Frontiers in Health Informatics ISSN-Online:2676-7104
www.healthinformaticsjournal.com
2024; Vol 13: Issue 3
Open Access

A Survey On Hybrid Lightweight Security Mechanisms For Cloud-IoT Healthcare Applications

J.Praveen kumar[1], M.Suresh Babu[2]
[1]Research Scholars in Department of Computer Science Bhartiar University Coimbatore.
[1]praveentkrecit@gmail.com
[2]Professor in Department of CSE, Teegala Krishna Reddy Engineering College Hyderabad
[2]surescse@tkrec.ac.in

Cite this paper as: J.Praveen kumar, M.Suresh Babu (2024) A Survey On Hybrid Lightweight Security Mechanisms For Cloud-IOT Healthcare Applications. *Frontiers in Health Informatics, 13* (3), 9053-9060

Abstract
The rapid expansion of the Internet of Things (IoT) and cloud computing has created a robust infrastructure for real-time data transmission, storage, and processing across domains like healthcare, smart cities, and industrial automation. However, this integration introduces significant security challenges, especially given the resource constraints of IoT devices. Traditional cryptographic methods struggle to balance robust security with the performance requirements of large-scale, real-time IoT-cloud environments. This paper surveys recent advancements in lightweight cryptographic frameworks aimed at addressing these challenges, focusing on hybrid cryptographic techniques that enhance data security while maintaining computational efficiency. It identifies key research gaps in scalability, real-time performance, and decentralized key management. The paper also explores the potential of chaotic encryption systems and Elliptic Curve Cryptography (ECC), proposing future research directions such as automated parameter optimization, quantum-resistant encryption, and lightweight multi-factor authentication for IoT-cloud systems. These advancements will be crucial in ensuring secure and efficient data handling in resource-constrained IoT environments.

1. INTRODUCTION

The exponential growth of the Internet of Things (IoT) and cloud computing technologies has enabled real-time data transmission, storage, and processing across various domains, including healthcare, smart cities, and industrial automation. The combination of IoT and cloud paradigms provides a robust infrastructure for monitoring, decision-making, and automation. However, this integration introduces significant security challenges. Data security, especially for sensitive and real-time information, is crucial to prevent unauthorized access, data breaches, and cyberattacks.

IoT devices are typically resource-constrained, with limited processing power, memory, and energy. These constraints pose unique challenges for implementing encryption and authentication protocols. Traditional cryptographic methods often fail to balance strong security with lightweight performance, resulting in inefficiencies in large-scale and real-time IoT-cloud environments.

Research Questions:

1. What are the primary data security threats in cloud-IoT environments?
2. How can hybrid cryptographic methods enhance data security while maintaining computational efficiency in IoT networks?
3. What future improvements are necessary to address the emerging challenges in cloud-IoT data security?

This paper surveys recent literature, identifies critical gaps in cloud-IoT security frameworks, and explores hybrid encryption techniques to achieve both robust security and efficiency.

II . LITERATURE OVERVIEW

2.1 Lightweight Revocable Hierarchical Attribute-Based Encryption (LW-RHABE)

Authors: Mohammad Ali, Mohammad-Reza Sadeghi, Ximeng Liu

Advantages: LW-RHABE offers a **scalable, cloud-based key delegation and revocation mechanism** specifically designed for IoT devices with limited computational resources. This method reduces the computational burden on IoT devices by offloading key management tasks to a cloud-based server

Limitations: The primary limitation of LW-RHABE is its **reliance on centralized key management**. The presence of a **centralized authority (CA)** introduces potential vulnerabilities, particularly in decentralized environments where a single point of failure or collusion among authorities could lead to a complete security breach. Future work needs to explore **decentralized key management** methods to mitigate this risk

2.2 LiSP-XK: Extended Lightweight Signcryption Protocol

Authors: Tai-Hoon Kim, Gulshan Kumar, William J. Buchanan, et al.

Advantages: The LiSP-XK protocol provides a lightweight encryption and signcryption mechanism using Elliptic Curve Cryptography (ECC), which is particularly suited for IoT environments with limited energy resources. By combining ECC with **Keccak hash functions**, LiSP-XK ensures high security with low energy consumption

Limitations: While effective in small-scale IoT networks (tested on 20 nodes), the scalability of the protocol in larger IoT ecosystems remains **untested**. Additionally, **key management and revocation** were not extensively covered, a critical aspect for secure and dynamic IoT environments

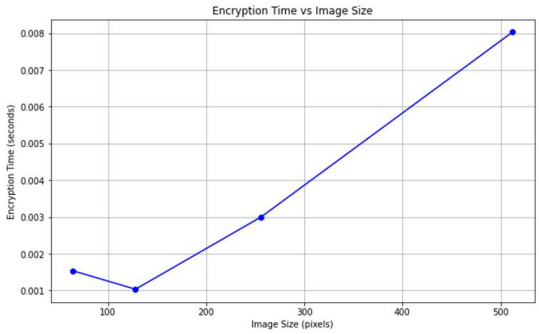
2.3 Cost-Efficient Image Encryption Using Parallel Chaotic Systems (IEPSBP)

Authors: Zhaoquan Gu, Hao Li, Sajid Khan, et al.

Advantages: **IEPSBP** focuses on secure image encryption for low-power IoT devices using **parallel chaotic systems**. This method demonstrates **energy-efficient encryption**, which is crucial for IoT devices with limited battery life.

Significant Increase for Larger Images: As the image size grows (likely from medium to larger resolutions), the encryption time increases more dramatically. This suggests that the IEPSBP algorithm has scalability limitations when applied to larger images, leading to greater computational burden.

Limitation: The plot highlights that **as** image size increases the encryption time raises significantly, indicating a potential performance bottleneck in real-time or large-scale applications, especially in environments requiring rapid encryption for larger datasets or images



2.4 Efficient Identity-Based Encryption with Revocation

Authors: Yinxia Sun, Pushpita Chatterjee, Yi Chen, Yudong Zhang

Advantages: This method integrates **efficient user revocation** and **lightweight encryption mechanisms**, ensuring secure communication between IoT devices in small networks. The use of **identity-based encryption (IBE)** simplifies key distribution and enhances security.

Limitations: The system struggles with **scalability**, particularly in large IoT networks. As the number of connected devices grows, key revocation and distribution processes can become **bottlenecks**, affecting system performance and security. The time-based key revocation may also be problematic in environments requiring **instantaneous revocation**.

2.5 Proxy Reciphering as a Service (PRaaS)

Authors: Shruthi Ramesh, Manimaran Govindarasu

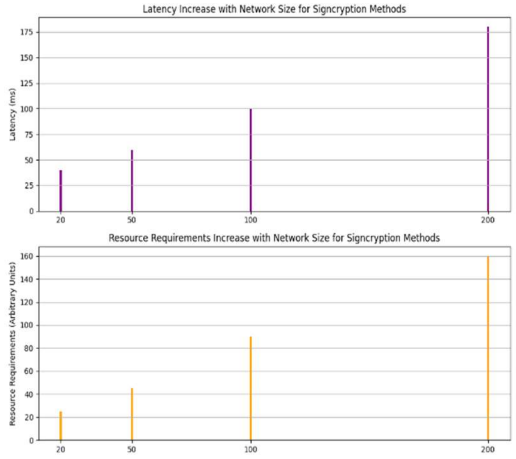
Advantages: PRaaS ensures **privacy-preserving computations** on encrypted data using **fully homomorphic encryption (FHE)**, allowing secure computations without decryption. This method is especially suitable for **resource-constrained IoT devices**.

Limitations: The method introduces significant **latency**, particularly in real-time IoT applications such as **ECG monitoring**. The high computational complexity of FHE also poses challenges for resource-limited devices, making it impractical for **real-time data processing**.

III. METHODOLOGIES AND APPROACHES

The methodologies used in the reviewed studies focus on lightweight cryptography, chaotic systems, and identity-based encryption. Key techniques include:

- **Simulation-based Testing**: Many of the studies used simulation environments to test encryption performance on small-scale IoT networks, with metrics such as encryption time, energy consumption, and memory usage. For example, the **LiSP-XK protocol** was tested using 20 nodes to demonstrate its energy efficiency



Observation:
As the network size increases, the latency significantly increases. For example, with 20 nodes, the latency is around 40 ms, while with 200 nodes, it reaches nearly 180 ms.This indicates that as the network grows, the delay in processing signcryption requests also grows, which poses a scalability issue

- **Key Management**: Several studies, including LW-RHABE, emphasized the importance of **key delegation and revocation** mechanisms. However, centralized approaches introduce vulnerabilities, and future work should explore decentralized methods like **blockchain-based key distribution**

- **Chaotic Map Systems**: Chaotic systems such as the **Henon map** and **3D logistic map** are used to generate pseudo-random sequences, enhancing encryption strength. However, parameter selection for these chaotic maps remains a manual, time-consuming process

IV. FINDINGS AND TRENDS

The key findings from the literature include:

- **Lightweight Encryption**: The use of ECC and chaotic systems has proven effective in reducing computational overhead while maintaining security. These methods show promise for IoT applications where energy efficiency is critical
- **Scalability Challenges**: Most encryption protocols are tested in small-scale networks, but their performance in large-scale IoT environments, such as smart cities or industrial IoT, remains largely untested
- **Key Management Vulnerabilities**: Centralized key management approaches introduce vulnerabilities in decentralized environments. There is a growing need for **decentralized key management solutions**, potentially leveraging blockchain technology

V. CHALLENGES AND GAPS

The following challenges and gaps were identified in the literature:

- **Scalability Issues**: Encryption methods that work well in small networks often face **scalability limitations** when applied to large IoT networks. Testing on large-scale deployments is necessary to determine real-world performance
- **Manual Parameter Selection**: Chaotic encryption systems require manual parameter selection, which is both time-consuming and inefficient. **Soft computing-based approaches** should be developed to automate the parameter optimization process.
- **High Latency in Real-Time Applications**: Methods like FHE introduce high computational latency, making them unsuitable for real-time IoT applications. Further research is needed to **optimize performance** for time-sensitive use cases

VI . FUTURE RESEARCH DIRECTIONS

1. Enhanced Lightweight Data Encryption for Cloud-IoT Paradigms: Future research should focus on developing more robust lightweight encryption frameworks for cloud-IoT networks. These frameworks must address the limitations of existing encryption methods by improving both security strength and computational efficiency. A focus on reducing the computational and energy overhead in resource-constrained IoT environments will ensure that data security is maintained without compromising device performance.

2. Hybrid Encryption Method for Scalability and Efficiency: There is a need to create a hybrid encryption method that combines multiple cryptographic techniques, such as Elliptic Curve Cryptography (ECC) with chaotic systems, to provide scalable and efficient security solutions. Future work should explore combining existing cryptographic techniques to form a method that balances lightweight processing with strong encryption. This hybrid approach should be capable of handling dynamic, large-scale cloud-IoT networks while ensuring secure real-time data communication

3. Lightweight Multi-factor Authentication for IoT-Cloud Healthcare Applications: As IoT is heavily used in healthcare applications, future research should aim to develop a lightweight multi-factor authentication (MFA) system that provides robust security while maintaining efficiency in resource-constrained environments. This MFA system should integrate biometric verification or token-based systems to improve security and protect against vulnerabilities such as replay attacks and man-in-the-middle attacks.

4. Scalability and Real-World Testing: Research should emphasize the scalability of proposed encryption methods. Testing should be conducted in real-world cloud-IoT environments, such as smart cities or healthcare systems, to ensure that these solutions can handle large-scale deployments and high volumes of real-time data transmission. This will ensure the practical applicability of encryption systems in ubiquitous environments

VII . CONCLUSION

This paper surveyed recent advancements in lightweight encryption methods for securing cloud-IoT environments. While techniques like ECC and chaotic systems have proven effective, significant challenges remain in terms of scalability, key management, and real-time performance. Future research should focus on addressing these limitations by exploring decentralized key management, quantum-resistant encryption, and soft computing-based optimization. With further development, hybrid encryption systems can enhance data security in cloud-IoT networks, ensuring efficiency and robustness in resource-constrained environments.

REFRENCES

1) M. Ali, M.-R. Sadeghi, and X. Liu, "Lightweight Revocable Hierarchical Attribute-Based Encryption for Internet of Things,"
2) T.-H. Kim, G. Kumar, R. Saha, W. J. Buchanan, T. Devgun, and R. Thomas, "LiSP-XK: Extended Light-Weight Signcryption for IoT in Resource-Constrained Environments,"
3) Z. Gu, H. Li, S. Khan, L. Deng, X. Du, M. Guizani, and Z. Tian, "IEPSBP: Cost-Efficient Image Encryption Using Parallel Chaotic Systems for Green IoT,".
4) Y. Sun, P. Chatterjee, Y. Chen, and Y. Zhang, "Efficient Identity-Based Encryption with Revocation for Data Privacy in IoT,"
5) S. Ramesh and M. Govindarasu, "An Efficient Framework for Privacy-Preserving Computations on Encrypted IoT Data," Accessed: Sep. 2024. [Online]. Available:
6) G. Kuldeep and Q. Zhang, "Lightweight Joint Compression and Encryption for Resource-Constrained IoT Devices,".
7) N. Gupta, A. Jati, and A. Chattopadhyay, "MemEnc: A Lightweight Low-Power and Transparent Memory Encryption Engine for IoT,".
8) R. Durga, et al., "CES Blocks—A Novel Chaotic Encryption Schemes-Based Blockchain System for IoT,"
9) U. Hijawi, D. Unal, R. Hamila, A. Gastli, and O. Ellabban, "Lightweight KPABE Architecture in Mesh Networked IoT Devices," Accessed: Sep. 2024. [Online].
10) 1. Song, T.; Li, R.; Mei, B.; Yu, J.; Xing, X.; Cheng, X. A privacy preserving communication protocol for IoT applications in smart homes. IEEE Internet Things J. 2017, 4, 1844–1852.
11) 2. Moosavi, S.R.; Gia, T.N.; Nigussie, E.; Rahmani, A.M.; Virtanen, S.; Tenhunen, H.; Isoaho, J. End-to-end security scheme for mobility enabled healthcare Internet of Things. Future Gener. Comput. Syst. 2016, 64, 108–124.
12) 3. Lee, I.; Lee, K. The Internet of Things (IoT): Applications, investments, and challenges for enterprises. Bus. Horizons 2015, 58, 431–440.
13) 4. Ion, M.; Zhang, J.; Schooler, E.M. Toward content-centric privacy in ICN: Attribute-based encryption and routing. In Proceedings of the 3rd ACM SIGCOMM workshop on Information-Centric Networking, Hong Kong, China, 12 August 2013; pp. 39–40.
14) 5. Rahman, Z.; Yi, X.; Khalil, I.; Sumi, M. Chaos and Logistic Map Based Key Generation Technique for AES-Driven IoT Security. In Proceedings of the International Conference on Heterogeneous Networking for Quality, Reliability, Security and Robustness, Online, 29–30 November 2021; pp. 177–193
15) 6. Rahaman, Z.; Corraya, A.D.; Sumi, M.A.; Bahar, A.N. A novel structure of advance encryption standard with 3-dimensional dynamic S-Box and key generation matrix. arXiv 2020, arXiv:2005.00157. 7. Ziv, J.;

Lempel, A. A universal algorithm for sequential data compression. IEEE Trans. Inf. Theory 1977, 23, 337–343.
16) 8. Vashi, S.; Ram, J.; Modi, J.; Verma, S.; Prakash, C. Internet of Things (IoT): A vision, architectural elements, and security issues. In Proceedings of the 2017 international conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud), Tamil Nadu, India, 10–11 February 2017; pp. 492–496.
17) 9. Farooq, U.; Aslam, M.F. Comparative analysis of different AES implementation techniques for efficient resource usage and better performance of an FPGA. J. King Saud Univ. Comput. Inf. Sci. 2017, 29, 295–302.
18) 10. Kocarev, L. Chaos-based cryptography: A brief overview. IEEE Circuits Syst. Mag. 2001, 1, 6–21.
19) 11. Mukhopadhyay, S.C.; Suryadevara, N.K. Internet of things: Challenges and opportunities. In Internet of Things; Springer: Berlin/Heidelberg, Germany, 2014; pp. 1–17.
20) 12. Tausif, M.; Ferzund, J.; Jabbar, S.; Shahzadi, R. Towards designing efficient lightweight ciphers for internet of things. KSII Trans. Internet Inf. Syst. 2017, 11, 4006–4024.
21) 13. Usman, M.; Ahmed, I.; Aslam, M.I.; Khan, S.; Shah, U.A. SIT: A lightweight encryption algorithm for secure internet of things. arXiv 2017, arXiv:1704.08688.
22) 14. Kumar, M.; Kumar, S.; Budhiraja, R.; Das, M.; Singh, S. Lightweight data security model for IoTapplications: A dynamic key approach. In Proceedings of the 2016 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), 2016; pp. 424–428.
23) 15. Patil, J.; Bansod, G.; Kant, K.S. LiCi: A new ultra-lightweight block cipher. In Proceedings of the 2017 International Conference on Emerging Trends & Innovation in ICT (ICEI), Pune, India, 3–5 February 2017; pp. 40–45.
24) 16. Bapat, C.; Baleri, G.; Inamdar, S.; Nimkar, A.V. Smart-lock security re-engineered using cryptography and steganography. In International Symposium on Security in Computing and Communication; Springer: Berlin, Germany, 2017; pp. 325–336.
25) 17. Indrayani, R.; Nugroho, H.A.; Hidayat, R.; Pratama, I. Increasing the security of mp3 steganography using AES Encryption and MD5 hash function. In Proceedings of the 2016 2nd International Conference on Science and Technology-Computer (ICST), Yogyakarta, Indonesia, 27–28 October 2016; pp. 129–132.
26) 18. Aljawarneh, S.; Yassein, M.B.; Talafha, W.A. A resource-efficient encryption algorithm for multimedia big data. Multimed. Tools Appl. 2017, 76, 22703–22724
27) 19.Schneier, B. Applied Cryptography: Protocols, Algorithms, and Source Code in C; John Wiley & Sons: Hoboken, NJ, USA, 2007.
28) 20. Lian, S.; Sun, J.; Wang, Z. A block cipher based on a suitable use of the chaotic standard map. Chaos Solitons Fractals 2005, 26, 117–129.
29) 21. Rahulamathavan, Y.; Phan, R.C.W.; Rajarajan, M.; Misra, S.; Kondoz, A. Privacy-preserving blockchain based IoT ecosystem using attribute-based encryption. In Proceedings of the 2017 IEEE International Conference on Advanced Networks and Telecommunications Systems (ANTS), Bhubaneswar, India, 17–20 December 2017; pp. 1–6
30) .22. Yang, J.; He, S.; Lin, Y.; Lv, Z. Multimedia cloud transmission and storage system based on internet of things. Multimed. Tools Appl. 2017, 76, 17735–17750.
31) 23. Rahman, A.; Islam, M.J.; Rahman, Z.; Reza, M.M.; Anwar, A.; Mahmud, M.A.P.; Nasir, M.K.; Noor, R.M. DistBCondo: Distributed Blockchain-Based IoT-SDN Model for Smart Condominium. IEEE Access 2020, 8, 209594–209609. doi:10.1109/ACCESS.2020.3039113.

32) 24. Rahman, A.; Nasir, M.K.; Rahman, Z.; Mosavi, A.; S., S.; Minaei-Bidgoli, B. DistBlockBuilding: A Distributed Blockchain-Based SDN-IoT Network for Smart Building Management. IEEE Access 2020, 8, 140008–140018. doi:10.1109/ACCESS.2020.3012435. 25. Rahman, Z.; Khalil, I.; Yi, X.; Atiquzzaman, M. Blockchain-Based Security Framework for a Critical Industry 4.0 Cyber-Physical System. IEEE Commun. Mag. 2021, 59, 128–134. doi:10.1109/MCOM.001.2000679.
33) 26.M. Ali, M. -R. Sadeghi and X. Liu, "Lightweight Revocable Hierarchical Attribute-Based Encryption for Internet of Things," in IEEE Access, vol. 8, pp. 23951-23964, 2020, doi: 10.1109/ACCESS.2020.2969957.
34) 27.T. -H. Kim, G. Kumar, R. Saha, W. J. Buchanan, T. Devgun and R. Thomas, "LiSP-XK: Extended Light-Weight Signcryption for IoT in Resource-Constrained Environments," in IEEE Access, vol. 9, pp. 100972-100980, 2021, doi: 10.1109/ACCESS.2021.3097267.
35) 28.Z. Gu et al., "IEPSBP: A Cost-Efficient Image Encryption Algorithm Based on Parallel Chaotic System for Green IoT," in IEEE Transactions on Green Communications and Networking, vol. 6, no. 1, pp. 89-106, March 2022, doi: 10.1109/TGCN.2021.3095707.
36) 29.Y. Sun, P. Chatterjee, Y. Chen and Y. Zhang, "Efficient Identity-Based Encryption With Revocation for Data Privacy in Internet of Things," in IEEE Internet of Things Journal, vol. 9, no. 4, pp. 2734-2743, 15 Feb.15, 2022, doi: 10.1109/JIOT.2021.3109655.
37) 30.S. Ramesh and M. Govindarasu, "An Efficient Framework for Privacy-Preserving Computations on Encrypted IoT Data," in IEEE Internet of Things Journal, vol. 7, no. 9, pp. 8700-8708, Sept. 2020, doi: 10.1109/JIOT.2020.2998109.
38) 31.Y. M. Al-Moliki, M. T. Alresheedi, Y. Al-Harthi and A. H. Alqahtani, "Robust Lightweight-Channel-Independent OFDM-Based Encryption Method for VLC-IoT Networks," in IEEE Internet of Things Journal, vol. 9, no. 6, pp. 4661-4676, 15 March15, 2022, doi: 10.1109/JIOT.2021.3107395.
39) 32.G. Kuldeep and Q. Zhang, "Design Prototype and Security Analysis of a Lightweight Joint Compression and Encryption Scheme for Resource-Constrained IoT Devices," in IEEE Internet of Things Journal, vol. 9, no. 1, pp. 165-181, 1 Jan.1, 2022, doi: 10.1109/JIOT.2021.3098859.
40) 33.N. Gupta, A. Jati and A. Chattopadhyay, "MemEnc: A Lightweight, Low-Power, and Transparent Memory Encryption Engine for IoT," in IEEE Internet of Things Journal, vol. 8, no. 9, pp. 7182-7191, 1 May1, 2021, doi: 10.1109/JIOT.2020.3040846.
41) 34.R. Durga, E. Poovammal, K. Ramana, R. H. Jhaveri, S. Singh and B. Yoon, "CES Blocks—A Novel Chaotic Encryption Schemes-Based Blockchain System for an IoT Environment," in IEEE Access, vol. 10, pp. 11354-11371, 2022, doi: 10.1109/ACCESS.2022.3144681.
42) 35.U. Hijawi, D. Unal, R. Hamila, A. Gastli and O. Ellabban, "Lightweight KPABE Architecture Enabled in Mesh Networked Resource-Constrained IoT Devices," in IEEE Access, vol. 9, pp. 5640-5650, 2021, doi: 10.1109/ACCESS.2020.3048192.
43) 36. R. Beaulieu, S. T.Clark, S. Douglas, S. Weeks, B. Smith, and J. Wingers, "TheSIMON and speck families of lightweight block ciphers," in 52nd ACM/EDAC/IEEE Design Automation Conference (DAC), San Francisco, 2013, pp. 1–6.
44) 37. S. Habeeb and R. F. Hassan, "Sensors data encryption using TSFS Algorithm," Journal of MadentAlelem College, Vol. 10, No. 1, 2018.
45) 38. J. R. Naif, GH A. Majeed, and A. K. Farhan, "Secure IoT System Based on Chaos- Modified Lightweight AES," International Conference on Advanced Science and Engineering (ICOASE), 2019
46) 39. A. H. Saeed Al-Wattar, "A Review of Block Ciphers S-Boxes Tests Criteria," Iraqi Journal of Statistical Science, pp.1-14, 2019.

47) 40. Beaulieu, R.; Shors, D.; Smith, J.; Treatman-Clark, S.; Weeks, B.; Wingers, L. The SIMON and SPECK lightweight block ciphers. In Proceedings of the 52nd Annual Design Automation Conference, San Francisco, CA, USA, 7–10 June 2015; pp. 1–6.
48) 41. S, A., G, U. S-DAC: A Novel Dynamic Substitution boxes using hybrid chaotic system and Deoxyribonuceic Acid(DNA) coding for counterfeiting Side-Channel Attacks. *Pers UbiquitComput* (2021). https://doi.org/10.1007/s00779-021-01579-4
49) 42. Ziaur Rahman , Xun Yi , Mustain Billah , Mousumi Sumi and Adnan Anwar," Enhancing AES Using Chaos and Logistic Map-Based Key Generation Technique for Securing IoT-Based Smart Home", Mdpi/Electronics 0. https://doi.org/10.3390/electronics1010000