Electronic Journal of Education, Social Economics and Technology
Vol. 6, No. 2, (2025), pp. 1~7, Article ID: 1161
ISSN 2723-6250 (online)
DOI: https://doi.org/10.33122/ejeset.v6i2.1161

SAINTIS publishing

Research Article

Lightweight Cryptography for IoT in Wireless Sensor Networks: Evaluating Speck, Simon, and Ascon Using NS-3

Bayu Widodo[1*], Mohammad Fazrie[2] , Dudi Parulian[2]

[1] Computer Engineering Technology Study Program, Vocational School, IPB University, Bogor, Indonesia, 16128

[2] Faculty of Computer Science Engineering, Universitas Indraprasta PGRI, Jakarta, Indonesia, 12530

*Corresponding Author: paruliandudi@gmail.com | Phone: +6282110878811

ABSTRACT

Communication security in Wireless Sensor Networks (WSNs) is a significant challenge in the implementation of the Internet of Things (IoT), particularly in smart city applications which have limitations in energy, memory, and computation. Conventional cryptographic algorithms are generally not suitable for IoT devices due to their complexity and high resource requirements, necessitating lightweight cryptography (LWC) algorithms that can balance security and efficiency. This research evaluates three lightweight encryption algorithms - Speck, Simon, and Ascon - using NS-3 simulations in a multi-hop network scenario with 30 nodes. The parameters analyzed include energy consumption, encryption/decryption time, and communication overhead. The simulation results show a significant trade-off: Speck and Simon excel in energy efficiency and low latency, but their security level is moderate; while Ascon provides stronger security according to NIST LWC standards, but with the consequence of higher energy consumption. The main contribution of this research is the provision of a reproducible NS-3 simulation-based framework that can link security and energy efficiency aspects, while also filling the literature gap, which is still limited to hardware testing. This finding is expected to serve as a practical reference for IoT system designers in determining the appropriate encryption algorithm for smart city application needs, and to open up opportunities for further research on real IoT devices.

Keywords: Internet of Things; Wireless Sensor Network; lightweight cryptography; Speck; Simon; Ascon; NS-3; smart city

1. INTRODUCTION

The Internet of Things (IoT) has become a major pillar in the development of smart cities due to its ability to integrate various public services, intelligent transportation, and environmental monitoring systems in real-time (Hoang, 2024 ; Belli et al., 2020). In its implementation, IoT heavily relies on Wireless Sensor Networks (WSNs), which function to collect and transmit data from sensors to a processing center (Gulati et al., 2021; Nourildean et al., 2022; Jamshed et al., 2022). Nevertheless, the resource limitations of WSN devices such as energy, memory, and computing capacity pose serious challenges to ensuring the operational sustainability of WSNs. These challenges become even more complex when communication security aspects must also be met to prevent data leakage and manipulation (Rozlomii et al., 2024 ; Lata et al., 2021; Ouni & Saleem, 2022).

Data security in WSNs is a critical issue given the potential attacks that can occur, such as eavesdropping, data injection, manipulation, and replay attacks (Li, 2010 ; Padmavathi & Shanmugapriya, 2009). Conventional cryptographic algorithms are considered capable of providing protection, but their high computational and energy requirements make them less suitable for IoT devices with limited resources (Thakor et al., 2021 ; Singh et al., 2024). Therefore, a solution is needed in the form of lightweight cryptography (LWC) algorithms designed to strike a balance between security and energy efficiency on IoT devices.

Speck and Simon, two block ciphers developed for lightweight needs, offer high efficiency with low overhead (Beaulieu et al., 2014; Beaulieu et al., 2015). Meanwhile, Ascon, which was selected as the standard by NIST for lightweight cryptography, provides a more robust authenticated encryption mechanism against various modern attack models (Sonmez et al., 2024; Kaur et al., 2023). Several previous studies have evaluated the performance of this algorithm thru both hardware and software experiments. However, network simulation-based studies, particularly using Network Simulator 3 (NS-3), are still rare (Campanile et al., 2020). In fact, network simulation allows for more realistic performance measurement by comprehensively considering communication conditions, energy consumption, and network reliability (Wu et al., 2011 ; Campanile et al., 2020 ; Adday et al., 2024).

This research aims to fill this gap by conducting a comparative analysis of Speck, Simon, and Ascon within the context of IoT-based WSNs using the NS-3 simulation approach. The evaluation focuses on energy efficiency, latency, and communication reliability to identify the trade-offs between security and network performance. The main novelty of this research lies in the combination of lightweight cryptography analysis with the NS-3 network simulation approach, which has not been widely explored in the literature. The research results are expected to provide practical guidance for developers and researchers in selecting the most suitable cryptographic algorithm for WSN-based smart city applications, while also enriching academic studies on the relationship between security and efficiency aspects in IoT. Thus, this research not only expands understanding of the performance of lightweight cryptographic algorithms but also contributes to the development of practical and efficient security solutions for the future smart city ecosystem

2. LITERATURE REVIEW

Beaulieu et al. (2015) introduced Speck and Simon as lightweight block ciphers designed with a focus on implementation efficiency, both in software and hardware (Beaulieu et al., 2015; Beaulieu et al., 2014). This algorithm is designed for resource-constrained devices, making it widely adopted in research related to IoT. On the other hand, Dobraunig et al. (2021) developed Ascon as an authenticated encryption algorithm that offers a higher level of security while maintaining efficiency, and it has since been established as a standard in the NIST Lightweight Cryptography Standard (Sonmez et al., 2024; Turan et al., 2021; Dobraunig et al., 2021).

Comprehensive studies on lightweight cryptography have been conducted by (Iqbal et al., 2025 and Rana et al., 2022) emphasizing the importance of the trade-off between security level, energy consumption, and communication performance in IoT applications. Research by Radhakrishnan et al. (2024) provides an empirical analysis of the efficiency of Speck, Simon, and Ascon on IoT devices, considering energy consumption and latency (Radhakrishnan et al., 2024). Furthermore, El-Hajj et al. (2023) complemented the study by benchmarking the algorithms on real hardware to directly measure performance (El-hajj et al., 2023). Although these studies have made significant contributions, the majority still focus on hardware testing or theoretical analysis without considering the complex network dynamics. In fact, in the implementation of WSN in IoT, multi-hop communication, transmission reliability, and energy efficiency at the network level are important factors that affect overall system performance (Altowaijri, 2022; Bakhsh, 2017; Anastasi et al., 2010).

To date, research examining the performance of lightweight cryptography thru a network simulation approach, particularly using Network Simulator 3 (NS-3), is still very limited. NS-3 offers advantages in representing real network conditions, such as multi-hop topology, node energy constraints, and IoT communication patterns (Ramonet et al., 2024; Kodali & Kirti, 2020; Campanile et al., 2020). Therefore, this research contributes by presenting a comparative evaluation of Speck, Simon, and Ascon based on NS-3 simulation, which links security aspects with energy efficiency in the context of WSN for smart cities. This literature review confirms the existence of a research gap that is still limitedly explored, particularly regarding the use of network simulations in assessing the trade-offs in lightweight cryptography algorithms. This study is expected to enrich academic perspectives while providing a practical foundation for selecting optimal encryption algorithms to support the sustainability of IoT and smart city implementation.

3. RESEARCH METHOD

The methodology for this research is designed to evaluate the performance of the lightweight cryptographic algorithms Speck, Simon, and Ascon within the context of an IoT-based wireless sensor network using a simulation approach. The methodological stages include the design of the simulation environment, algorithm implementation, and performance evaluation based on measurable parameters.

3.1 Simulation Environment

The experiments in this study were conducted using Network Simulator 3 (NS-3) version 3.40. The simulation environment was designed to closely resemble real-world conditions for WSN implementation in IoT applications. The main focus of the simulation is to evaluate the performance of multi-hop communication with energy constraints, which is one of the key characteristics of wireless sensor networks. The simulation parameters used can be seen in **Table 1**.

Table 1. Simulation Environment

Parameters	Value/ Specification
Nettwork topology:	Multi-hop with 30 IoT nodes communicating toward a single sink node.
Communication protocol	IEEE 802.15.4 (MAC/PHY) with IPv6 support at the network layer.
Energy node	Each node is equipped with a 1000 mAh battery.
Simulation duration	Each node is equipped with a 1000 mAh battery.
Interval pengiriman data	Data transmission interval
Ukuran payload	Payload size

The selection of this configuration is intended to represent a WSN scenario in smart city implementation, where each node operates with limited resources but is still required to maintain communication reliability. To provide a visual representation of the simulation scenario, **Figure 1** shows the network topology used in this study. Node sensors are depicted as randomly distributed, with one node acting as the sink node, which is the central data collection point. The relationship between nodes is built based on distance proximity, which describes the pattern.

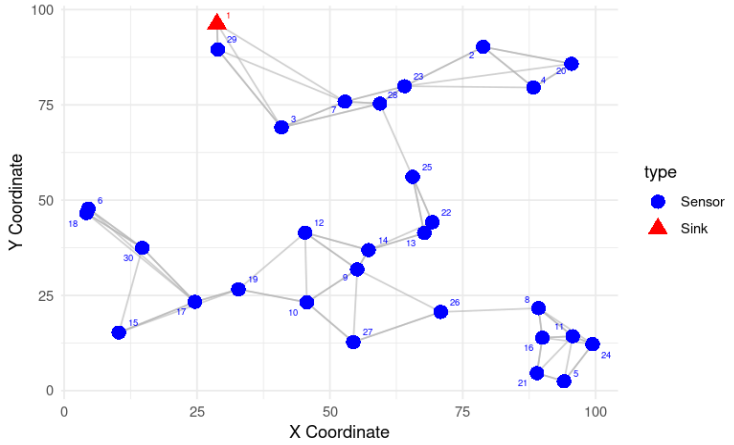

Figure 1. Wireless Sensor Network Topology

3.2 Algorithm Implementation

Three lightweight cryptographic algorithms, namely Speck, Simon, and Ascon, were implemented at the NS-3 application layer. The encryption mechanism is performed on the sender side before the data is transmitted, while decryption is done on the receiver side to verify data integrity. The algorithm implementation refers to the official source code from the developers, which was then modified to be compatible with NS-3. This approach ensures that the evaluation is conducted under controlled and uniform conditions across all scenarios.

3.3 Evaluation Parameters

The evaluation was conducted using three main parameters that represent the trade-off between security and energy efficiency, namely: 1. Energy consumption (mJ) the total battery energy used by all nodes during the simulation. 2. Encryption/decryption time (ms) the average time required to process each data packet. 3. Communication overhead (%) – the percentage increase in packet size due to the encryption process, which affects network capacity.

3.4 Data Analysis

The simulation results were analyzed quantitatively by comparing the performance of the three algorithms on the predetermined parameters. The analysis was conducted using a comparative approach to identify the strengths and weaknesses of each algorithm. Next, the measurement results are used to evaluate the trade-offs between security, energy efficiency, and communication performance in IoT networks. With this methodology, the research is expected to provide valid results, measurable replication, and direct relevance to the development of secure and efficient IoT systems in the context of smart cities.

4. RESULTS AND DISCUSSION

4.1 Simulation Results

The simulation results are presented in **Table 2**, which compares the performance of three lightweight cryptographic algorithms: Ascon, Speck, and Simon, based on encryption time, energy consumption, packet overhead, and security level.

Table 2. Comparison of Algorithm Performance

Security Algorithm	Encryption Time (ms)	Energy Consumption (mJ)	Overhead Package (%)	Security Level
Algorithm: Ascon	Low (3.5 ms)	High (1160 mJ total / 38.7 mJ/node)	Medium (~20%)	High
Algorithm: Speck	Low (1 ms)	Low (290 mJ total / 9.67 mJ/node)	Low (~6.25% From payload)	Medium
Algorithm: Simon	Low–Medium (1.2 ms)	Low (348 mJ total / 11.6 mJ/node)	Low (~6.25%)	Medium

To facilitate visualization of this comparison, **Figure 1** shows a bar chart illustrating the values of each parameter for the three algorithms. With this image, the performance differences between the algorithms can be seen at a glance, making it easier for readers to understand the quantitative information presented in **Table 1**.

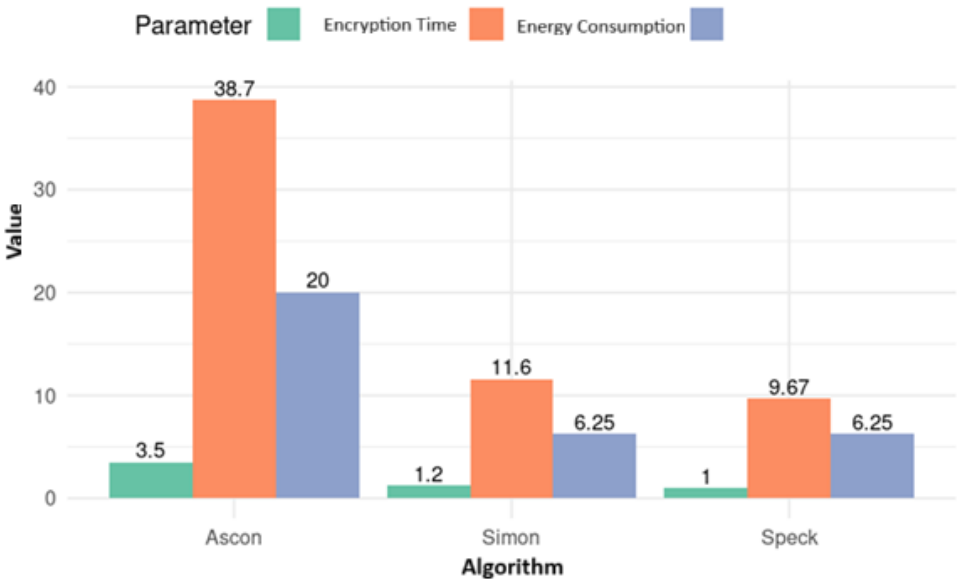

Figure 2. Comparison of Lightweight Cryptography Algorithm Performance

Regarding encryption time parameters, Ascon required the highest time at 3.5 ms, followed by Simon at 1.2 ms, and Speck, which had the lowest encryption time at 1 ms. In terms of energy consumption, Ascon also recorded the highest value with a total of 1160 mJ or an average of 38.7 mJ per node, while Speck and Simon had lower energy consumption, at 290 mJ (9.67 mJ per node) and 348 mJ (11.6 mJ per node), respectively. For the packet overhead parameter, Ascon shows a value of around 20%, while Speck and Simon both have low overhead of about 6.25% of the payload size. Regarding security level, Ascon has the highest security level, while Speck and Simon show a medium security level. Overall, **Table 2** presents a comprehensive performance comparison of the three algorithms within the context of a WSN system, providing quantitative information regarding the performance of each algorithm on the tested parameters.

4.2 Trade-off Analysis

The simulation results show a significant difference in the performance of the three lightweight cryptographic algorithms tested, namely Speck, Simon, and Ascon. In terms of computational performance and energy efficiency, Speck and Simon showed relatively better results compared to Ascon. The average encryption time for Speck was 1 ms with an energy consumption of 9.67 mJ per node, while Simon was slightly higher with an encryption time of 1.2 ms and an energy consumption of 11.6 mJ per node. Both also generate low communication overhead, around 6.25% of the payload size, so they don't significantly impact the transmission channel capacity. This indicates that Speck and Simon are more suitable for application in sensor networks with limited energy and long-term data transmission requirements. However, from a security perspective, Speck and Simon are still considered to be at a moderate level. Several cryptanalysis studies have shown that both algorithms have weaknesses in some variants, posing a risk if used in high-security applications. Therefore, although efficient in terms of energy and communication, the Speck and Simon implementation is more suitable for non-critical WSN applications, such as environmental monitoring, smart agriculture, or simple monitoring systems that do not contain sensitive data.

Unlike Speck and Simon, Ascon exhibits performance characteristics that are more resource-intensive. With an encryption time of 3.5 ms and energy consumption of 38.7 mJ per node, this algorithm has the highest energy requirements in this simulation. The communication overhead generated is also higher, around 20% of the payload. Nevertheless, the high consumption of these resources is in line with the level of security offered. As an Authenticated Encryption with Associated Data (AEAD) algorithm, Ascon not only provides data confidentiality but also guaranties message integrity and authentication. This advantage led to Ascon being selected as the winner in the 2023 NIST Lightweight Cryptography competition, solidifying its position as an algorithm with a high level of security.

Based on these results, it can be concluded that there is a clear trade-off between energy efficiency and security level in selecting lightweight cryptographic algorithms for WSNs. Speck and Simon are superior in terms of energy efficiency and low overhead, but their security level is limited. Conversely, Ascon provides strong security guaranties at the cost of

increased energy consumption and overhead. Therefore, the choice of algorithm should be tailored to the application's needs: Speck and Simon are more suitable for energy-saving applications, while Ascon is more appropriate for critical applications requiring high data security even at a greater energy cost.

4.3 Comparison with Previous Studies

The findings of this study are consistent with the results of Radhakrishnan et al. (2024), who reported that Ascon excels in terms of security but is more energy-intensive than Speck and Simon. The study by El-Hajj et al. (2023) also supports these results thru hardware benchmarking, although limited to the single-node level (El-hajj et al., 2023). The main difference in this research lies in the use of NS-3 simulation, which allows for analysis in the context of multi-hop communication on WSN networks. Thus, this research not only evaluates the performance of the algorithm from the encryption perspective on a single node, but also considers the impact of encryption on network energy efficiency, transmission reliability, and communication overhead. This result strengthens the argument that network simulation can be an important approach for evaluating lightweight cryptography in the context of IoT and smart cities, and provides a practical basis for developers to tailor algorithm choices to application needs.

4.4 Practical Implications

This research has several practical implications:

1. Adaptive algorithm selection: The simulation results show that there is no single optimal algorithm for all applications. Therefore, IoT system developers can choose algorithms based on their needs: Speck or Simon for energy-efficient applications, and Ascon for applications with high security priorities.
2. IoT security policy design basis: Local governments or smart city service providers can use these results as a reference in formulating data security policies tailored to application characteristics.
3. Smart city infrastructure efficiency: By considering the trade-off between security and energy consumption, the results of this research can help reduce long-term operational costs, particularly for applications with a large number of nodes.
4. Hybrid system development: This research opens up opportunities for implementing hybrid encryption systems, where different algorithms can be used selectively based on data type or service sensitivity, thus achieving a balance between security and energy efficiency.

Thus, the practical implications of this research are not only academic but also relevant in supporting the development of safe, efficient, and sustainable smart cities.

5. CONCLUSION

This study evaluates the performance of three lightweight cryptography algorithms—Speck, Simon, and Ascon—on a wireless sensor network (WSN) based on NS-3 simulation. Simulation results show a significant trade-off between energy efficiency and security level. Generally, Speck and Simon excel in energy efficiency and encryption speed, making them highly suitable for non-critical IoT applications that prioritize long battery life, such as environmental monitoring and smart agriculture. Meanwhile, Ascon provides a higher level of security, befitting its status as a NIST LWC standard, but requires greater energy consumption. This makes Ascon more suitable for critical IoT applications, such as smart health monitoring or intelligent transportation, which require high data security guaranties. The main contribution of this research is to provide a simulation-based comparative analysis using NS-3 in the context of multi-hop WSN communication, which has been rarely done in the literature until now. Thus, this research expands the perspective of lightweight cryptography studies, which previously focused more on hardware studies or single-node testing. For future research, it is recommended to implement the system on real IoT devices (e.g., ESP32, STM32) and test it on more complex network topologies. This is necessary to validate the simulation results and ensure their relevance to real-world scenarios. Practically, the results of this research can serve as a reference for IoT system designers and smart city policymakers in determining lightweight cryptographic algorithms that are suitable for specific application needs, both in terms of energy efficiency and data security.

REFERENCES

Adday, Hassan, G., Subramaniam, S. K., Zukarnain, Z. A., & Samian, N. (2024). Investigating and analyzing simulation tools of wireless sensor networks: A comprehensive survey. IEEE Access, 12, 22938–22977.

Altowaijri, S. M. (2022). Efficient Next-Hop Selection in Multi-Hop Routing for IoT Enabled Wireless Sensor Networks. Future Internet, 14(2), 1–16. https://doi.org/10.3390/fi14020035

Anastasi, G., Conti, M., Francesco, D. M., & Neri, V. (2010). Reliability and energy efficiency in multi-hop IEEE 802.15.4/ZigBee Wireless Sensor Networks. Proceedings - IEEE Symposium on Computers and Communications, 336–341. https://doi.org/10.1109/ISCC.2010.5546804

Bakhsh, S. T. (2017). Energy-efficient distributed relay selection in wireless sensor network for Internet of Things. In 2017

13th International Wireless Communications and Mobile Computing Conference, IWCMC, 1802–1807. https://doi.org/10.1109/IWCMC.2017.7986557

Beaulieu, R., Shors, D., Smith, J., Treatman-Clark, S., Weeks, B., & Wingers, L. (2014). The simon and speck block ciphers on avr 8-bit microcontrollers. In International Workshop on Lightweight Cryptography for Security and Privacy, 8898, 3–20. https://doi.org/10.1007/978-3-319-16363-5_1

Beaulieu, R., Shors, D., Smith, J., Treatman-Clark, S., Weeks, B., & Wingers, L. (2015). Simon and Speck: Block Ciphers for the Internet of Things. Cryptology EPrint Archive, 1–15.

Belli, L., Cilfone, A., Davoli, L., Ferrari, G., Adorni, P., Di Nocera, F., Dall'olio, A., Pellegrini, C., Mordacci, M., & Bertolotti, E. (2020). IoT-enabled smart sustainable cities: Challenges and approaches. Smart Cities, 3(3), 1039–1071. https://doi.org/10.3390/smartcities3030052

Campanile, L., Gribaudo, M., Iacono, M., Marulli, F., & Mastroianni, M. (2020). Computer network simulation with ns-3: A systematic literature review. Electronics, 9(2), 1–25. https://doi.org/10.3390/electronics9020272

Dobraunig, C., Eichlseder, M., Mendel, F., & Schläffer, M. (2021). Ascon v1.2: Lightweight Authenticated Encryption and Hashing. Journal of Cryptology, 34(3), 1–42. https://doi.org/10.1007/s00145-021-09398-9

El-hajj, M., Mousawi, H., & Fadlallah, A. (2023). Analysis of Lightweight Cryptographic Algorithms on IoT Hardware Platform. Future Internet, 15(2), 1–29. https://doi.org/10.3390/fi15020054

Gulati, K., Boddu, R. S. K., Kapila, D., Bangare, S. L., Chandnani, N., & Saravanan, G. (2021). A review paper on wireless sensor network techniques in Internet of Things (IoT). Materials Today: Proceedings, 51, 161–165. https://doi.org/10.1016/j.matpr.2021.05.067

Hoang, T. Van. (2024). Impact of Artificial Intelligence and Internet of Things Technologies on Smart Cities and Urban Planning. JOURNAL OF TECHNICAL EDUCATION SCIENCE, 19(1), 64–73. https://doi.org/10.1049/icp.2025.0851

Iqbal, R., Ansari, N. M., Awan, M. ur R., Ismail, M., & Gul, H. (2025). Design and Evaluation of Lightweight Cryptographic Algorithms for Internet of Things (IoT) Devices: Achieving Optimal Trade-Offs Between Security, Computational Speed, and Energy Efficiency in Resource-Constrained Environments. THE PROGRESS: A Journal of Multidisciplinary Studies, 6(1), 85–99. https://doi.org/10.71016/tp/smfybz24

Jamshed, M. A., Ali, K., Abbasi, Q. H., Imran, M. A., & Ur-Rehman, M. (2022). Challenges, Applications, and Future of Wireless Sensors in Internet of Things: A Review. IEEE Sensors Journal, 22(6), 5482–5494. https://doi.org/10.1109/JSEN.2022.3148128

Kaur, J., Canto, A. C., Kermani, M. M., & Azarderakhsh, R. (2023). A Comprehensive Survey on the Implementations, Attacks, and Countermeasures of the Current NIST Lightweight Cryptography Standard. ACM Comput, 1–16. http://arxiv.org/abs/2304.06222

Kodali, R. K., & Kirti, B. (2020). NS-3 Model of an IoT network. In 2020 IEEE 5th International Conference on Computing Communication and Automation, ICCCA, 699–702. https://doi.org/10.1109/ICCCA49541.2020.9250808

Lata, S., Mehfuz, S., & Urooj, S. (2021). Secure and Reliable WSN for Internet of Things: Challenges and Enabling Technologies. IEEE Access, 9, 161103–161128. https://doi.org/10.1109/ACCESS.2021.3131367

Li, C. T. (2010). Security of Wireless Sensor Networks: Current Status and Key Issues. Smart Wireless Sensor Networks.

Nourildean, S. W., Hassib, M. D., & Mohammed, Y. A. (2022). Internet of things based wireless sensor network: a review. Indonesian Journal of Electrical Engineering and Computer Science, 27(1), 246–261. https://doi.org/10.11591/ijeecs.v27.i1.pp246-261

Ouni, R., & Saleem, K. (2022). Framework for Sustainable Wireless Sensor Network Based Environmental Monitoring. Sustainability, 14(14), 1–26. https://doi.org/10.3390/su14148356

Padmavathi, D. G., & Shanmugapriya, M. D. (2009). A Survey of Attacks, Security Mechanisms and Challenges in Wireless Sensor Networks. (IJCSIS) International Journal of Computer Science and Information Security, 4(1), 1–9. http://arxiv.org/abs/0909.0576

Radhakrishnan, I., Jadon, S., & Honnavalli, P. B. (2024). Efficiency and Security Evaluation of Lightweight Cryptographic Algorithms for Resource-Constrained IoT Devices. Sensors, 24(12), 1–19. https://doi.org/10.3390/s24124008

Ramonet, A. G., Pecorella, T., Picano, B., & Kinoshita, K. (2024). Perspectives on IoT-oriented network simulation systems. Computer Networks, 253, 1–9. https://doi.org/10.1016/j.comnet.2024.110749

Rana, M., Mamun, Q., & Islam, R. (2022). Lightweight cryptography in IoT networks: A survey. Future Generation Computer Systems, 129, 77–89. https://doi.org/10.1016/j.future.2021.11.011

Rozlomii, I., Yarmilko, A., & Naumenko, S. (2024). Data security of IoT devices with limited resources: challenges and potential solutions. Doors, 3666, 85–96.

Singh, S., Sharma, P. K., Moon, S. Y., & Park, J. H. (2024). Advanced lightweight encryption algorithms for IoT devices: survey, challenges and solutions. Journal of Ambient Intelligence and Humanized Computing, 15(2), 1625–1642. https://doi.org/10.1007/s12652-017-0494-4

Sonmez, T., Meltem, McKay, K., Chang, D., Kang, J., & Kelsey, J. (2024). Ascon-based lightweight cryptography standards for constrained devices: authenticated encryption, hash, and extendable output functions. (No. NIST Special Publication (SP), 800-232 (Draft)).

Thakor, V. A., Razzaque, M. A., & Khandaker, M. R. A. (2021). Lightweight Cryptography Algorithms for Resource-Constrained IoT Devices: A Review, Comparison and Research Opportunities. IEEE Access, 9, 28177–28193. https://doi.org/10.1109/ACCESS.2021.3052867

Turan, M. S., McKay, K., Chang, D., Calik, C., Bassham, L., Kang, J., & Kelsey, J. (2021). Status Report on the First Round of the NIST Lightweight Cryptography Standardization Process. In National Institute of Standards and Technology (pp. 1–92).

Wu, H., Nabar, S., & Poovendran, R. (2011). An energy framework for the network simulator 3 (ns-3). In Proceedings of the 4th International ICST Conference on Simulation Tools and Techniques, 3, 222–230. https://doi.org/10.4108/icst.simutools.2011.245584