International Journal On Engineering Technology and Sciences – IJETS
ISSN (P):2349-3968, ISSN (O): 2349-3976 Volume XIII - Issue I, January - 2026

Survey of Data Privacy Enhancement in Internet of Things security using lightweight cryptography

[1]Evangeline Selva Kumari K, [2]S. Mary Evanchalin, [3]R. Mallika Pandeeswari, [4]Dr. R. Ravi,
[1]Principal, Jeya Polytechnic College, Thoothukudi. [2]Research scholar, Department of Computer Science and Engineering, Francis Xavier Engineering College, Tirunelveli, India.
Email: maryevanchalinphd@gmail.com, [3]Research Scholar, Department of ECE, Francis Xavier Engineering College, Tirunelveli, Tamil Nadu, India. Email: mallikapandeeswari@francisxavier.ac.in, [4]Professor, Department of Computer Science and Engineering, Francis Xavier Engineering College, Tirunelveli, India.
Email: fxhodcse@gmail.com

Abstract

Data privacy become the serious topic in the today's digital industry for maintaining the data integrity. Several cryptography algorithms are already existing, but often causes high computation time and required more resources. Considering this the light weight cryptosystem was analyzed better in this domain. The present study has drawn the survey about light weight crypto system for the internet of Things (IoT) data security. finally, the performance was tested with different light weight models. In that, the asymmetric model recorded the finest security strength score with high memory usage then other models. In addition, low latency, memory usage is recorded for the SPECK model, but it has recorded the average security strength compared to the asymmetric model.

Keywords: light weight cryptography, data privacy, Internet of Things, digital industry

1. Introduction

The IoT is a network of gadgets that are inter including people, things, objects, mechanical machinery, and digital gadgets [1]. These gadgets are uniquely identified. and are able to transfer data across the internet without the need for human-to-human or human-to-computer cooperation [2]. Kevin Ashton initially used the term "Internet of Things" in 1982. His goal was to make it possible for people to interact with the digital or fictional world [3]. In addition, the IoT can be any electronic device that has the capacity to send data across a connection and to which we may allocate an IP address. These gadgets are equipped with sensors that allow them to detect their surroundings and gather data, which is then transmitted over the internet [4]. The IoT makes it possible to recognize and regulate "things" from a distance. Nowadays, all are gradually moving into an online setting due to the extremely rapid advancement of online technology [5]. In this online environment, individuals can do everything, including work, communicate, and shop. The IoT is a novel, developing field that will significantly alter people's daily lives [6]. Big Data is mostly produced by the IoT idea, which connects anything to the internet. Big Data represents the newest topic of attention and a growing discipline [7]. The number of IoT devices is growing daily, as is the amount of data they produce [8]. IoT devices generate data that is structured, unstructured, as well as [9]. Clouds, mobile phones, social media, and online communities are the primary providers of massive amounts of data. volume, speed, and diversity are the three V's that make up the Big Data paradigm.

2. Light weight cryptography

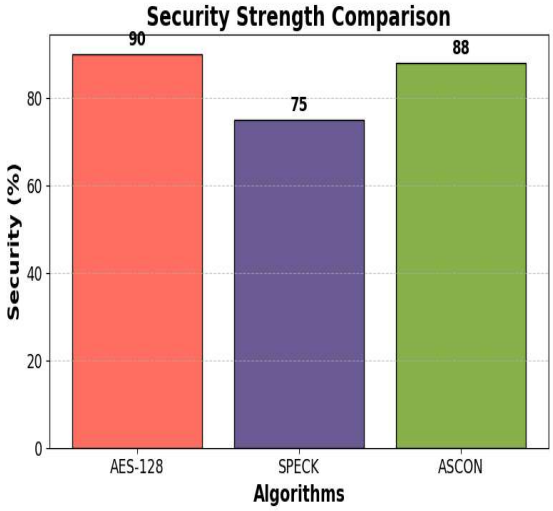
The IoT has enabled the linking of several devices capable of gathering enormous amounts of data thanks to the development of contemporary technology. IoT safety features are so crucial [11].

Network management, data integrity, secrecy, and authentication are all protected by cryptography. However, conventional protocols for cryptography are not any more appropriate for all IoT scenarios, including smart cities, because of the numerous limitations of connected devices. In order to secure information about IoT devices, academics have been putting out a number of lightweight cryptographic techniques and protocols. In addition to discussing cutting-edge lightweight secure protocols for IoT systems, this study offers a comparison of well-known modern ciphers.

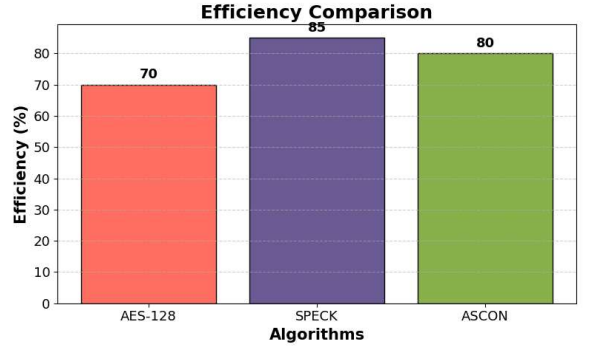
Most Tiny Encryption Algorithm (TEA) [12] has become one of the fastest and most efficient lightweight algorithms for encoding for Internet of Things implementations. With the goal to conceal statistical components of simple text, TEA uses a few fragments of code that are based on the Feistel architecture to give cryptographic fundamental dispersion and dispersion features. It is susceptible to attacks utilizing comparable and equivalent keyboard attacks, though. This study introduced a new producing keys function that uses two Linear Reset Shift Registrations to change TEA.

The Internet of Things has grown to be a crucial component of the state of the art on which all rely. Security problems have also arisen as the variety of IoT gadgets has increased. Simple encryption has developed into a viable way to enhance the confidentiality and privacy of Internet of Things devices. Selecting the best algorithm from a wide range of options is the difficult part. Three distinct LWC algorithms—AES-128, SPECK, and ASCON—are compared in this work [13]. A number of metrics, including execution time, memory usage, latency, efficiency, and security resilience of the methods on IoT boards with limited computational power and capabilities, are measured in order to compare them. In order to choose the best cryptographic algorithms and achieve a balance amongst security and effectiveness, these measures are essential for determining suitability. According to the assessment, SPECK performs higher in IoT gadgets with limited resources.

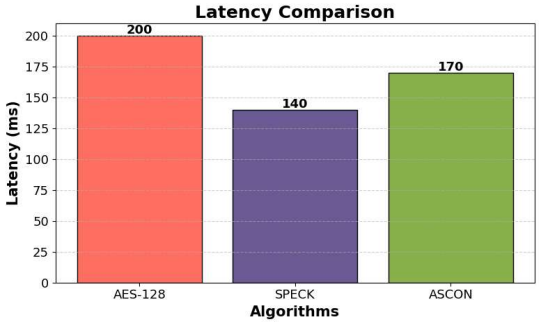
IoT gadgets, which allow everything to interact and share information in scenarios like Industry 4.0, intelligent cities, intelligent homes, and medical imaging, are becoming more and more in necessity. IoT gadgets, such as those found in residences, workplaces, healthcare facilities, wearable technology, and agriculture, are essential to daily lives. Securing communications between devices has become increasingly important as IoT devices have developed, and must guarantee the confidentiality and safety of data between these devices [14]. When integrating IoT devices to the internet, user authentication has become a significant security risk. To guarantee that only verified users are able to depend on their choices, numerous authentication systems, such as mutual identification and group verification, have been developed. Both symmetric and asymmetric key-based approaches have been put forth, but creating lightweight, reliable, provably secure authentication techniques is difficult since IoT gadgets have limited resources. This study presents a lightweight IoT verification methodology and examines the different authentication methods intended for lightweight IoT gadgets. The performance analysis is exposed in Fig.1.



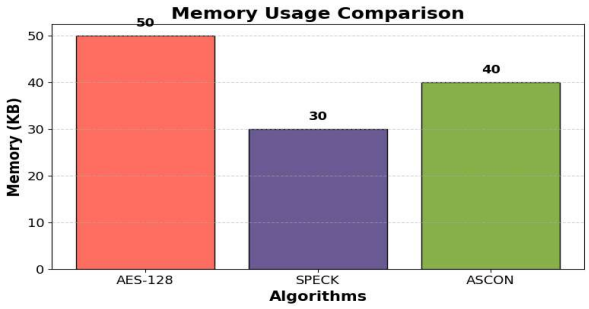
(a)



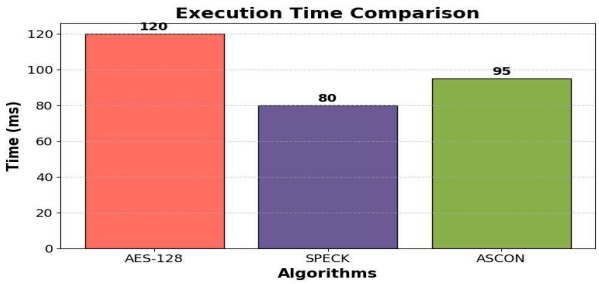
(b)



(c)



(d)



(e)

Fig. 1: performance analysis: a) Security, b) Efficiency, c) latency, d) Memory and e) Execution time

3. Conclusion

The present survey discusses about the few cryptography model for securing the digital information from the third parties. The performance indicator considered for this study is time, security, efficiency, latency, memory, and security strength. Finally, the comparison is made the three strong models that are AES-128, SPECK and ASCON, each models were best in specific metrics. The asymmetric model recorded the outstanding data privacy score as 90%, even though it has reported high execution time and resource usage. Hence, each model is well suitable for the specific performance improvement. Including any optimization constraints along with those models will give better outcomes further.

References

1. Yasmin, N., & Gupta, R. (2023). Modified lightweight cryptography scheme and its applications in IoT environment. *International Journal of Information Technology*, *15*(8), 4403-4414.https://doi.org/10.1007/s41870-023-01486-2

2. Suryateja, P. S., & Rao, K. V. (2024). A survey on lightweight cryptographic algorithms in IoT. *Cybernetics and Information Technologies*, *24*(1), 21-34.

3. Ahmed, A. A., Malebary, S. J., Ali, W., & Alzahrani, A. A. (2023). A provable secure cybersecurity mechanism based on combination of lightweight cryptography and authentication for Internet of Things. *Mathematics*, *11*(1), 220. https://doi.org/10.3390/math11010220

4. Chaturvedi, S. P., Yadav, A., Kumar, A., & Mukherjee, R. (2023, December). Unlocking IoT security: Enabling the future with lightweight cryptographic ciphers. In *International Conference on Intelligent Computing Techniques For Smart Energy Systems* (pp. 189-199). Singapore: Springer Nature Singapore.https://doi.org/10.1007/978-981-97-8429-5_15

5. 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

6. Goulart, A., Chennamaneni, A., Torre, D., Hur, B., & Al-Aboosi, F. Y. (2022). On wide-area IoT networks, lightweight security and their applications—a practical review. *Electronics*, *11*(11), 1762. https://doi.org/10.3390/electronics11111762

7. Nujumudeen, F., Mubarak, M. N., Sharma, Y. K., Lilhore, U. K., Aldossary, S. M. A., Hussien, S. A., ... & Khan, M. (2026). A hybrid chaos-based cryptographic framework for lightweight IoT security: enhancing efficiency and security in low-power devices. *Peer-to-Peer Networking and Applications*, *19*(2), 53.https://doi.org/10.1007/s12083-025-02188-1

8. Haider, Z. A., Zeb, A., Islam, A. M., Rahman, T., Arishi, A., & Ullah, I. (2026). Enhancing IoT security with resource-efficient cryptography: A comprehensive review of lightweight and hybrid algorithms. *Computer Science Review*, *59*, 100861.https://doi.org/10.1016/j.cosrev.2025.100861

9. Haider, Z. A., Zeb, A., Islam, A. M., Rahman, T., Arishi, A., & Ullah, I. (2026). Enhancing IoT security with resource-efficient cryptography: A comprehensive review of lightweight and hybrid algorithms. *Computer Science Review*, *59*, 100861.https://doi.org/10.1016/j.cosrev.2025.100861

10. Maheswari, B., Ambika, S., Dayana Peter, T. P., & Siva Subramanian, R. (2026). Development of Lightweight Image Encryption Algorithm for Ensuring Confidentiality and Privacy in Internet of Things Devices. *International Journal of Communication Systems*, *39*(4), e70389. https://doi.org/10.1002/dac.70389

11. 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

12. Mhaibes, H. I., Abood, M. H., &Farhan, A. K. (2022). Simple Lightweight Cryptographic Algorithm to Secure Imbedded IoT Devices. *international journal of interactive mobile technologies*, *16*(20).https://doi.org/10.3991/ijim.v16i20.34505

13. Radhakrishnan, I., Jadon, S., &Honnavalli, P. B. (2024). Efficiency and security evaluation of lightweight cryptographic algorithms for resource-constrained IoT devices. *Sensors*, *24*(12), 4008.https://doi.org/10.3390/s24124008

14. Goyal, T. K., Sahula, V., & Kumawat, D. (2022). Energy efficient lightweight cryptography algorithms for IoT devices. *IETE Journal of Research*, *68*(3), 1722-1735. https://doi.org/10.1080/03772063.2019.1670103