transport Layer Security (TLS) or Datagram Transport Layer Security (DTLS), can provide end-to-end encryption and integrity checks for data exchanged between IoT devices and backend systems [10]. Additionally, intrusion detection and prevention systems can be deployed to monitor network traffic, detect malicious activities, and respond promptly to potential threats. Furthermore, network segmentation and isolation techniques can help contain the impact of attacks and prevent lateral movement within IoT networks. By dividing the network into smaller segments and implementing strong network segmentation policies, the potential attack surface is reduced, limiting the propagation of threats across IoT devices [8]. Continuous monitoring and vulnerability management practices are essential to detect and address network vulnerabilities. Regular security assessments, including penetration testing and vulnerability scanning, can identify potential weaknesses in the network infrastructure and IoT devices, enabling proactive mitigation measures. By

implementing robust authentication and access control mechanisms, utilizing secure communication protocols, adopting network segmentation techniques, and implementing continuous monitoring practices, network vulnerabilities in IoT security systems can be effectively addressed, enhancing the overall security posture of IoT deployments.

2.6 Interoperability

Interoperability is a significant challenge in IoT security systems due to the heterogeneous nature of IoT devices, protocols, and platforms. The diverse range of devices, each with different communication interfaces, data formats, and security mechanisms, makes it challenging to establish seamless and secure interactions among them. Ensuring interoperability is crucial for achieving cohesive and integrated IoT deployments. Researchers have proposed several approaches to address this challenge. One key aspect is the standardization of communication protocols and data formats. Standardization efforts, such as the Constrained Application Protocol (CoAP) and Message Queuing Telemetry Transport (MQTT), facilitate interoperability by providing common protocols for device communication and data exchange [39]. In addition to protocol standardization, semantic interoperability is essential for effective communication and collaboration among IoT devices. Semantic technologies, such as the Web Ontology Language (OWL) and Resource Description Framework (RDF), enable the representation and exchange of meaningful data and metadata, promoting interoperability at a semantic level [40]. Interoperability can also be improved by middleware platforms that provide abstraction layers and standard interfaces for connecting and managing heterogeneous devices. Middleware frameworks, such as the Open Connectivity Foundation (OCF) and the IoTivity framework, enable interoperability by abstracting device-specific details and providing uniform APIs for device discovery, communication, and security [41]. Moreover, the adoption of interoperability testing and certification programs can help ensure compatibility and compliance with established standards. Certification programs, such as the Global Certification Forum (GCF) and the Zigbee Alliance Certification, validate the interoperability of IoT devices and provide assurance to users and stakeholders [42]. By promoting protocol standardization, semantic interoperability, middleware frameworks, and certification programs, the challenge of interoperability in IoT security systems can be effectively addressed. These approaches contribute to seamless device integration, data exchange, and collaboration within IoT ecosystems.

2.7 Human Factors Challenge

Human factors play a crucial role in the security of IoT systems as they involve the interactions between users, devices, and the overall IoT ecosystem. The behavior, awareness, and decision-making of individuals can significantly impact the security posture of IoT deployments. Understanding and addressing human factors are essential for promoting secure practices and mitigating risks associated with human error and malicious activities. One aspect of the human factors challenge is user awareness and education. Providing effective security awareness programs and educational resources can empower users to make informed decisions and adopt secure practices [43]. Training programs should cover topics such as device configuration, password management, and recognizing phishing. By improving users' security knowledge and awareness, the likelihood of falling victim to social engineering attacks and other common security threats can be reduced. Moreover, the usability of IoT devices and security mechanisms is critical in influencing users' behavior. Designing intuitive and user-friendly interfaces, coupled with clear security prompts and feedback, can encourage users to engage in secure practices. Additionally, incorporating user-centered design principles and conducting usability testing can help identify and address potential usability issues that may hinder security-conscious behaviors. Furthermore, the privacy and ethical considerations surrounding IoT data collection and usage are important human factors to consider. Users should have control over their personal data and be informed about the types of data collected, how it is used, and the associated privacy risks. Consent mechanisms and transparent privacy policies can promote user trust and engagement with IoT systems [44]. Respecting ethical principles, such as data minimization and purpose limitation, ensures responsible data handling practices in IoT deployments. Additionally, organizational culture and policies play a significant role in addressing human factors in IoT security. Creating a security-conscious culture that values and prioritizes cybersecurity can foster a proactive approach to security among employees and stakeholders. Well-defined security policies, incident response plans, and ongoing training programs can help reinforce secure behaviors and ensure compliance with security protocols. By addressing human factors through user awareness and education, improving the usability of IoT devices and security mechanisms, considering privacy and ethical implications, and promoting a security-conscious organizational culture, the challenges associated with human factors in IoT security systems can be effectively mitigated.

2.8 Supply Chain Security User Challenge

Supply chain security is a critical aspect of IoT systems, as it involves the procurement, manufacturing, distribution, and maintenance of IoT devices and components. Users face specific challenges in ensuring the security of their IoT devices throughout the supply chain lifecycle. One challenge is the trustworthiness of the supply chain. Users need to trust that the devices they purchase are genuine and have not been tampered with during the manufacturing or distribution process. Counterfeit or compromised devices can introduce vulnerabilities and compromise the overall security of the IoT system. Therefore, establishing trusted supply chain processes and engaging with reputable manufacturers, suppliers, and distributors is essential [45]. Another challenge is the lack of

visibility into the supply chain. Users often have limited visibility into the various stages of the supply chain, making it difficult to assess the security practices employed by different stakeholders. Supply chain transparency is crucial to identify potential security risks, such as unauthorized modifications or malicious insertions of hardware or software components. Promoting supply chain transparency through mechanisms like third-party audits and certifications can enhance users' confidence in the security of their IoT devices. Furthermore, users face challenges in maintaining the security of IoT devices over their operational lifespan. This includes ensuring timely firmware updates, patch management, and vulnerability remediation. Device manufacturers play a vital role in providing regular security updates, but users must actively apply these updates to their devices. Establishing effective update mechanisms, providing clear instructions, and raising user awareness about the importance of updates can help address this challenge. Additionally, users need to consider the disposal or end-of-life phase of their IoT devices from a security perspective. Improper disposal can lead to potential data breaches or unauthorized access to sensitive information. User education on secure device disposal practices, including data sanitization and responsible recycling, is crucial to mitigate these risks [46]. Addressing supply chain security challenges from a user perspective requires establishing trust in the supply chain, enhancing visibility, ensuring timely updates, and promoting secure device disposal practices. These measures contribute to a more secure and resilient IoT.

3. Security Measures and Best Practices

Ensuring the security of IoT systems is of paramount importance due to the sensitive nature of the data being transmitted and processed. The widespread adoption of IoT has introduced a complex and interconnected ecosystem, making IoT networks an attractive target for cybercriminals. A breach in IoT security can lead to severe consequences, including data breaches, privacy violations, disruption of critical services, and physical harm. To address these challenges, it is crucial to implement robust security measures and adhere to best practices throughout the lifecycle of IoT systems which can be summarize through the following steps:

Firstly, security by design principles should be followed, integrating security features from the early stages of IoT system development. This approach ensures that security considerations are not an afterthought but an integral part of the system architecture. By considering security requirements and conducting thorough threat modeling during the design phase, potential vulnerabilities can be identified and mitigated proactively [27]. Secure software development practices are essential for building resilient IoT systems. Adhering to coding standards, conducting secure code reviews, and performing rigorous testing can help identify and address software vulnerabilities. Secure development frameworks and methodologies, such as the Open Web Application Security Project (OWASP), can guide developers in building secure IoT applications. Proper configuration and management of IoT devices and infrastructure are critical. Default credentials should be changed, unnecessary services and ports should be disabled, and regular security patches and updates should be applied. Robust device management protocols, such as the Lightweight M2M (LwM2M) protocol, facilitate secure device provisioning, configuration, and firmware updates [47]. Continuous monitoring and incident response are vital components of IoT security. Implementing robust monitoring mechanisms enables the detection of potential security incidents or anomalies in real-time. Security information and event management (SIEM) solutions centralize logs and provide insights into security events. Establishing an effective incident response plan with predefined procedures and roles can minimize the impact of security breaches and ensure timely mitigation. User education and awareness play a critical role in IoT security. Educating users about security best practices, such as strong passwords, regular updates, and cautious sharing of personal information, helps reduce the risk of attacks. Providing user-friendly interfaces and clear instructions for device setup and configuration can enhance security awareness and usability. By implementing these security measures and best practices, organizations can significantly improve the security posture of their IoT systems and mitigate potential risks.

4. Emerging Trends and Future Directions

In addition to addressing the current challenges and implementing best practices, it is crucial to consider emerging trends and future directions in IoT security. By staying ahead of potential threats and leveraging innovative solutions, organizations can proactively enhance the security of their IoT systems. This section explores some notable emerging trends and provides insights into future directions for IoT security.

4.1 Machine Learning and Artificial Intelligence (AI) in IoT Security

These techniques are gaining traction in the field of IoT security. These technologies can analyze vast amounts of data collected from IoT devices, identify patterns, and detect anomalies or potential security breaches in real-time. Machine learning algorithms can aid in behavioral analysis, anomaly detection, and threat intelligence, enhancing the overall security posture of IoT systems [48].

4.2 Blockchain Technology for Secure Transactions

It offers potential solutions for ensuring secure and transparent transactions in IoT systems. By leveraging the decentralized and tamper-resistant nature of blockchain, IoT devices can securely exchange data and establish trust without the need for intermediaries. Blockchain-based smart contracts enable secure and automated execution of IoT transactions, reducing the risk of fraud and unauthorized access [49].

4.3 Secure device-to-cloud communication

As the number of connected devices increases, securing the communication between IoT devices and cloud platforms becomes paramount. Techniques such as secure end-to-end encryption, mutual authentication, and secure tunneling protocols like Transport Layer Security (TLS) ensure the confidentiality and integrity of data transmitted between IoT devices and cloud infrastructure [50].

4.4 Privacy-preserving techniques in IoT

Privacy concerns are a significant aspect of IoT security. Emerging privacy-preserving techniques aim to protect sensitive user data while enabling efficient data analysis. Differential privacy, homomorphic encryption, and secure multi-party computation techniques provide means to perform data analysis on encrypted data, minimizing the risk of data exposure and privacy breaches.

4.5 Security standards and regulatory frameworks

To establish a strong foundation for IoT security, the development and adoption of security standards and regulatory frameworks are essential. Collaborative efforts between industry stakeholders and policymakers are necessary to define guidelines, certifications, and compliance frameworks that ensure consistent security practices across IoT deployments. Examples of existing standards include the ISO/IEC 27000 series, NIST Cybersecurity Framework, and IoT security guidelines from organizations like the Industrial Internet Consortium (IIC) [51]. By exploring these emerging trends and considering future directions, organizations can proactively address evolving security challenges in the dynamic IoT landscape. By embracing innovative technologies, collaborating on standardization efforts, and continuously improving security practices, the potential of IoT can be fully realized while ensuring the confidentiality, integrity, and availability of IoT

5. Conclusions

In conclusion, this research paper provides a comprehensive and unique perspective on IoT security. While several papers have explored various aspects of IoT security, our paper stands out for its comprehensive analysis of the challenges, effective strategies, and emerging trends in securing IoT systems. What sets our paper apart is its holistic approach to IoT security. We not only delve into the technical challenges but also emphasize the significance of human factors, supply chain security, and interoperability. By addressing a wide range of challenges, it provides a comprehensive understanding of the complexities involved in securing IoT deployments, making it a valuable resource for organizations seeking to enhance their IoT security posture. We identified various challenges that organizations must overcome to secure IoT deployments. These challenges include device heterogeneity, resource constraints, scalability, privacy concerns, network vulnerabilities, interoperability, human factors, and supply chain security. Understanding these challenges is crucial for developing comprehensive security measures and adopting a proactive approach to mitigate risks. To address these challenges, we proposed a range of strategies and best practices. These include implementing strong authentication mechanisms, employing secure communication protocols, enforcing access control mechanisms, and applying robust data encryption. Additionally, we highlighted the importance of continuous monitoring, prompt firmware updates, and efficient incident response strategies. By adhering to established regulatory frameworks and standards, organizations can ensure compliance and create a more secure IoT environment. Moreover, we discussed emerging trends and future directions in IoT security systems. These trends include the integration of Machine Learning (ML) and Artificial Intelligence (AI) techniques, federated learning for privacy preservation, explainable AI for transparent decision-making, and collaborative threat intelligence sharing. These trends hold promise for enhancing the effectiveness and resilience of IoT security systems, enabling proactive threat detection, and improving incident response capabilities.

In conclusion, securing the Internet of Things requires a multi-faceted approach that addresses the unique challenges and complexities of this interconnected landscape. By implementing effective strategies, organizations can mitigate risks and protect the confidentiality, integrity, and availability of IoT systems. Embracing emerging trends and staying informed about the evolving threat landscape will enable organizations to stay one step ahead and ensure the ongoing security of IoT deployments. By emphasizing the importance of collaboration, knowledge sharing, and ongoing research, this paper serves as a comprehensive guide for practitioners and researchers in the field of IoT security. It offers valuable insights into the challenges, best practices, and future directions of securing the Internet of Things, helping organizations build robust and resilient IoT systems in the face of evolving security threats.

References

[1] L. B. a. J. H. S. Farzad, "IoT technologies for embedded computing: A survey," in International Conference on Hardware/Software Codesign and System Synthesis (CODES+ ISSS), Pittsburg, 2016, doi:10.1145/2968456.2974004.

[2] O. B. a. S. B. G. Pradyumna, "Introduction to IOT," International Advanced Research Journal in Science, Engineering and Technology, vol. 5, no. 1, pp. 41-44, 2018, doi:10.17148/IARJSET.2018.515.

[3] M. J. D. W. M. H. B. Z. S. S. M. &. A. M. S. mdad, "Internet of things (IoT); security requirements, attacks and counter measures," Indonesian Journal of Electrical Engineering and Computer Science (IJEECS), vol. 18, no. 3, pp. 1520-1530, 2020, doi: 10.11591/ijeecs.v18.i3.pp1520-1530.

[4] A. T. S. A. M. S. Mohammed M. Sultan, "Design and implementation of an adaptive multilevel wireless," Indonesian Journal of Electrical Engineering and Computer Science, vol. 23, no. 3, pp. 1804-1813, 2021, doi: 10.11591/ijeecs.v23.i3.pp1804-1813.

[5] M. S. I. M. &. S. E. Alamsyah, "Internet of things–based vital sign monitoring system," International Journal of Electrical and Computer

Engineering (IJECE), vol. 10, no. 6, pp. 5891-5898, 2020, doi: 10.11591/ijece.v10i6.pp5891-5898.

[6] S. Bahizad, "Risks of increase in the iot devices," in In 2020 7th IEEE international conference on cyber security and cloud computing (CSCloud)/2020 6th IEEE international conference on edge computing and scalable cloud (EdgeCom), IEEE, 2020, doi: 10.1109/CSCloud-EdgeCom49738.2020.00038.

[7] H. F. &. W. G. B. Atlam, "IoT security, privacy, safety and ethics," Digital twin technologies and smart cities, pp. 123-149, 2020, doi: 10.1007/978-3-030-18732-3_8.

[8] O. I. A. E. O. A. M. A. R. S. &. A. H. Abiodun, "A Review on the Security of the Internet of Things: Challenges and Solutions," Wireless Personal Communications, vol. 119, pp. 2603-2637, 2021, doi: 10.1007/s11277-021-08348-9.

[9] J. M. E. &. S. J. S. Granjal, "End-to-end transport-layer security for Internet-integrated sensing applications with mutual and delegated ECC public-key authentication," in 2013 IFIP Networking Conference, IEEE, 2013, ISBN:978-3-901882-55-5.

[10] A. Z. X. W. J. &. L. X. Bhattacharjya, "CoAP—application layer connection-less lightweight protocol for the Internet of Things (IoT) and CoAP-IPSEC Security with DTLS Supporting CoAP.," in Digital Twin Technologies and Smart Cities, Springer, 2020, doi: 10.1007/978-3-030-18732-3_9, pp. 151-175.

[11] R. W. G. &. L. A. M. Atiqur, "Mobile edge computing for internet of things (IoT): security and privacy issues," Indonesian Journal of Electrical Engineering and Computer Science (IJEECS), vol. 18, no. 3, pp. 1486-1493, 2020, doi: 10.11591/ijeecs.v18.i3.pp1486-1493.

[12] S. R. H. Z. H. K. &. V. F. Ismail, "A Blockchain-based IoT Security Solution Using Multichain," in In 2023 IEEE 13th Annual Computing and Communication Workshop and Conference (CCWC) (pp. 1105-1111), IEEE, 2023, doi: 10.1109/CCWC57344.2023.10099128.

[13] M. R. M. M. A. S. P. &. G. S. K. Mahmood, "A comprehensive review on artificial intelligence/machine learning algorithms for empowering the future IoT toward 6G era," IEEE Access, Vols. 87535-87562, p. 10, 2022, doi: 10.1109/ACCESS.2022.3199689.

[14] C. Sobin, "A Survey on Architecture, Protocols and Challenges in IoT," Wireless Personal Communications, vol. 112, no. 3, pp. 1383-1429, 2020, doi: 10.1007/s11277-020-07108-5.

[15] A. Karale, "The Challenges of IoT Addressing Security, Ethics, Privacy, and Laws," Internet of Things, vol. 15, p. 100420, 2021, doi: 10.1016/j.iot.2021.100420.

[16] A. K. G. G. M. K. B. M. L. Shikha Mathur, "A Survey on Role of Blockchain for IoT: Applications and Technical Aspects," Computer Networks, vol. 227, p. 109726, 2023, doi: 10.1016/j.comnet.2023.109726.

[17] P. K. M. Chanal, "Security and Privacy in IoT: A Survey," Wireless Personal Communications, vol. 15, pp. 1667-1693, 2020, doi: 10.1007/s11277-020-07649-9.

[18] A. V. R. &. K. S. Pandey, "Handling device heterogeneity and orientation using multistage regression for GMM based localization in IoT networks," IEEE Access, vol. 7, pp. 144354-144365, 2019, doi: 10.1109/ACCESS.2019.2945539.

[19] T. A. N. &. S. W. Park, "Learning how to communicate in the Internet of Things: Finite resources and heterogeneity.," IEEE Access, vol. 4, p. IEEE Access, 2016, doi: 10.1109/ACCESS.2016.2615643.

[20] K. S. K. A. F. T. H. &. B. E. Zandberg, "Secure firmware updates for constrained iot devices using open standards: A reality check," IEEE Access, vol. 7, pp. 71907-71920, 2019, doi: 10.1109/ACCESS.2019.2919760.

[21] A. S. G. Y. &. S. F. Siddiqui, "Secure Boot for Reconfigurable Architectures," Cryptography, vol. 4, no. 26, p. 4, 2020, doi: 10.3390/cryptography4040026.

[22] S. C. R. Yugha, "A survey on technologies and security protocols: Reference for future generation IoT," Journal of Network and Computer Applications, vol. 169, p. 102763, 2020, doi: 10.1016/j.jnca.2020.102763.

[23] K. C. a. I. R. B. Alamri, "Blockchain-Based Identity Management Systems in Health IoT: A Systematic Review," IEEE Access, vol. 10, pp. 59612-59629, 2022, doi: 10.1109/ACCESS.2022.3180367.

[24] J. O. A. G. S. K. J. O. B. Jerry John Kponyo, "Lightweight and host-based denial of service (DoS) detection and defense mechanism for resource-constrained IoT devices," Internet of Things, vol. 12, p. 100319, 2020, doi: 10.1016/j.iot.2020.100319.

[25] F. K. &. M. S. Ali, "An efficient lightweight key exchange algorithm for internet of things applications," International Journal of Electrical and Computer Engineering (IJECE), vol. 12, no. 5, p. 5609~5618, 2022, doi: 10.11591/ijece.v12i5.pp5609-5618.

[26] E. -H. Y. a. J. W. X. -W. Wu, "Lightweight security protocols for the Internet of Things," in 2017 IEEE 28th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC), Montreal, QC, Canada, 2017, doi: 10.1109/PIMRC.2017.8292779.

[27] A. G. M. M. M. A. M. &. A. M. Al-Fuqaha, "Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications," IEEE Communications Surveys & Tutorials, vol. 17, no. 4, pp. 2347-2376, 2015, doi: 10.1109/COMST.2015.2444095.

[28] K. H. A. H. L. a. A. A. G. R. Lu, "A Lightweight Privacy-Preserving Data Aggregation Scheme for Fog Computing-Enhanced IoT," IEEE Access, vol. 5, pp. 3302-3312, 2020, doi: 10.1109/ACCESS.2017.2677520.

[29] A. K. S. S. J. R. &. G. P. Dorri, "Blockchain for IoT Security and Privacy: The Case Study of a Smart Home," in 2017 IEEE international conference on pervasive computing and communications workshops (PerCom workshops), IEEE, 2017, doi: 10.1109/PERCOMW.2017.7917634.

[30] M. C. F. Abdmeziem, "Fault-Tolerant and Scalable Key Management Protocol for IoT-Based Collaborative Groups," in Security and Privacy in Communication Networks: SecureComm 2017 International Workshops, ATCS and SePrIoT, Niagara Falls, ON, Canada, October 22–25, 2017, Proceedings 13, Springer International Publishing, 2018, doi: 10.1007/978-3-319-78816-6_22.

[31] N. J. M. A. M. I. a. N. N. M. Rehman, "Cloud Based Secure Service Providing for IoTs Using Blockchain," in 2019 IEEE Global Communications Conference (GLOBECOM), Waikoloa, 2019, doi: 10.1109/GLOBECOM38437.2019.9013413.

[32] N. M. K. Osama A. Khashan, "Efficient hybrid centralized and blockchain-based authentication architecture for heterogeneous IoT systems," Journal of King Saud University - Computer and Information Sciences, vol. 35, no. 2, pp. 726-739, 2023, doi: 10.1016/j.jksuci.2023.01.011.

[33] T. M. F.-C. a. P. Fraga-Lamas, "A Review on the Use of Blockchain for the Internet of Things," IEEE Access, vol. 6, pp. 32979-33001, 2018, doi: 10.1109/ACCESS.2018.2842685.

[34] C. &. B. M. Villarán, "User-Centric Privacy for Identity Federations Based on a Recommendation System," Electronics , vol. 11, no. 8, p. 1238, 2022, doi: 10.3390/electronics11081238.

[35] H. Goyal and S. Saha, "Multi-Party Computation in IoT for Privacy-Preservation," in 2022 IEEE 42nd International Conference on Distributed Computing Systems (ICDCS), Bologna, Italy, 2022, doi: 10.1109/ICDCS54860.2022.00133.

[36] Y. W. L. W. J. &. L. C. Yang, "Block-SMPC: a blockchain-based secure multi-party computation for privacy-protected data sharing," in Proceedings of the 2020 The 2nd International Conference on Blockchain Technology, 2020, doi: 10.1145/3390566.3391664.

[37] J. C. M. a. M. A. B. D. Davis, "Vulnerability Studies and Security Postures of IoT Devices: A Smart Home Case Study," IEEE Internet of Things Journal, vol. 7, no. 10, pp. 10102-10110, 2020, doi: 10.1109/JIOT.2020.2983983.

[38] A. J. S. A. M. &. M. A. Ben Amor, "A secure lightweight mutual authentication scheme in social industrial IoT environment," The Journal of Supercomputing, vol. 79, p. 13578–13600 , 2023, doi: 10.1007/s11227-023-05176-5.

[39] Z. H. K. &. B. Shelby, "The Constrained Application Protocol (CoAP)," RFC 7252. IETF, 2014.

[40] C. P. &. C. A. A. Vandana, "Semantic ontology based IoT-resource description," International Journal of Advanced Networking and Applications, vol. 11, no. 1, pp. 4184-4189, 2019.

[41] A. R. R. A. D. H. K. Anam Nawaz Khan, "An OCF-IoTivity enabled smart-home optimal indoor environment control system for energy and comfort optimization," Internet of Things, vol. 22, p. 100712, 2023, doi: 10.1016/j.iot.2023.100712.

[42] Zigbee Alliance. (n.d.)," [Online]. Available: https://zigbeealliance.org/.

[43] V. G. C. H. A. D. d. R. M. B. K. &. F. T. Schrama, "Understanding the Knowledge Gap: How Security Awareness Influences the Adoption of Industrial IoT," 20th Annual Workshop on the Economics of Information Security (WEIS 2020), pp. 1-17, 2020.

[44] Y. a. Y. Y. a. S. N. Feng, "A Design Space for Privacy Choices: Towards Meaningful Privacy Control in the Internet of Things," in In Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems (CHI '21), New York, 2021, doi: 10.1145/3411764.3445148.

[45] V. C. V. G. S. J. a. N. G. V. Hassija, "A Survey on Supply Chain Security: Application Areas, Security Threats, and Solution Architectures," IEEE Internet of Things Journal, vol. 8, no. 8, pp. 6222-6246, 2021, doi: 10.1109/JIOT.2020.3025775.

[46] S. S. R. J. J. &. S. S. Gowri, "IoT forensics: What kind of personal data can be found on discarded, recycled, or re-sold IoT devices," Journal of Discrete Mathematical Sciences and Cryptography, vol. 25, no. 4, pp. 999-1008, 2022, doi: 10.1080/09720529.2022.2072422.

[47] M. S. &. S. B. R. Shankar, "Incorporating OMA LWM2M for Firmware Update," International Journal of Innovative Research in Applied Sciences and Engineering (IJIRASE), vol. 4, no. 4, 2020, doi: 10.29027/IJIRASE.v4.i4.2020.699-703.

[48] H. K. P. S. Syeda Manjia Tahsien, "Machine learning based solutions for security of Internet of Things (IoT): A survey," Journal of Network and Computer Applications, vol. 161, no. , p. 102630, 2020, doi: 10.1016/j.jnca.2020.102630.

[49] Y. L. a. L. L. L. D. Xu, "Embedding Blockchain Technology Into IoT for Security: A Survey," IEEE Internet of Things Journal, vol. 8, no. 3, pp. 10452-10473, 2021, doi: 10.1109/JIOT.2021.3060508.

[50] N. C. W. J. C. M. B. P. A. P. a. K. C. G. D. C. G. Valadares, "Systematic Literature Review on the Use of Trusted Execution Environments to Protect Cloud/Fog-Based Internet of Things Applications," IEEE Access, vol. 9, pp. 80953-80969, 2021, doi: 10.1109/ACCESS.2021.3085524.

[51] M. Malatji, "Management of enterprise cyber security: A review of ISO/IEC 27001:2022," in 2023 International Conference On Cyber Management And Engineering (CyMaEn), Bangkok, Thailand, 2023, doi: 10.1109/CyMaEn57228.2023.10051114

Cite this article as: Mohammed M. Sultan, Securing the internet of things: challenges, strategies, and emerging trends in IoT Security Systems, International Journal of Research in Engineering and Innovation Vol-7, Issue-6 (2023), 266-273. *https://doi.org/10.36037/IJREI.2023.7607*.