Protection of IoT networks: cryptographic solutions for cybersecurity management

Emil Faure[1,2,*,†], Inna Rozlomii[1,†], Andrii Yarmilko[3,†] and Serhii Naumenko[3,†]

[1] *Cherkasy State Technological University, Shevchenko Blvd., 460, Cherkasy, 18006, Ukraine*

[2] *State Scientific and Research Institute of Cybersecurity Technologies and Information Protection, M. Zaliznyaka Str., 3 (6), Kyiv, 03142, Ukraine*

[3] *Bohdan Khmelnytsky National University of Cherkasy, Shevchenko Blvd., 81, Cherkasy, 18031, Ukraine*

Abstract

In the modern world, where the Internet of Things (IoT) is gaining increasing prevalence and importance, the issue of data security becomes a key challenge for both organizations and individual users. With the growing number of IoT devices and the deepening of their interactions, there is an increased need to develop reliable protection mechanisms, especially in the context of rising cyber threats and conflicts. This article focuses on exploring the challenges and potential protection strategies for IoT infrastructure in the current environment of growing quantity and sophistication of cyberattacks. The authors concentrate on a detailed analysis of both traditional and innovative encryption methods adapted to the resource constraints of IoT devices. Special attention is given to lightweight encryption, identified as a key tool for data protection while maintaining high device performance. The critical priorities of lightweight encryption are linked to its ability to provide effective data protection while simultaneously reducing demands on computational resources, which is crucial considering the limited capabilities of IoT devices. The article thoroughly examines the current state of IoT infrastructure, the challenges it faces, and the role of lightweight encryption in managing and minimizing the risks of cyber incidents. The authors also discuss in detail the possibilities of integrating lightweight encryption into the IoT architecture, revealing its impact on ensuring overall system security. The article contributes to the field by proposing a mathematical model for assessing risks associated with cyber incidents and illustrates how encryption can be effectively integrated at various levels of the IoT architecture. This aids in developing a comprehensive approach to protection in the face of constant growth and evolution of cyber threats.

Keywords

internet of things, cybersecurity, lightweight encryption, data protection, IoT architecture, cyber incident, resource constraints, cryptographic algorithms

1. Introduction

In the modern world, the Internet of Things (IoT) is gaining increasing significance. The development of IoT has brought numerous advantages across various domains, from smart homes to industrial systems. However, with the rapid growth in the number of IoT devices, the incidents of cyber threats also increase, posing a threat to data security and user privacy. There is a continual increase in the complexity and power of attacks, necessitating the enhancement of existing cybersecurity methods. This is particularly crucial in high-risk sectors such as education, healthcare, and industry. Undoubtedly, the issue of security in IoT becomes more critical as these technologies become more prevalent in everyday life and production.

Considering the mentioned challenges, it is essential to develop and implement effective data protection mechanisms in IoT networks, especially in the context of cyber incidents [1, 2]. One

CH&CMiGIN'24: Third International Conference on Cyber Hygiene & Conflict Management in Global Information Networks, January 24–27, 2024, Kyiv, Ukraine

* Corresponding author.

† These authors contributed equally.

e.faure@chdtu.edu.ua (E. Faure); inna-roz@ukr.net (I. Rozlomii); a-ja@ukr.net (A. Yarmilko); naumenko.serhii1122@vu.cdu.edu.ua (S. Naumenko)

0000-0002-2046-481X (E. Faure); 0000-0001-5065-9004 (I. Rozlomii); 0000-0003-2062-2694 (A. Yarmilko); 0000-0002-6337-1605 (S. Naumenko)

approach to data protection is the use of lightweight encryption, taking into account the limited computational capabilities of most IoT devices [3]. This method not only ensures reliable data protection but also maintains a high level of device performance.

The significance of lightweight encryption in the context of IoT is heightened with the increasing number of cyber attacks [4, 5]. Utilizing this method helps reduce the risks of cyber incidents while ensuring the effectiveness of the primary functionalities and energy efficiency of IoT devices.

The aim of this research is a systematic analysis of contemporary approaches to cryptographic protection, specifically the implementation of lightweight encryption, in IoT networks. This includes identifying their advantages and disadvantages and developing recommendations for their practical application to enhance cybersecurity. The focus is on assessing the effectiveness of various lightweight encryption methods in managing cyber incidents and conflicts in IoT networks.

2. Related works

The analysis of IoT system security has been a focal point of researchers' attention for quite some time [6]. In recent years, the problem has deepened, as illustrated in Figure 1, depicting the trend of cyber incidents in IoT networks based on data from the analytical report by Check Point Research [7]. As evident, the number of such incidents has multiplied significantly over six years. This trend underscores the growing need for the development and implementation of more effective security measures in IoT networks.

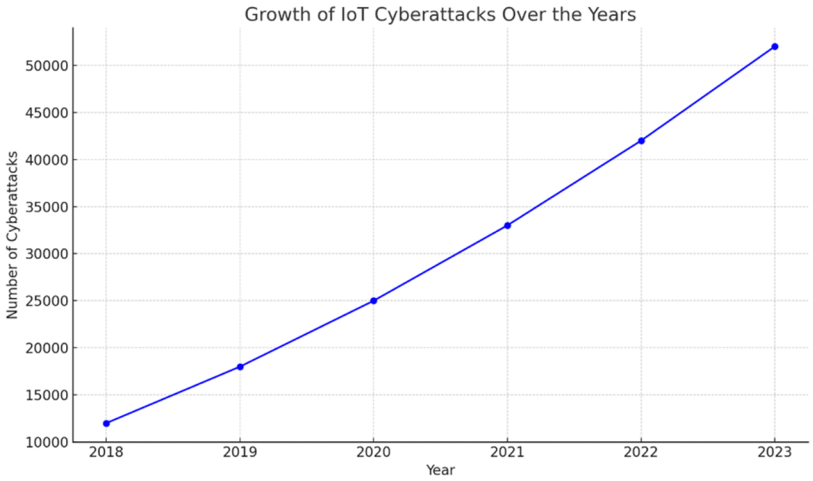

Figure 1: Dynamics of cyber incidents growth in IoT networks from 2018 to 2023.

One of the crucial aspects of studying the impact of cyber incidents in the IoT domain is analyzing the distribution of these incidents across various economic sectors. It is essential to understand which industries are most vulnerable to cyber attacks to identify key areas for improving security measures and developing protection strategies. Utilizing data from Check Point Research [7], we have created a diagram illustrating the percentage distribution of cyber incidents across different sectors, such as education, banking services, and healthcare (Figure 2). As revealed, the most vulnerable sector is education, accounting for 40% of all cyber attacks in the IoT sphere. The banking services and healthcare sectors also experience significant impact, each constituting 30% of the total incidents. This statistic highlights the necessity of developing targeted security measures for each sector individually, considering their specific risks and vulnerabilities.

One of the key aspects highlighted in publications on IoT security is the challenges associated with implementing robust encryption under the constraints of IoT devices. For instance, the research by Mousavi and colleagues [8] emphasizes the need to optimize encryption algorithms to strike a balance between security and efficiency. Other studies underscore the importance of integrating encryption at various levels of IoT architecture to ensure comprehensive protection [9, 10].

Specifically, in the work [9], recommendations for securing each level of the IoT architecture are provided, along with a security module for overall monitoring of IoT security issues.

Simultaneously, several studies focus on analyzing contemporary cyber incidents and their impact on IoT networks. For example, the works of Mohammad [11] and Meneghello [12] demonstrate how weaknesses in IoT security can lead to serious system disruptions. These examples highlight the relevance of cybersecurity issues in the context of IoT and the need for the development of more effective encryption methods.

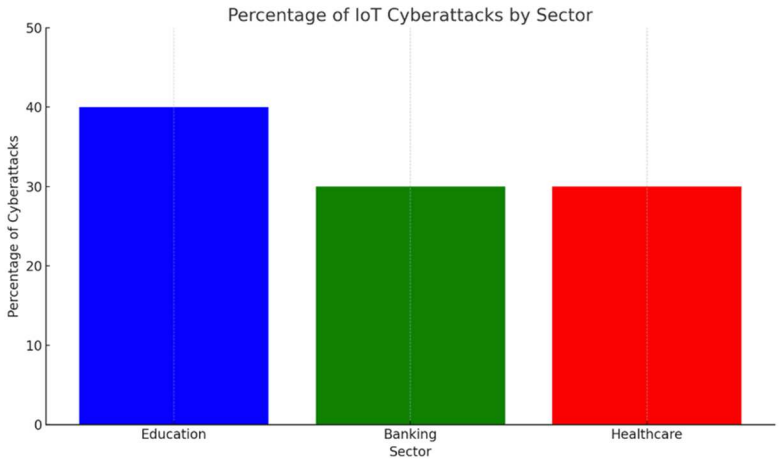

Figure 2: Distribution of cyber incidents in IoT networks across various economic sectors.

Analysis of information sources indicates that the significance of research in this direction is associated with the continually increasing number of cyber incidents in the IoT sphere, presenting new challenges for developers and system administrators. This necessitates the development of efficient encryption methods that cater to the unique requirements of IoT, such as limited computational resources and energy consumption characteristics. At the same time, it is crucial to ensure that these methods do not compromise the overall functionality and security of devices. Such an approach aims to minimize the risks associated with cyber attacks and ensure reliable data protection in IoT networks.

3. Foundations of lightweight encryption in IoT

Ensuring data security in the rapidly evolving field of IoT is becoming increasingly complex and critical [13]. Lightweight encryption plays a key role in protecting data transmitted and stored on IoT devices, which often have limited computational capabilities and constrained energy resources [14]. This section explores the methods of lightweight encryption, its principles, challenges, limitations, and advantages for IoT, considering the real-world constraints.

Lightweight encryption encompasses various cryptographic algorithms specifically designed or optimized for devices with constrained resources. They must provide data security while maintaining computational efficiency and energy consumption of the computing platform. Such algorithms include, for example, AES (Advanced Encryption Standard), but with optimizations that reduce computational power and memory requirements [15]. Lightweight algorithms like AES, DES, and other encryption variants have different levels of security and efficiency, which need to be carefully balanced for specific IoT applications [16].

3.1. Challenges and limitations in the IoT context

There are significant challenges associated with integrating lightweight encryption into IoT. In particular, the limited computational power and memory capacity of IoT devices complicate the use of traditional cryptographic methods [17, 18]. The issue of energy consumption is also crucial, as

most IoT devices operate from autonomous sources – batteries with limited power resources. Consequently, cryptographic algorithms must be highly efficient to minimize computation and storage costs [19, 20].

Therefore, the utilization of lightweight encryption in IoT is accompanied by unique challenges and limitations [21]. The primary ones include:

- Limited computational power and memory. Most IoT devices have significantly fewer computational resources compared to conventional computers.
- Energy constraints. IoT devices often operate on batteries or with energy-saving modes, limiting the available power for data processing.
- Ensuring security without compromising performance. It is essential to maintain a high level of security without compromising the performance of the devices.

The importance of researching these challenges and limitations has been emphasized in previous publications addressing this issue [22]. Based on this foundation, we can better understand why it is crucial to use specially designed or adapted ciphers for the IoT environment.

There is a certain set of lightweight ciphers that have undergone practical testing in IoT systems. Their parameters, presented in Table 1, demonstrate how various lightweight ciphers balance computational costs, memory usage, and energy consumption – critical parameters for IoT devices. It is essential to note that each cipher has unique characteristics that make it more or less suitable for specific usage scenarios in IoT.

Table 1
Modern Lightweight Ciphers Used in IoT

Cipher	Computational Costs	Memory Usage	Energy Consumption
SPECK	Low	Low	Low
SIMON	Medium	Low	Medium
Chaskey	Low	Low	Low
Ascon	Medium	Medium	Medium

3.2. Advantages of lightweight encryption for IoT

Despite the mentioned challenges, the advantages of lightweight encryption for IoT are significant. Lightweight encryption helps reduce the burden on systems while maintaining a reliable level of security. This includes the ability to operate efficiently even on devices with very limited capabilities, such as sensors and other simple IoT devices [23, 24]. This, in turn, paves the way for a safer and more extensive implementation of IoT technologies in various areas of life, from home systems to industrial networks.

Lightweight encryption offers a range of advantages that make it ideal for use in the IoT environment (Table 2). The most important advantages include:

- Energy Efficiency. Minimizing energy consumption is critical for IoT devices that operate on batteries.
- Resource Utilization Optimization. Lightweight ciphers can provide a reliable level of security using fewer computational and memory resources.
- Flexibility. Lightweight algorithms can be easily adapted to different types of devices and applications.

In addition to the advantages mentioned in Table 2, lightweight encryption for IoT also holds significant importance in the face of growing cybersecurity threats. Given the broad spectrum of IoT applications, ranging from home automation systems to industrial control networks, the need for

effective security mechanisms is critical. Lightweight encryption enables IoT system developers to ensure data and communication protection without compromising the functionality or energy efficiency of devices according to their intended purpose. This, in turn, contributes to a broader acceptance and trust in IoT technologies among users and enterprises, which is crucial for the further development of this field.

Table 2
Advantages of Lightweight Encryption for IoT

Benefit	Description
Energy Efficiency	Reduction of energy consumption
Resource Utilization Minimization	Minimization of resource usage
Flexibility	Adaptation to different usage conditions

4. Architecture of IoT and the application of encryption

The architecture of IoT serves as the foundation for understanding how encryption can be integrated into these systems. It encompasses a wide range of components, from end-user devices to cloud services and data processing [25]. Applying encryption at different levels of the IoT architecture ensures data protection at each stage of transmission and processing, which is crucial for securing these increasingly complex and interconnected systems.

The architecture of IoT may vary depending on the application and requirements, but there are certain common elements and principles that are widely accepted. These structures often include end devices (such as sensors and controllers), gateways for collecting and transmitting data, network infrastructures, and servers for processing and storing data.

4.1. Typical architectures of IoT

Architectures of IoT can be classified into several main types, each having its own features and encryption requirements.

4.1.1. Three-tier architecture

The three-tier architecture of IoT consists of the peripheral level (data collection devices), the network level (data transmission), and the cloud level (data processing) [26]. It is one of the simplest forms of IoT architecture, providing a clear separation between different functional components of the system.

In the three-tier IoT architecture, security at the peripheral level is ensured by device authentication and authorization, crucial for safeguarding the collected data. These procedures guarantee that only authorized devices have access to the network and can transmit data to the next level. After successful authentication, lightweight encryption is used to protect the data while maintaining the efficiency of devices with limited resources. Security at the network level is achieved through secure data transmission protocols, and at the cloud level, it involves protecting stored data and APIs.

4.1.2. Five-tier architecture

The five-tier architecture extends the three-tier model by adding processing and applications levels [27]. This modification allows for additional data management mechanisms and integration with various applications, from simple monitoring systems to complex analytical tools.

Thus, the five-tier IoT architecture, compared to the three-tier model, provides greater flexibility in data management and utilization. Encryption can be integrated at its additional structural levels to ensure confidentiality during data processing and analysis.

4.1.3. Fog computing architecture

The fog computing architecture is an evolution of cloud approaches, where data processing partially occurs on peripheral devices or gateways [28, 29]. Such solutions reduce delays and enhance real-time data processing efficiency.

Fog architecture implements data processing closer to the edge of the network, reducing delays and the bandwidth requirements of centralized servers. Encryption in fog architecture focuses on ensuring security at gateways and devices that serve as data processors [30].

Each of these architectures has its peculiarities concerning the application of encryption. It is crucial to understand how encryption can be integrated at different levels and points of the system to ensure the highest level of data security in IoT.

4.2. Integration of encryption across various levels of IoT architecture

Integration of encryption into the IoT architecture is a fundamental element for ensuring the confidentiality, integrity, and authenticity of data. The importance of this process lies in establishing a reliable protective shield for data at all levels: from end devices to cloud services.

Integrating encryption at various levels of IoT architecture not only ensures data protection but also serves as a safeguard against attacks and information leaks. In this context, innovation involves the development of multi-layered encryption systems tailored to the specifics of the IoT ecosystem, with a particular focus on scalability and energy efficiency.

At the end-device level, encryption should be lightweight to minimize resource usage. In the network layer, it is crucial to employ protocols with strong encryption for secure data transmission. At the processing and data storage level in the cloud, encryption should be dynamic, capable of rapid scalability. Table 3 details the features of encryption integration at each level of IoT architecture, allowing the identification of key security measures and encryption methods, their characteristics, and their impact on overall system security.

Table 3
Integration of Encryption into IoT Architecture

IoT Architecture Level	Security Measures	Encryption Method	Features
End Devices	Lightweight Encryption	Symmetric/Asymmetric	Resource Minimization
Network Layer	Secure Network Protocols	TLS/SSL	Data Transmission Protection
Cloud Services	Server-Side Data Encryption	SPECK, SIMON, Chaskey, Ascon	Data Storage and Processing Protection

Table 3 illustrates an integrated approach to encryption in the IoT architecture, covering three key levels: end devices, the network layer, and cloud services. Each level requires specific security measures tailored to its requirements and capabilities.

At the end-device level, the focus is on lightweight encryption, allowing data protection without significant burden on the limited computational resources of devices. This can be implemented using symmetric or asymmetric encryption depending on the needs and capabilities of end devices.

The network layer involves the use of secure network protocols such as TLS/SSL, ensuring data security during transmission. This is crucial for preventing data interception and other forms of network attacks.

Cloud services demand dynamic data encryption to protect information during storage and processing. The application of various encryption methods, such as SPECK, SIMON, Chaskey, Ascon, enables flexible and reliable protection against diverse threats.

The proposed security measures and encryption methods enable the creation of a multi-layered protective system that is scalable and adaptive to different IoT usage scenarios. Such an approach ensures comprehensive data protection at all stages of their lifecycle, from collection to analysis, with minimal impact on system performance and high energy efficiency.

4.3. Mathematical model of encryption integration into the IoT architecture

For the analysis of the proposed encryption integration model into the IoT architecture, let's consider a system consisting of a set of end nodes *N*, network gateways *G* and cloud servers *S*. Each node in the system $n \in N$ can communicate through gateways $g \in G$ with cloud servers $s \in S$, and each level has its encryption protocol.

1. Model for end devices. Let each end device n have a state vector x_n, which includes all device parameters, including its encryption key k_n. Then the encryption process for a message m_n can be represented as:
$$c_n = E(k_n, m_n), \quad (1)$$
where E is the encryption function.

2. Model for the network layer. For the network layer, introduce the function F_g, which maps the encryption process on the gateways:
$$c_g = F_g(\{n \in N_g\}), \quad (2)$$
where N_g is the set of nodes connected to the gateway g.

3. Model for cloud services. At the level of cloud services, introduce the function H_s, which maps the encryption process on the servers:
$$c_s = H_s(\{g \in G_s\}), \quad (3)$$
where G_s is the set of gateways connected to the server s.
This model allows analyzing the impact of encryption at each level and determining optimal configurations for maximum security and efficiency. The introduction of dynamic encryption functions F_g and H_s allows the system to adapt to changes in network load and security requirements.

4. Efficiency analysis of the model. To assess the efficiency of the model, we can introduce a cost function *C*, which takes into account the costs of encryption, energy consumption, and processing time:
$$C = \alpha \sum_{n=1}^{N_{max}} Cost(E, x_n) + \beta \sum_{g=1}^{G_{max}} Cost(F_g) + \gamma \sum_{s=1}^{S_{max}} Cost(H_s), \quad (4)$$
where $Cost$ reflects the costs of the encryption operation, and α, β, γ – are weighting coefficients reflecting the importance of each level in the overall system structure.
This model allows determining optimal encryption parameters for each level, balancing between security and costs, and adapting the system to changing operating conditions. Such an approach enhances the overall security of IoT systems while reducing costs and improving the user experience.

5. Cyber incidents and the role of encryption

Cyber Incidents in IoT can lead to unauthorized modifications of the entire system or its devices, resulting in significant losses, including leaks of confidential information, financial losses, and even physical damage to equipment. As the number of connected devices increases, cyber incidents become more frequent and destructive, forcing organizations to seek new ways to secure their systems.

Encryption plays a key role in protecting against such incidents. This is especially crucial in IoT, where devices are often located in unprotected environments and can easily become targets for attacks. Even if an IoT device is compromised, encryption helps keep sensitive data inaccessible to attackers.

Mathematical models help us better understand and quantitatively assess the risks associated with cyber incidents and the effectiveness of encryption as a preventive measure. Let's consider a model that evaluates the probability of a successful cyber incident in the presence of lightweight encryption.

Let $P(A)$ be the probability of an attack on the system, $P(E)$ – the probability of vulnerability exploitation, and $P(S|E)$ – the probability of applying successful encryption that prevents vulnerability exploitation. Then the probability of a successful cyber incident $P(B)$ can be expressed as:

$$P(B) = P(A) \times P(E) \times \big(1 - P(S|E)\big). \quad (5)$$

This formula indicates that the overall risk of a successful attack is a function of the probability of an attack, the probability of vulnerability exploitation, and the effectiveness of encryption. Implementing lightweight encryption on peripheral devices can significantly reduce $P(E)$, thereby reducing $P(B)$.

Lightweight encryption can have a significant impact on reducing the probability of $P(E)$ and, consequently $P(B)$. Considering the resource constraints of IoT devices, such encryption must be performance and energy-efficient. Algorithms such as SPECK, SIMON, Chaskey, and Ascon are examples of lightweight encryption optimized for use in IoT and can significantly reduce the risks of cyber incidents.

To further elaborate on the mathematical models mentioned above, these models can also be used to simulate various attack scenarios, providing insights into how different types of encryption affect the system's resilience. By using these simulations, organizations can better plan their defenses and allocate resources where they are most needed.

Another consideration is the balance between security and usability. While strong encryption is desirable for maximum security, it is also important to maintain a level of convenience for legitimate users. This is particularly relevant in user-facing IoT applications, where cumbersome security measures may deter usage or lead to insecure workarounds by end-users.

The integration of encryption into IoT systems should be done with an understanding of the lifecycle of both the devices and their data. Secure key management is critical, as compromised keys can render encryption moot. This includes the secure generation, storage, distribution, and eventual destruction of keys in accordance with industry best practices and regulatory requirements.

When a cyber incident does occur, proper encryption can significantly mitigate losses by restricting access to sensitive data. In post-incident analysis, encrypted data can aid in identifying and restoring only the compromised data, without the need for a complete system restoration.

Additionally, encryption policies should be included in the incident response plan to ensure that encryption keys are updated and managed properly, and encrypted data is restored from backups securely.

6. Discussion

In future research on lightweight cryptographic solutions for securing IoT, the development of adaptive cryptographic protocols holds great significance. Such protocols should be capable of dynamically adjusting their security parameters, taking into account the current needs and threats in the IoT environment. This will ensure the flexibility and efficiency of the security system, adapted to diverse device operating conditions.

Another crucial direction is studying the impact of quantum technology advancements on cryptography. The advent of quantum computing poses new challenges to the security of existing cryptographic systems. Therefore, it is pertinent to develop new quantum-resistant encryption methods that can safeguard data in the future.

The integration of artificial intelligence into cryptography also opens up new possibilities for enhancing IoT security. Utilizing artificial intelligence algorithms allows for the creation of more flexible and efficient systems that can predict and adapt to new types of cyberattacks.

Furthermore, improving authentication mechanisms for IoT devices remains a pertinent issue. Ensuring reliable authentication is key to protecting devices from unauthorized access and other forms of cyber threats. This requires continuous refinement and updating of authentication methods.

In conclusion, the analysis of real-world cyber incidents is a crucial aspect that will provide a deeper understanding of current and potential threats. This will facilitate the development of effective strategies for preventing and responding to cyber threats, contributing to the creation of a more secure IoT environment.

7. Conclusions

Research on the importance and application of lightweight encryption in the context of IoT is crucial for ensuring cybersecurity amid the rapid growth of IoT devices and the trend of escalating cyber threats. The primary contribution of this work lies in a detailed analysis of existing and innovative encryption methods tailored for the limited resources of IoT devices and an assessment of their impact on minimizing risks associated with cyber incidents.

Particular attention in this context is given to identifying and evaluating potential cyber threats to IoT devices, as well as developing strategies for their mitigation or minimization. The authors emphasize the critical importance of further refinement and implementation of these methods, which will enhance the overall security not only in terms of data protection but also in safeguarding IoT devices themselves against potential cyberattacks.

Additionally, the article underscores the integral importance of continuously updating and improving cryptographic methods in response to evolving cyber threats. This is essential for ensuring long-term security in IoT networks. The proposed strategies and approaches to encryption in the paper open new perspectives for organizations and developers in the IoT domain, allowing them to gain a deeper understanding of the possibilities and challenges associated with the use of lightweight encryption in contemporary conditions. Thus, this research not only contributes to the theoretical foundation in the field of IoT cybersecurity but also provides practical recommendations that can be applied to enhance the security of IoT networks in real-world scenarios.

Acknowledgments

This research was funded by the Ministry of Education and Science of Ukraine under grant 0123U100270.

Declaration on Generative AI

The author(s) have not employed any Generative AI tools.

References

[1] G. Ahmed, Improving IoT privacy, data protection and security concerns, International Journal of Technology, Innovation and Management (IJTIM) 1(1) (2021).

[2] S. Qi, Y. Lu, W. Wei, X. Chen, Efficient data access control with fine-grained data protection in cloud-assisted IioT, IEEE Internet of Things Journal 8(4) (2020) 2886–2899.

[3] W. Xue, C. Luo, Y. Shen, R. Rana, G. Lan, S. Jha, A. Seneviratne, W. Hu, Towards a compressive-sensing-based lightweight encryption scheme for the Internet of Things, IEEE Transactions on Mobile Computing 20(10) (2020) 3049–3065.

[4] C. Patel, N. Doshi, Security challenges in IoT cyber world, in: Security in smart cities: models, applications, and challenges, 2019, pp. 171–191, doi:10.1007/978-3-030-01560-2_8

[5] V. Dutta, M. Choras, M. Pawlicki, R. Kozik, Detection of cyberattacks traces in IoT data, J. Univers. Comput. Sci. 26(11) (2020) 1422–1434.
[6] I. Stellios, P. Kotzanikolaou, M. Psarakis, C. Alcaraz, J. Lopez, A survey of iot-enabled cyberattacks: Assessing attack paths to critical infrastructures and services, IEEE Communications Surveys & Tutorials 20(4) (2018) 3453–3495.
[7] The tipping point: Exploring the surge in IoT cyberattacks globally, 2023. URL: https://blog.checkpoint.com/security/the-tipping-point-exploring-the-surge-in-iot-cyberattacks-plaguing-the-education-sector/.
[8] S. K. Mousavi, A. Ghaffari, S. Besharat, H. Afshari, Security of internet of things based on cryptographic algorithms: a survey, Wireless Networks 27 (2021) 1515–1555.
[9] P. R. Kumar, A. T. Wan, W. S. H. Suhaili, Exploring data security and privacy issues in internet of things based on five-layer architecture, International journal of communication networks and information security 12(1) (2020) 108–121.
[10] Z. Dar, A. Ahmad, F. A. Khan, F. Zeshan, R. Iqbal, H. H. R. Sherazi, A. K. Bashir, A context-aware encryption protocol suite for edge computing-based IoT devices, The Journal of Supercomputing 76 (2020) 2548–2567.
[11] Z. Mohammad, T. A. Qattam, K. Saleh, Security weaknesses and attacks on the Internet of Things applications, in: Proceedings of 2019 IEEE Jordan International Joint Conference on Electrical Engineering and Information Technology (JEEIT), IEEE, Amman, Jordan, 2019, pp. 431–436. doi: 10.1109/JEEIT.2019.8717411.
[12] F. Meneghello, M. Calore, D. Zucchetto, M. Polese, A. Zanella, IoT: Internet of threats? A survey of practical security vulnerabilities in real IoT devices, IEEE Internet of Things Journal 6(5) (2019) 8182–8201.
[13] K. Dineva, T. Atanasova, Security in IoT systems, Int. Multidiscip. Sci. GeoConference Surv. Geol. Min. Ecol. Manag. SGEM 19(2.1) (2019) 569–577.
[14] S. Srivastava, S. Prakash, An analysis of various IoT security techniques: a review, in: Proceedings of 8th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO), IEEE, Noida, India, 2020, pp. 355–362. doi: 10.1109/ICRITO48877.2020.9198027.
[15] M. Qasaimeh, R. S. Al-Qassas, F. Mohammad, S. Aljawarneh, A novel simplified aes algorithm for lightweight real-time applications: Testing and discussion, Recent Advances in Computer Science and Communications (Formerly: Recent Patents on Computer Science) 13(3) (2020) 435–445.
[16] A. Hamza, B. Kumar, A review paper on DES, AES, RSA encryption standards, in: Proceedings of 2020 9th International Conference System Modeling and Advancement in Research Trends (SMART), IEEE, Moradabad, India, 2020, pp. 333–338. doi: 10.1109/SMART50582.2020.9336800.
[17] N. A. Gunathilake, W. J. Buchanan, R. Asif, Next generation lightweight cryptography for smart IoT devices: implementation, challenges and applications, in: Proceedings of 2019 IEEE 5th World Forum on Internet of Things (WF-IoT), IEEE, Limerick, Ireland, 2019, pp. 707–710, doi: 10.1109/WF-IoT.2019.8767250.
[18] M. Azrour, J. Mabrouki, A. Guezzaz, A. Kanwal, Internet of things security: challenges and key issues, Security and Communication Networks (2021) 1–11.
[19] M. N. Khan, A. Rao, S. Camtepe, Lightweight cryptographic protocols for IoT-constrained devices: A survey, IEEE Internet of Things Journal 8(6) (2020) 4132–4156.
[20] M. Rana, Q. Mamun, R. Islam, Lightweight cryptography in IoT networks: A survey, Future Generation Computer Systems 129 (2022) 77–89.
[21] V. A. Thakor, M. A. Razzaque, M. R. Khandaker, Lightweight cryptography algorithms for resource-constrained IoT devices: A review, comparison and research opportunities, IEEE Access 9 (2021) 28177–28193.
[22] N. A. Gunathilake, A. Al-Dubai, W. J. Buchana, Recent advances and trends in lightweight cryptography for IoT security, in: Proceedings of 2020 16th International Conference on

Network and Service Management (CNSM), IEEE, Izmir, Turkey, 2020, pp. 1–5. doi: 10.23919/CNSM50824.2020.9269083.

[23] M. A. Latif, M. B. Ahmad, M. K. Khan, A review on key management and lightweight cryptography for IoT, in: Proceedings of 2020 Global Conference on Wireless and Optical Technologies (GCWOT), IEEE, Malaga, Spain, 2020, pp. 1–7. doi: 10.1109/GCWOT49901.2020.9391613.

[24] L. M. Shamala, G. Zayaraz, K. Vivekanandan, V. Vijayalakshmi, Lightweight cryptography algorithms for Internet of Things enabled networks: an overview, in: Journal of Physics: Conference Series, volume 1717, no. 1, IOP Publishing, 2021, p. 012072. doi:10.1088/1742-6596/1717/1/012072.

[25] B. B. Gupta, M. Quamara, An overview of Internet of Things (IoT): Architectural aspects, challenges, and protocols, Concurrency and Computation: Practice and Experience 32(21) (2020) e4946. doi: 10.1002/cpe.4946.

[26] A. A. Abba Ari, A. C. Djedouboum, A. M. Gueroui, O. Thiare, A. Mohamadou, Z. Aliouat, A three-tier architecture of large-scale wireless sensor networks for big data collection, Applied Sciences 10(15) (2020) 5382. doi: 10.3390/app10155382.

[27] J. Jose, D. V. Jose, The Internet of Things architectures and use cases, in: Enterprise digital transformation, Auerbach Publications, 2022, pp. 101–125.

[28] H. Sabireen, V. J. I. E. Neelanarayanan, A review on fog computing: Architecture, fog with IoT, algorithms and research challenges, Ict Express 7(2) (2021) 162–176. doi: 10.1016/j.icte.2021.05.004.

[29] P. Habibi, M. Farhoudi, S. Kazemian, S. Khorsandi, A. Leon-Garcia, Fog computing: a comprehensive architectural survey, IEEE access, 8 (2020) 69105–69133. doi: 10.1109/ACCESS.2020.2983253.

[30] S. Kunal, A. Saha, R. Amin, An overview of cloud-fog computing: Architectures, applications with security challenges, Security and Privacy 2(4) (2019) e72. doi: 10.1002/spy2.72.