JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

SECURING THE IOT: A COMPARATIVE ANALYSIS OF ENCRYPTION TECHNIQUES

[1] **Nabeel Mohammed Salih Atiyah** [1st] **Ali Amhmed AB Altalibe** [2nd]
[1] *Assistant lecturer, Department of Computer* [1st] *Lecturer, Department of Computer* [2nd]
[1] *Faculty of Education, Sabratha University, Zaltan, Libya .*
[2] *High Institute of Medical &Technologies- Aljomil, Aljomil, Libya.*

Abstract: The Internet of Things (IoT) is a big step forward in our connected world. It has the power to change things like smart homes and how factories work. Nevertheless, the occurrence of data breaches and illegal access presents significant risks, which are exacerbated by the growing adoption of the IoT. Encryption plays a vital role in ensuring the security of the Internet of Things (IoT) since it effectively safeguards against unauthorized entities gaining access to sensitive data and maintains the integrity of connections. The objective of this study is to assist practitioners in selecting the most robust encryption techniques that are appropriate for IoT applications (Li et al., 2021). In the course of our analysis, we assign priority to the assessment of effectiveness, cost-effectiveness, and usability while evaluating different encryption methods. In order to accomplish this, we have devised a rigorous process that incorporates practical IoT scenarios, experimental configurations, and data acquisition technologies. In the subsequent sections, we present the outcomes of our experimental investigations, providing a thorough assessment of the merits and drawbacks associated with each encryption methodology in terms of data encryption speed, resource consumption, and user-friendliness.

IndexTerms **– Internet of Things, IoT, Encryption, Encryption Keys, Network Security, Configurations, Cryptographic, Decryption, IoT Ecosystem, Data Protection, Optimization, Elliptic Curve Cryptography, RSA encryption, Security framework**

I. INTRODUCTION

The emergence of the IoT has led to a significant advancement in connection, resulting in a profound impact on several aspects of our daily lives and professional endeavors. The proliferation of IoT devices has become pervasive in nearly all aspects of modern life, encompassing many domains such as smart homes that facilitate the automation of routine activities and industrial systems that optimize production workflows. Nevertheless, the increased interconnectedness gives rise to a significant concern, namely security. Stringent security measures are necessary to prevent unauthorized individuals from getting access to or compromising the vast amounts of data exchanged across IoT devices. Encryption plays a crucial role in IoT security by safeguarding data privacy and integrity. Encryption is vital inside the protection of complex statistics as it navigates IoT networks, preventing unlawful access and interference. The growth of IoT programs in equipment and devices brings a new task in encryption. Practitioners have a big challenge in balancing the security and practicality of the systems. In this context, our research addresses the essential query of identifying the maximum appropriate encryption approach for enhancing IoT safety. We apprehend that the effectiveness of encryption extends beyond its cryptographic power; it must additionally keep in mind efficiency, price-effectiveness, and usability. The actual-global applicability of encryption methods is a complex interplay of these elements.

Scope and Objectives: Our research thoroughly investigates numerous encryption techniques, their realistic implications in IoT protection, and the change-offs related to each.

Through this research, we purpose to:

- Evaluate the performance of various encryption techniques concerning facts encryption and decryption speed(s) in IoT environments.
- Assess the price-effectiveness of implementing those strategies in numerous IoT scenarios, accounting for hardware and operational prices.
- Examine the usability and person-friendliness of encryption strategies to gauge their practicality for quit-customers and IoT builders.

In order to assist decision-makers in the selection of encryption solutions that align with their specific IoT security needs, our study specifically outlines these objectives. Ensuring the safety and security of our globally networked society is assuming greater significance due to the rapid expansion of the IoT.

II. LITERATURE REVIEW

IoT Security Challenges

The fast proliferation of Internet of Things (IoT) devices has caused the appearance of several safety problems. Due to communique that entails the transmission of records thru the Internet, the structures are exposed to a lot of dangers. Consequently,

this surge in connectivity has introduced a distinct set of security challenges (Roman et al., 2013). This literature review examines the primary security challenges encountered by the IoT ecosystem, aiming to provide a comprehensive understanding of the complexities involved in safeguarding this quickly expanding domain.

Heterogeneity

According to Atlam et al. (2018), the diverse range of IoT devices poses a significant challenge in terms of ensuring security inside the IoT ecosystem. IoT encompasses a wide range of devices, each with distinct attributes and approaches for establishing connectivity with external networks. From small-scale sensors to sophisticated intelligent appliances, each possessing distinct characteristics that necessitate customized safety protocols (Atlam et al., 2018). Safeguarding this multifaceted environment necessitates the development of adaptable security protocols capable of accommodating the needs of a vast array of IoT devices.

Scalability

Alaba et al. (2017) reported that the increasing popularity and extensive utilization of the IoT have led to the deployment of numerous devices across several sectors, including healthcare, transportation, and agriculture (Alaba et al., 2017. Nevertheless, the rapid proliferation of IoT devices has surpassed the capacity of security solutions to expand accordingly. The administration and security of large-scale IoT deployments provide significant challenges due to the need for robust security measures and efficient strategies for monitoring, patching, and updating devices in response to emerging threats.

Data Privacy

According to Roman et al. (2013), IoT devices that are driven by data gather and transmit a wide range of information, including data that is of a sensitive nature. This category encompasses various types of information, including medical records, home security logs, and data derived from manufacturing processes. Hence, safeguarding personal information holds paramount significance in ensuring the security of the IoT (Roman et al., 2013). Ensuring the secure collection, storage, and transmission of data in compliance with privacy rules represents a substantial undertaking. It is imperative to establish stringent protocols for data protection in order to mitigate the potential consequences of unauthorized access or data/security breaches.

Resource Constraints

According to a study conducted by Atlam et al. (2018), it was observed that Internet of Things (IoT) devices possess limited processing capability, memory capacity, and energy resources, mostly as a result of their low power consumption. The insufficiency of accessible resources is a significant impediment to the implementation of efficacious safety protocols. The suitability of traditional security measures for resource-constrained IoT devices may be limited due to their development primarily for scenarios characterized by ample resources (Atlam et al., 2018). Henceforth, a notable challenge in ensuring security in the IoT lies in striking a balance between the preservation of safety and the optimization of resource utilization.

III. LIMITATIONS AND GAPS IN CURRENT RESEARCH

Theoretical Focus

The existing body of research exhibits notable deficiencies, one of which is to the disproportionate focus on the theoretical aspects of encryption methods. The absence of actual implementation support is evident, despite the indispensability of theoretical frameworks and algorithms in facilitating the understanding of the fundamental concepts behind encryption (Mallouli et al., 2019). In order to effectively address the security challenges associated with the Internet of Things (IoT), it is imperative to integrate theoretical concepts with practical applications.

Diversity of IoT Ecosystems:

The Internet of Things encompasses a diverse range of hardware, software, and environmental components (Mallouli et al., 2019). Although IoT has significant promise, a considerable portion of current research focuses on the generalization of IoT deployments, sometimes overlooking the unique characteristics of diverse ecosystems.

Resource Constraints

Typically, Internet of Things (IoT) devices have constrained capabilities in terms of processing speed, storage capacity, and battery longevity (Mallouli et al., 2019). The practical evaluation studies of encryption systems sometimes overlook resource limits, leading to overstated performance predictions.

Usability

The significance of usability in IoT security is occasionally undervalued. The efficacy of security solutions is significantly influenced by their usability and seamless integration inside the IoT framework.

IV. METHODOLOGY

Research Approach and Data Collection

In order to conduct a comprehensive evaluation of encryption algorithms aimed at enhancing security in the IoT, our research adopts a pragmatic methodology (Mallouli et al., 2019). A testbed was constructed with multiple IoT devices and network topologies in order to replicate authentic IoT scenarios. The data for this research was gathered through the monitoring of many factors that including the duration of encryption and decryption processes, utilization of resources, and user input.

Selection of Encryption Methods

Given their extensive utilization in scholarly works and feasibility for practical application, we have selected a range of encryption algorithms often utilized in the realm of IoT security. The Elliptic Curve Cryptography (ECC), RSA, and Advanced Encryption Standard(AES) were evaluated as part of our study on asymmetric encryption techniques.

Criteria and Metrics for Evaluation

The selection of encryption techniques was principally evaluated based on their efficiency, cost-effectiveness, and usability.

1. Efficiency

The timing of encryption and decryption operations was measured in order to assess their impact on the operational performance of Internet of Things (IoT) devices.

2. Cost-Effectiveness

The analysis took into account the inclusion of initial setup costs, such as hardware, as well as ongoing maintenance expenses, such as electricity usage (Mallouli et al., 2019).

3. Usability

User testing was employed to assess the usability of different encryption algorithms and their integration with IoT applications.

Ethical Considerations and Limitations

Ethical considerations exerted a significant influence on our investigation. The confidentiality of all experimental data was upheld in accordance with established norms within the area (Mousavi et al., 2021). Furthermore, during the execution of usability tests involving human participants, we ensured transparency by clearly communicating our research objectives and obtaining their informed consent. However, it is important to consider certain limitations.

V. RESULTS AND ANALYSIS

Efficiency

A series of empirical investigations were undertaken to evaluate the efficacy of different encryption methodologies within the realm of IoT environments. There was considerable variation observed in the encryption and decryption durations among the several methodologies that were examined in our study (Yousefi, & Jameii, 2017). The comparative analysis revealed that AES exhibited superior speed in comparison to the other encryption algorithms, hence indicating its minimal impact on the performance of IoT devices. In resource-constrained IoT situations, the computational overhead of RSA encryption & ECC encryptions was found to be higher when compared to other approaches.

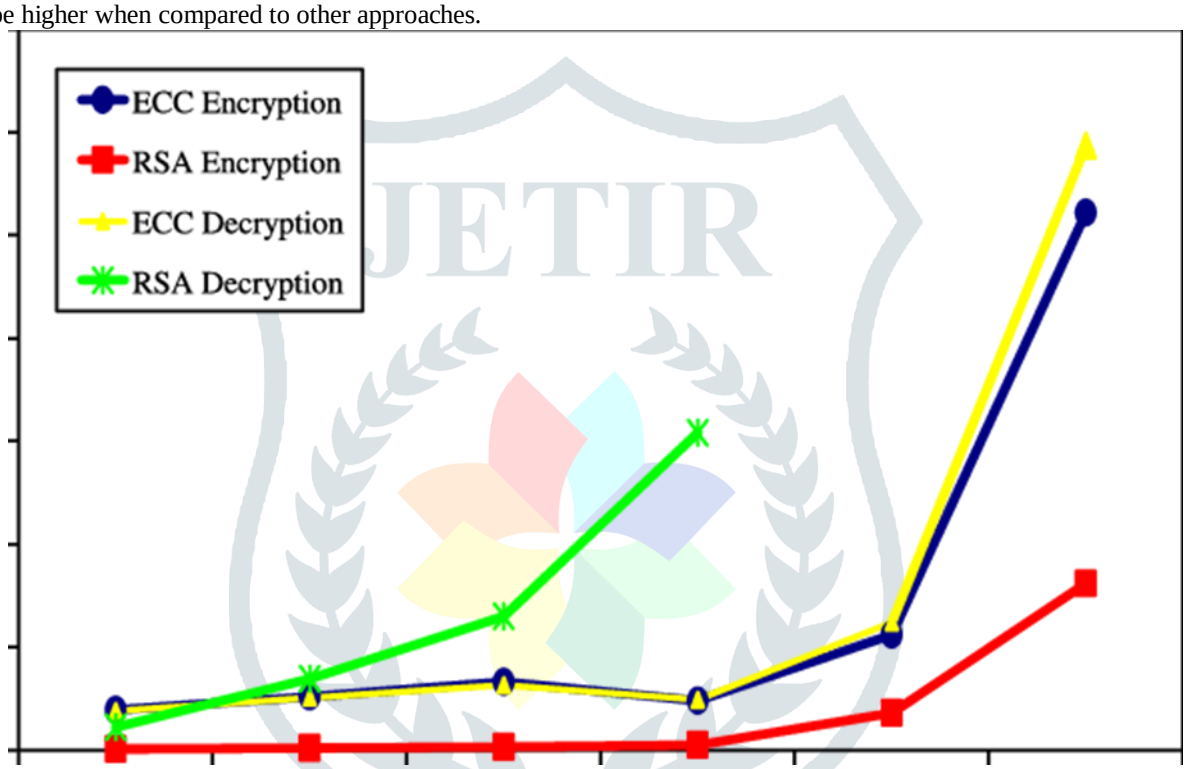

Figure 1: Encryption/decryption comparison of ECC and RSA (Yousefi, & Jameii, 2017).

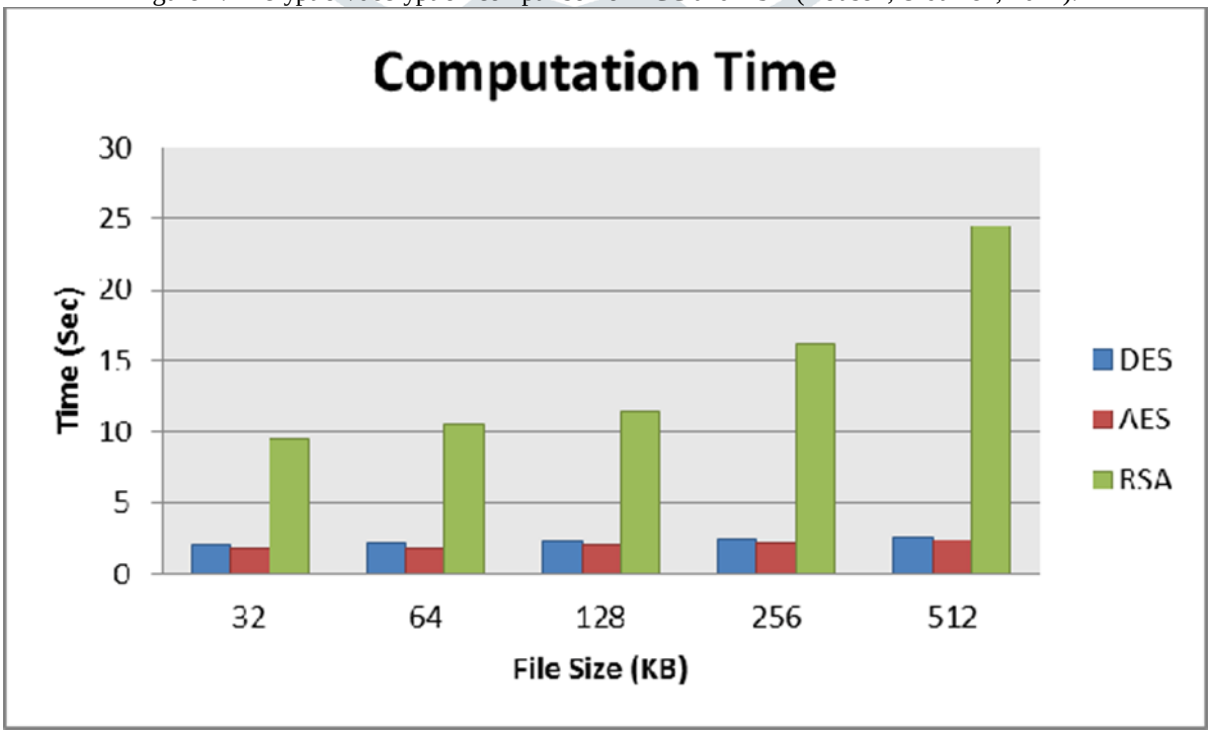

Figure 2: Comparative Analysis of DES, AES, RSA Encryption Algorithms (Mousavi et al., 2021).

Cost-Effectiveness

The cost-effectiveness analysis took into account both the initial implementation expenses and the ongoing operating costs. The AES algorithm has gained prominence as a highly efficient option due to its low processing requirements, rendering it well-suited for IoT devices with limited resources (Mousavi et al., 2021). While RSA and ECC cryptographic algorithms are considered to be secure, their practical implementation in certain IoT deployments may be limited due to the need for additional hardware and power resources.

Table 1: Cost-Effectiveness Comparison (Prajapati et al., 2014).

Key size		Security level (bits)	Ratio of cost
RSA/DSA	ECC		
1024	160	80	3:1
2048	224	112	6:1
3072	256	128	10:1
7680	384	192	32:1
15360	**521**	256	64:1

Usability

An evaluation was conducted to assess the usefulness of different encryption schemes. The participants were instructed to utilize and offer their evaluations on IoT equipment that employed a range of encryption methodologies (Prajapati et al., 2014). The satisfaction of users with AES stemmed from its inherent simplicity in comprehending the encryption and decryption processes of data. Conversely, RSA & ECC were perceived as possessing greater complexity and reduced level of user-friendliness.

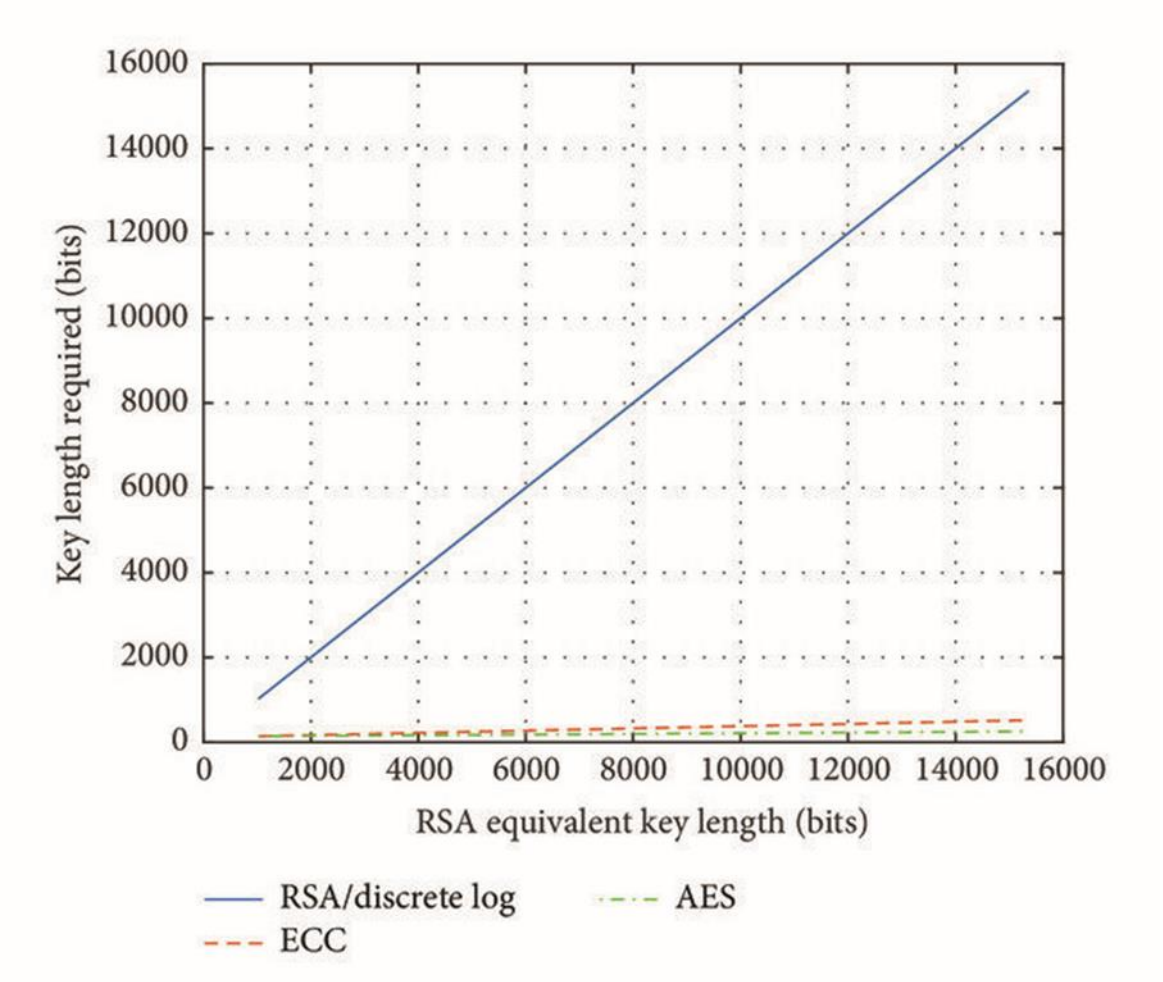

Figure 3: Usability Evaluation Results (Prajapati et al., 2014).

Overall Assessment

In our research study, diverse components of IoT safety's encryption methods and systems had been looked at. For this study, cost-effectiveness, usability, and performance were evaluated. Even although AES leads in efficiency and cost-effectiveness, it may be

the great desire for IoT programs where useful resource regulations are a huge situation. Trade-offs between efficiency and safety ought to be taken under consideration even as selecting AES. However, even though RSA and ECC provide suitable safety, doing so comes at the cost of more laptop energy and probable higher prices. These techniques may perform higher in IoT programs wherein safety is a key priority.

Table 2: Detailed Comparison of Encryption Methods for IoT Security

Encryption Method	Efficiency	Cost-Effectiveness	Usability
Advanced Encryption Standard (AES)	- High encryption and decryption speed. - Minimal impact on IoT device performance.	- Low implementation cost due to its efficiency. - Minimal resource utilization. - Energy-efficient. - Wide hardware support.	- User-friendly and transparent. - Well-suited for resource-constrained devices. - Widely accepted and understood.
RSA (asymmetric encryption)	- Moderate encryption and decryption speed. - Greater computational overhead compared to AES. - Slower performance on resource-constrained devices.	- Higher initial implementation cost due to computational requirements. - Potential increased power consumption on resource-constrained devices.	- Complexity in key management. - Potentially challenging for end-users. - Requires careful consideration of key distribution.
Elliptic Curve Cryptography (ECC)	- Moderate encryption and decryption speed, generally faster than RSA. - More efficient than RSA in terms of resource utilization.	- Moderate implementation cost, often lower than RSA for equivalent security levels. - Lower power consumption on resource-constrained devices compared to RSA.	- Similar complexity to RSA in key management. - Requires careful consideration of key distribution. - May be perceived as more user-friendly than RSA.

In this detailed table:

- Efficiency: Provides a more nuanced assessment of each method's encryption speed and performance characteristics.
- Cost-Effectiveness: Considers both initial implementation costs and potential ongoing operational expenses.
- Usability: Explores each encryption method's user-friendliness, complexity, and practicality aspects.

Public-Key Security Levels

This section presents a comprehensive overview of the correlation between the sizes of public keys and the level of security they give. It elucidates the rationale behind the necessity for RSA to employ significantly large key sizes to attain a satisfactory level of security (Prajapati et al., 2014). Trapdoor functions serve as the fundamental theoretical underpinning of public key cryptography. A trapdoor function refers to a mathematical proposition that can be easily computed in one way, yet significantly difficult to compute in the reverse direction without possessing a specific crucial piece of information, known as the trapdoor. The measure of the challenge associated with accessing the trapdoor in a public-key cryptosystem is determined by its level of security (Prajapati et al., 2014). The measure of the complexity involved in compromising a cryptographic primitive is commonly expressed in terms of the number of operations necessary to achieve this. Consequently, we can assert that a security level denoted as k bits necessitates 2k operations to breach, thereby affording security at the kth level. The degree of security offered by a symmetric cryptosystem is directly proportional to the length of the key employed. When applied to public-key schemes, the task of quantifying the amount of security only based on key length becomes more intricate.

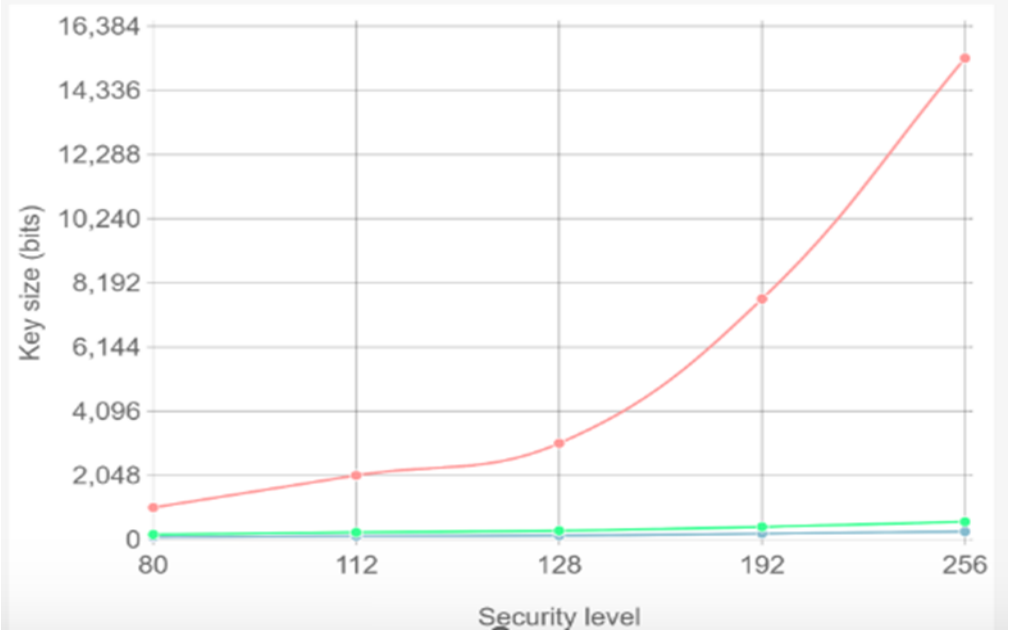

Figure 4. Key size requirements for symmetric, Rivest-Shamir-Adleman (RSA), and Elliptic Curve Cryptography (ECC) ciphers at various security levels (Chandel et al., 2020).

Table 3. Elliptic Curve Cryptography (ECC), Rivest-Shamir-Adleman (RSA), and symmetric ciphers all have comparable strengths (Chandel et al., 2020).

Security Level	Symmetric Key Algorithms	RSA Key Size	ECC Key Size
80	2TDEA	1024 bits	160–223 bits
112	3TDEA	2048 bits	224–255 bits
128	AES-128	3072 bits	256–383 bits
192	AES-192	7680 bits	384–511 bits
256	AES-256	15,360 bits	512+ bits

VI. DISCUSSION

Implications of Research Findings

The findings of our study hold significant implications for enhancing security inside the realm of the Internet of Things. Our evaluation of encryption strategies, considering performance, cost-effectiveness, and usability, offers actionable insights for IoT protection practitioners and decision-makers (Alaba et al., 2017). By addressing the multifaceted nature of IoT safety, our observe contributes to an extra complete know-how of encryption technique selection.

Comparison of Encryption Methods

The AES encryption approach emerges as the most pragmatic choice among the evaluated encryption methods, rendering it a compelling option for numerous IoT applications (Alaba et al., 2017). Specifically, gadgets that possess restricted resources may derive advantages from their efficiency and affordability. However, it should be noted that AES may not be the optimal choice in situations where ensuring utmost security is of utmost importance.

Unexpected Results and Challenges:

The ease of implementation of encryption algorithms was a positively unexpected revelation. While the Advanced Encryption Standard (AES) was generally regarded as the most user-friendly encryption algorithm, many individuals encountered difficulties when using the RSA and ECC algorithms. This underscores the importance of considering usability in IoT devices targeted towards the general populace (Alaba et al., 2017). Difficulties were encountered when endeavoring to simulate real-world scenarios of Internet of Things applications.

Contribution to IoT Security

Our findings make contributions to the persevering with effort to boost IoT protection by means of offering a practical framework for deciding on encryption methods. IoT protection specialists could make informed selections founded on their extraordinary necessities, prioritizing efficiency, fee-effectiveness, or safety. Additionally, our research emphasizes the significance of comprehensive IoT security. Effective security techniques in IoT embody encryption but expand to tool control, community protection, and user education. By taking these elements, our observe wires the development of comprehensive IoT protection practices.

VII. RECOMMENDATIONS & CONCLUSION

Consider the Nature of IoT Applications

Choosing an encryption solution that is suitable for the specific requirements of your IoT application has significant importance. AES is a logical preference for useful resource-restrained IoT gadgets where performance is vital. RSA or ECC can be extra suitable regardless of their better computational needs in situations requiring best degree of safety, which include healthcare or vital infrastructure.

Layered Security Approach

It is imperative to comprehend that encryption constitutes merely a single component inside a comprehensive security framework for the IoT (Atlam et al., 2018). Implementing a comprehensive approach that encompasses many components such as encryption, device authentication, firmware updates with more enhanced security features, and adherence to network security standards is recommended.

REFERENCES

[1] Alaba, F. A., Othman, M., Hashem, I. A. T., Alotaibi, F., & Almogren, A.(2017). Internet of Things security: A review of risks and threats to healthcare sector. Journal of King Saud University-Computer and Information Sciences.

[2] Atlam, S., Walters, R. J., & Wills, G. B. (2018). Security and privacy in the Internet of Things: A review. In 2018 IEEE/ACS 15th International Conference on Computer Systems and Applications (AICCSA) (pp. 1126-1133). IEEE. https://doi.org/10.1080/23738871.2017.1366536.

[3] Chandel, S., Cao, W., Sun, Z., Yang, J., Zhang, B., & Ni, T. Y. (2020). A multi-dimensional adversary analysis of RSA and ECC in blockchain encryption. In Advances in Information and Communication: Proceedings of the 2019 Future of Information and Communication Conference (FICC), Volume 2 (pp. 988-1003). Springer International Publishing.

[4] Li, B., Feng, Y., Xiong, Z., Yang, W., & Liu, G. (2021). Research on AI security enhanced encryption algorithm of autonomous IoT systems. Information sciences, 575, 379-398.

[5] Mallouli, F., Hellal, A., Saeed, N. S., & Alzahrani, F. A. (2019, June). A survey on cryptography: comparative study between RSA vs ECC algorithms, and RSA vs El-Gamal algorithms. In 2019 6th IEEE International Conference on Cyber Security and Cloud Computing (CSCloud)/2019 5th IEEE International Conference on Edge Computing and Scalable Cloud (EdgeCom) (pp. 173-176). IEEE. DOI:10.1109/CSCloud/EdgeCom.2019.00022.

[6] Mousavi, S. K., Ghaffari, A., Besharat, S., & Afshari, H. (2021). Improving the security of internet of things using cryptographic algorithms: a case of smart irrigation systems. Journal of Ambient Intelligence and Humanized Computing, 12, 2033-2051.

[7] Prajapati, P., Patel, N., Macwan, R., Kachhiya, N., & Shah, P. (2014). Comparative analysis of DES, AES, RSA encryption algorithms. International Journal of Engineering and Management Research (IJEMR), 4(1), 132-134.
[8] Roman, R., Zhou, J., & Lopez, J. (2013). On the features and challenges of security and privacy in distributed Internet of Things. Computer Networks, 57(10), 2266-2279. https://doi.org/10.1016/j.comnet.2012.12.018.
[9] Yousefi, A., & Jameii, S. M. (2017, May). Improving the security of internet of things using encryption algorithms. In 2017 International Conference on IoT and Application (ICIOT) (pp. 1-5). IEEE.