International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 9s
Article Received: *15 April 2023* ***Revised:*** *25 July 2023* ***Accepted:*** *18 August 2023*

Designing and Executing Security Solutions for IoT-5G Environment

Pratik Shah
Department of Computer Science & Engineering
Dr. A.P.J. Abdul Kalam University
Indore, India
pratikshah009@yahoo.com

Dr. Deepika Pathak
Department of Computer Science & Engineering
Dr. A.P.J. Abdul Kalam University
Indore, India
deepikapathak23@gmail.com

Abstract—The integration of the Internet of Things (IoT) with 5G networks presents a transformative approach to modern connectivity solutions, yet it introduces significant security challenges. This paper focuses on the design and implementation of robust security techniques tailored for IoT-5G systems. We commence by analyzing the unique security requirements posed by the confluence of IoT devices and 5G technology, emphasizing the need for advanced security protocols to address increased data volumes, device heterogeneity, and potential vulnerabilities. Subsequently, we propose a comprehensive security framework that includes innovative encryption methods, intrusion detection systems, and secure communication protocols specifically developed for the IoT-5G environment. Our approach integrates multi-layered security mechanisms to ensure data integrity, confidentiality, and availability across the network. The effectiveness of our proposed techniques is demonstrated through a series of simulations and real-world deployments, showcasing significant enhancements in security and resilience for IoT-5G systems. This study contributes to the field by providing a practical and scalable security solution, paving the way for secure and reliable IoT-5G integration in various applications, from smart cities to industrial automation.

Keywords- Internet of Things , IoT-5G , Multi-Layered Security , 4G , 5G , RSA.

I. INTRODUCTION

Over recent years, the Internet of Things (IoT) has significantly propelled technological progress and industry growth. IoT devices, often equipped with sensors, collect data from their surroundings and use the internet for data processing and action initiation. These devices are characterized by their communication capabilities, data storage, and unique physical addresses. The IoT revolution has impacted various sectors such as agriculture, smart cities, water management, and environmental monitoring. For example, in agriculture, IoT aids in monitoring soil moisture and greenhouse conditions, while in smart cities, it assists in parking management and health monitoring. In water management, IoT is crucial for leak detection and water level monitoring, and it also plays a key role in detecting forest fires and monitoring air pollution.

The primary challenge lies in establishing a secure and confidential communication infrastructure to protect data from unauthorized access. As data security, integrity, and privacy are paramount for organizations and individuals, there is a growing demand for secure IoT devices. These devices, which function with minimal human intervention, are leading to increased automation. Various companies offer products and technologies that utilize the internet for data sharing and communication.

The IoT primarily consists of two components: the internet and physical objects. The internet is a vast network system facilitating resource and data sharing, while 'things' refer to a wide range of devices like street lights, appliances, vehicles, and air conditioners, with applications in sectors like retail, education, healthcare, and smart cities. In essence, IoT is a system where objects intelligently interact by exchanging data over the internet, aiming to minimize human-machine interaction and enhance machine-to-machine communication.

The IoT journey began in the 1960s with the advent of embedded internet, but the term 'IoT' was coined in 1999, initially associated with Radio Frequency Identification (RFID) and sensor technology. It gained prominence in 2010, especially with the Chinese government's five-year plan to develop IoT. Today, with approximately 30 billion devices globally, IoT has become a staple in daily life, with its rapid growth leading to significant business opportunities. However, this rapid expansion has also brought data security and privacy concerns. IoT devices are often vulnerable to hacking and malfunction due to weaker security protocols. Various security measures have been developed, but inadequate adherence to security guidelines has left users exposed to cyber attacks.

IoT-enabled devices have long been used in manufacturing for competitive advantage, but data leakage concerns are prevalent. Hence, data security experts are essential for assessing risks and ensuring service continuity. With the advent of the 5G network in 2023, its impact on IoT and associated security vulnerabilities is a key research focus.

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 9s
Article Received: *15 April 2023* ***Revised:*** *25 July 2023* ***Accepted:*** *18 August 2023*

This study aims to provide a comprehensive analysis of IoT devices, including their applications, benefits, risks, and potential solutions. It involves a thorough literature review of current data security methods, followed by the deployment of a proposed solution and its performance evaluation against existing methods. This research will serve as a basis for future studies in data security and provide guidance to concerned stakeholders.

IoT devices, increasingly used by businesses and households, lack a universally accepted architecture. The typical IoT architecture comprises sensors, actuators, protocols, networking systems, and cloud services, often organized into four levels for effective management. These layers facilitate data transmission from sensors to networks and the cloud for processing, analysis, and storage. The following image presents the commonly accepted four-layer design of IoT architecture.

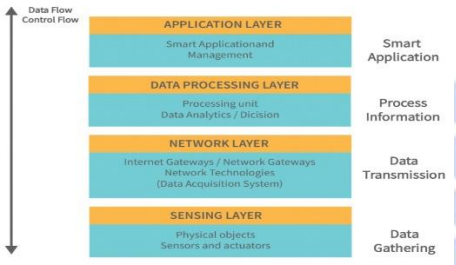

Figure 1: Architecture of IoT

The functioning of the four levels is as follows:

The sensing layer, as the foundational component of the IoT architecture, is primarily responsible for collecting data from a variety of sources. This layer comprises sensors and actuators embedded in the environment, tasked with recording various parameters such as light, temperature, sound, humidity, and moisture. These components are crucial for gathering the initial data that IoT systems rely on.

Following the sensing layer is the Network Layer, often considered the second tier of IoT architecture. Its main function is to establish a communication network among IoT devices. This layer includes various communication protocols and technologies that not only facilitate inter-device connectivity but also link IoT devices to the cloud for data storage and processing. Examples of technologies used in this layer include Wi-Fi, Bluetooth, and mobile networks like 4G and 5G. It also encompasses routers and gateways that bridge IoT devices with the Internet. Additionally, this layer is responsible for providing encryption and decryption services, playing a critical role in ensuring the security of data transmission.

The third tier is the data processing layer, which handles the aggregation, summarization, and analysis of data received from IoT devices. This layer processes the raw data collected by devices, employing mathematical algorithms to transform it into actionable information. It typically consists of database management systems and various algorithms for data analysis, which are instrumental in extracting meaningful insights from the amassed data. A key component of this layer is the data lake, a storage repository that holds vast amounts of raw data gathered from IoT devices and products.

At the pinnacle of the IoT architecture is the application layer, which serves as the user's gateway to the IoT system. This layer provides an interface through which users can control and interact with IoT devices. It is accessible via mobile applications, websites, and other user interfaces, enabling direct user interaction with the IoT system. The application layer relies on the data provided by the data processing layer and may incorporate machine learning algorithms, data visualization techniques, and other advanced methods to enhance user experience and decision-making processes.

II. LITERATURE REVIEW

Due to the widespread digitalization and the continuous improvement in internet speed, the user base is growing steadily. Each internet user shares data with their acquaintances, relatives, colleagues, etc. However, almost every user is undoubtedly concerned about the security and privacy of their data as it traverses the internet. Multiple hackers and cyber attackers persistently target consumers' personal information using innovative ways. Conversely, the team of researchers and software engineers have devised several tools and methodologies to safeguard user data, such as firewalls, antivirus software, network security protocols, and cryptographic approaches. The number 21.

Cryptography is essential for safeguarding data from cyber-attacks. Encryption is the process in cryptography where the sender transforms the original message, which is readable text, into cypher text, which is unreadable text, using specific procedures and formulas. On the other hand, decryption refers to the process in which the receiver obtains the original message by decoding the encrypted text, or cypher text, using specific techniques and formulas. Data encryption and decryption rely on the use of cryptographic keys.

The original RSA technique utilises two prime numbers, while [40] has used four prime numbers to enhance the data security of the algorithm. However, this modification inevitably leads to an increase in the time complexity of both encryption and decryption processes. The calculative capacity of RSA has been enhanced by using the formula N=PrQ, where r is greater than or equal to 2. This modification has significantly increased the level of data protection. The RSA method has been enhanced by including Digital Signatures. This enhancement involves the use of big prime numbers and the exclusion of the variable "N". As a result of this alteration, the performance of the algorithm has increased. The RSA algorithm has been enhanced by using three big prime numbers, resulting in greater data security. However, this modification increases the decryption time for encrypted data.

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 9s
Article Received: *15 April 2023* ***Revised:*** *25 July 2023* ***Accepted:*** *18 August 2023*

The RSA method has been enhanced by using the DFA - Diffie Hellman method and utilising a database for mathematical computations. This modification has significantly enhanced the algorithm's performance. The RSA method has been enhanced by using multiple prime numbers, resulting in higher algorithmic complexity and better data security. However, the execution of such complicated operations necessitates high-performance computers. The researchers have enhanced RSA by using the homomorphic features of data, resulting in a variant called hybrid RSA. However, the implementation of sophisticated operations using this method requires very advanced machinery.

To enhance the efficiency of RSA, several researchers have made alterations to key generation processes, enhanced encryption methods, and accelerated decoding methods. Multiple variations of RSA have become popular, including Multi-Power RSA, Batch RSA, Rebalanced RSA, Multi-Prime RSA, Dual RSA, and Twin RSA.

To enable the use of RSA on compact devices, researchers [27] have lowered the bit size. This allows for faster decoding of encrypted data and significantly reduces computational complexity. A major problem arises when the encrypted text is lengthy and the recipient attempts to decode it using a small-sized device. This situation may result in much longer processing times or even cause the device to freeze. However, this approach has shown enhanced performance on small-sized devices.

[28] has devised Multi-Prime RSA, which employs the same encryption technique as the classic approach. However, the decryption process differs. The Multi-Prime RSA algorithm derives its name from its utilisation of multiple prime numbers. However, this approach compromises the security of the data. If the size of the prime numbers is small, an attacker may access them by performing the modulus operation on N.

[29] Researchers have devised an energy-efficient technique to mitigate packet loss resulting from congestion during data transmission and reception. The team has integrated queue size, traffic rate, and contention to develop a technique for estimating congestion. A hybrid solution, including both data rate control and multipath routing control protocol, is used to effectively manage congestion. This technology has shown a significant enhancement in packet delivery, reduction in drop and latency. However, it lacks sufficient improvement in data security and has not been compared to current methods in terms of performance.

Researchers have created a revised edition of PEGASIS. It is a protocol used to route packets in wireless sensor networks. This procedure relies on the measurement of distance and the remaining energy. Given the limited energy of the sensors, it is imperative that the routing protocol be designed to be energy efficient. The team has devised a novel approach to evaluate the adjacent nodes. The primary objective of the development was to enhance the quantity of active nodes while simultaneously preserving low energy usage. The researchers also proposed that the use of appropriate optimisation techniques would result in reduced energy consumption for this approach.

III. PROPOSED SOLUTION & IMPLEMENTATION

In this section, we will implement several measures to achieve data security objectives for IoT-5G systems, utilizing the Boltzmann Machine for secure key generation and enhancing the RSA algorithm.

1. **Boltzmann Machine for Key Generation:** The Boltzmann Machine will be employed to generate secure keys. Its performance in key generation, along with encryption and decryption times, will be assessed and compared with other existing methods.

Characteristics of the Boltzmann Machine:

- **Nodes:** Comprising synthetic neurons, the Boltzmann Machine's nodes form layers. These include visible and hidden layers, each serving a specific purpose.
- **Connectivity:** The nodes across different layers are intricately interconnected, with each visible node connected to a hidden node and vice versa. However, there is no interconnectivity within the same layer.
- **Energy Function:** An energy function is utilized to measure the compatibility between hidden and visible nodes. It configures the network by assigning an energy value to the setup.
    - **Stochasticity:** The Boltzmann Machine exhibits stochastic behavior, employing a probabilistic approach for data representation.
    - **Learning:** The training of Boltzmann Machines focuses on minimizing the energy of the network configuration by reducing the weight of connections between nodes.

2. **RSA Algorithm Enhancement:** We aim to improve the RSA algorithm to boost its performance. This enhanced version will then be compared with the current iterations of RSA to evaluate its efficacy.
3. **Application of Restricted Boltzmann Machines (RBM):** The proposed approach involves using RBMs for the generation of dynamic and efficient asymmetric key generators. RBMs will be employed for both encrypting plaintext and decrypting encrypted content.
4. **Security Analysis:** A thorough security analysis will be conducted to demonstrate the effectiveness of the system. During encryption and decryption, each character is altered. The output from eight neurons is concealed in a single layer responsible for encrypting diverse sets of eight-bit inputs.

Through these steps, we aim to establish a robust and secure framework for IoT-5G systems, ensuring data security through advanced cryptographic methods and machine learning algorithms.

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 9s
Article Received: *15 April 2023* ***Revised:*** *25 July 2023* ***Accepted:*** *18 August 2023*

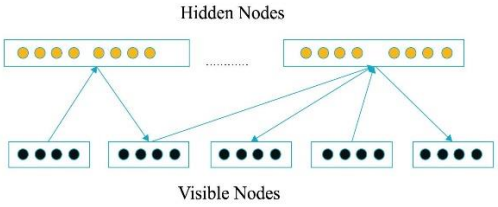

Figure 2: Working of Hidden nodes and Visible Nodes

Given that the activation function of the hidden layer operates within a range of 0 to 1, the process involves storing the encrypted text as an eight-dimensional vector. This vector, when multiplied with the input data, results in an array consisting of eight floating-point values. This method effectively leverages the constrained range of the activation function to generate a structured and secure encrypted output.

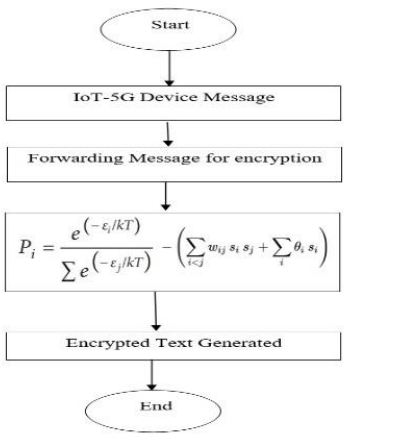

Figure 3: Encryption Process Working

The decryption of the text in the output layer is facilitated using the Boltzmann Machine Distribution function and the proposed formula. This process involves the utilization of twelve-dimensional floating-point values, ensuring a precise and effective decryption mechanism.

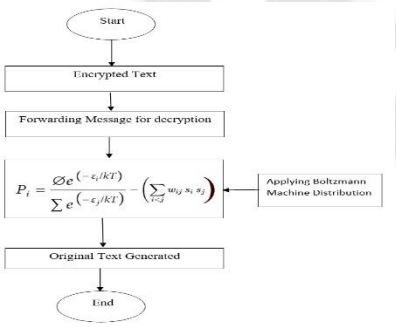

Figure 4: Decryption Process Working

The author's proposed approach offers a secure method for encrypting and decrypting data.

To implement this approach and the accompanying formula, the following hardware and software components are utilized:

Hardware Components:

- Hard Disk Drive: 1 Terabyte (TB) for ample storage capacity.
- Random Access Memory (RAM): 8 Gigabytes (GB) to ensure smooth processing and multitasking capabilities.
- Central Processing Unit (CPU): Intel Core i3, providing sufficient computational power for the encryption and decryption processes.

Software Components:

- Application Software: Notepad++ is used as the primary application software, offering a versatile platform for coding and script editing.
- Operating System: Windows 10, providing a stable and user-friendly environment for running the application and programming tasks.
- Programming Language: Python, chosen for its efficiency, readability, and wide range of libraries, making it suitable for implementing complex cryptographic algorithms.

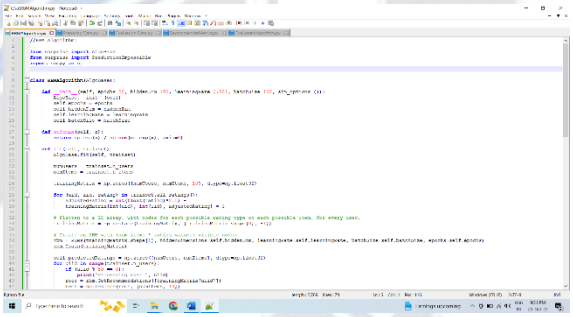

Figure 5: RBM Algorithm Implementation

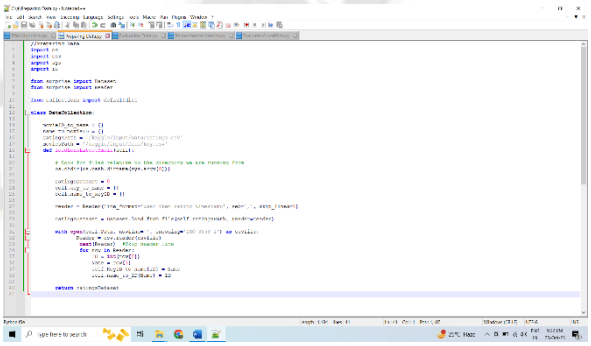

Figure 6: Preparing Data Implementation

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 9s
Article Received: *15 April 2023* ***Revised:*** *25 July 2023* ***Accepted:*** *18 August 2023*

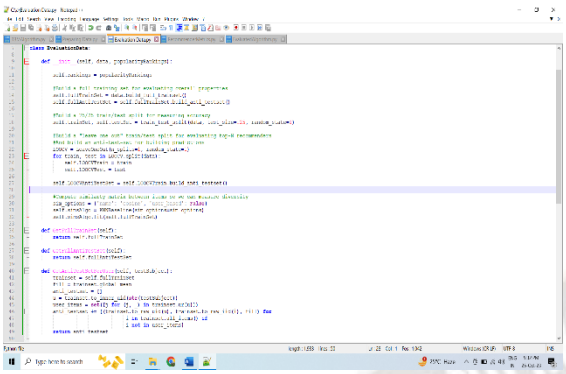

Figure 7: Evaluation Data & Key Generation Implementation

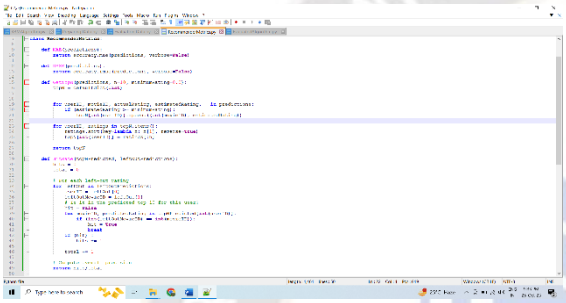

Figure 8: Recommended Matrix Implementation

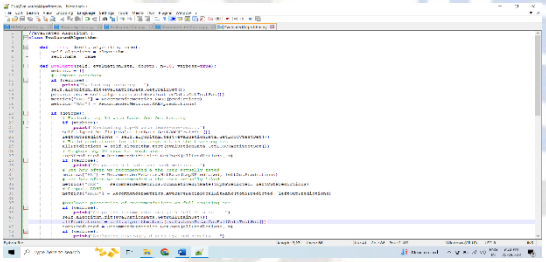

Figure 9: Cryptography Evaluation Implementation

The screenshots provided above illustrate the implementation of the proposed method for key generation, encryption, and decryption using the Restricted Boltzmann Machine. The subsequent chapter will delve into a detailed analysis of the results obtained from this proposed system.

IV. RESULT

There are a number of issues about the future of data security in Internet of Things (5G) systems. This is due to the fact that the area of technology is rather dynamic in nature, network speed is rising, and latency is extremely low. Additionally, Internet of Things devices are creating a massive quantity of data, and it will always be a topic of worry to ensure that the data is kept secure. The security procedures should be updated on a consistent basis in order to ensure that the devices are constantly prepared to protect against the most recent assaults and threats.

Table 1 Encryption and Decryption Time of all Files

File Input Size	Encryption Time take by the proposed method and formula	Decryption Time take by the proposed method and formula
600 KB	76	54
800 KB	100	80
6 MB	150	120
12 MB	300	220
40 MB	500	420
100 MB	600	510
150 MB	926	813

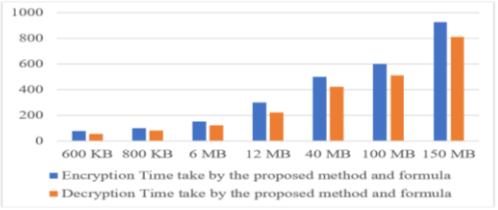

Figure 10 Encryption and Decryption Time by the proposed work

Based on the analysis of the data presented in Table 1 and Figure 10, it is observed that the Encryption Method generally requires more time compared to the Decryption Method. To further assess the effectiveness of the proposed methodology and formula, a comparative study will now be conducted against other cryptographic techniques, namely Diffie-Hellman, RSA, ECC (Elliptic Curve Cryptography), and ECDH (Elliptic Curve Diffie-Hellman).

The performance evaluation will focus on the total time required for both encrypting and decrypting files of specific sizes, as outlined in the aforementioned table. These file sizes include 600 KB, 800 KB, 6 MB, 12 MB, 40 MB, 100 MB, and 150 MB. This approach will provide a comprehensive understanding of how the suggested method stacks up against established cryptographic protocols, particularly in terms of processing time for encrypting and decrypting data files of varying sizes.

Table 2: Analysis of encryption time of proposed work with others

File Input Size	Encryption Time take by the proposed method and formula	Diffie-Hellman	RSA	ECC	ECDH
600 KB	76	246	243	228	236
800 KB	100	370	377	288	350
6 MB	150	388	570	298	359
12 MB	300	398	588	399	568
40 MB	500	588	656	596	636
100 MB	600	687	745	688	689
150 MB	926	1023	1021	940	935

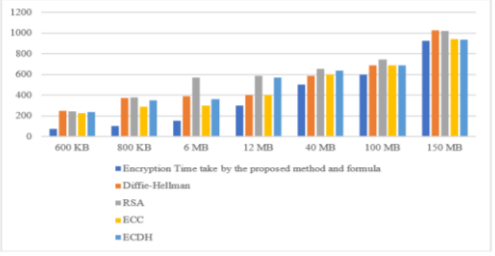

Figure 11: Comparison of encryption time of proposed work with others

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 9s
Article Received: *15 April 2023* ***Revised:*** *25 July 2023* ***Accepted:*** *18 August 2023*

From the data presented in Table 2 and Figure 11, it is evident that the proposed method and formula are more time-efficient in encrypting data compared to other methods. This efficiency in processing under various input conditions, with file sizes ranging diversely, indicates an enhanced performance of the suggested approach. The results clearly demonstrate that the proposed technique outperforms others in terms of speed, especially in the context of encrypting data files of different sizes.

File Input Size	Decryption Time take by the proposed method and formula	Diffie-Hellman	RSA	ECC	ECDH
600 KB	54	86	198	98	93
800 KB	80	275	290	190	198
6 MB	120	296	298	199	298
12 MB	220	298	480	470	460
40 MB	420	432	498	489	499
100 MB	510	552	510	599	632
150 MB	813	853	898	802	898

Table 3: Analysis of decryption time of proposed work with others

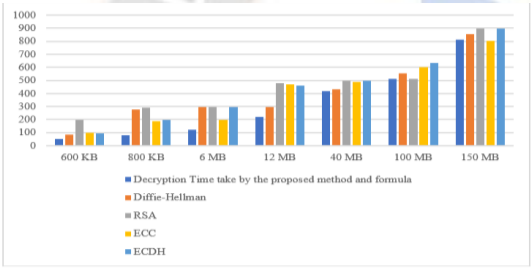

Figure 12: Comparison of decryption time of proposed work with others

Analyzing the data presented in Table 3 and Figure 12, it becomes apparent that the proposed technique and formula require less time for decrypting data compared to previous methods. This efficiency in handling a range of input file sizes showcases the enhanced performance of the suggested approach in terms of decryption.

Furthermore, considering the combined data from Tables 2 and 3, we can conclude that the overall performance of the proposed method in both encryption and decryption processes surpasses that of the conventional methods in use. This superiority in performance is evident across different file sizes, indicating the effectiveness and efficiency of the proposed technique in handling data security tasks.

V. CONCLUSION & FUTURE SCOPE

5.1 Conclusion

This Section delves into a detailed analysis of the outcomes produced by the proposed work. In this chapter, the results of the proposed cryptosystem are extensively compared with those of other well-known cryptographic systems. It is found that the proposed method demonstrates a notable efficiency, being able to perform encryption and decryption tasks in a shorter timeframe compared to other cryptosystems. This comparative analysis highlights the enhanced performance and time efficiency of the proposed system in handling cryptographic operations..

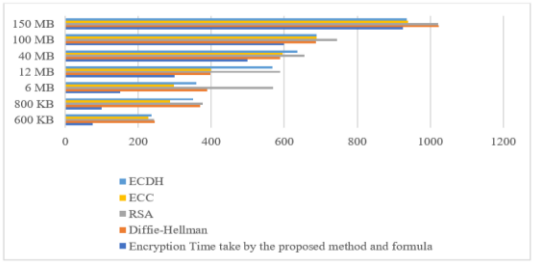

Figure 13: Encryption Time by the proposed work and others

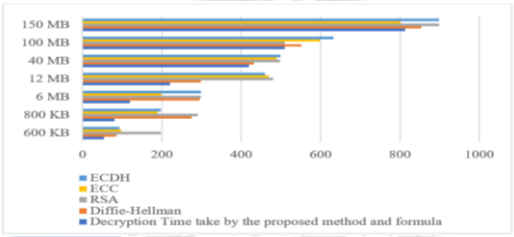

Figure 14: Decryption Time by the proposed work and others

The second study in the thesis focuses on the modification and enhancement of the RSA algorithm. This revised version of RSA, as discussed in the thesis, employs five distinct prime numbers along with Euler's totient function for the generation of public and private keys. The proposed version is adept not only in encrypting and decrypting data but also in generating these crucial cryptographic keys. An in-depth discussion of this algorithm is presented in Chapter 4, where its implementation is carried out using the Python programming language.

To measure the time efficiency of this modified RSA algorithm, the **timeit()** function from the Python Timeit module is utilized. This function provides the execution time in seconds, which are typically in decimal form. To facilitate easier comparison and to represent the values on a larger scale, these decimal values are converted into milliseconds.

The results of this program are thoroughly analyzed. To evaluate the performance of this modified RSA approach, its results are compared with various altered versions of RSA, such as HRSA, MRSA, and R-RSA. The comparative analysis in this chapter showcases the findings, allowing for a clear understanding of how the proposed RSA modification stands in relation to other similar cryptographic methods in terms of key generation, encryption, decryption, and overall time efficiency.:

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 9s
Article Received: *15 April 2023* ***Revised:*** *25 July 2023* ***Accepted:*** *18 August 2023*

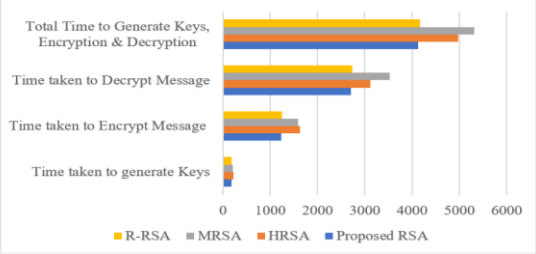

Figure 15. Performance evaluation of the proposed work with other RSA

The results indicate that the suggested RSA algorithm significantly outperforms the existing versions of RSA in terms of efficiency and effectiveness.

5.2 Future Scope : The future of data security in Internet of Things (IoT) systems, particularly with the advent of 5G technology, presents several challenges. This stems from the dynamic nature of technology, where network speeds are continually increasing, and latency is becoming exceptionally low. Furthermore, IoT devices are generating vast amounts of data, making the security of this data a persistent concern. To address these challenges, security protocols must be regularly updated to ensure that devices are always equipped to defend against the latest attacks and threats. This ongoing evolution in security measures is crucial to maintain the integrity and safety of data in IoT-5G ecosystems.

References

1. E. Leloglu, "A Review of Security Concerns in Internet of Things," Journal of Computer and Communications, vol. 5, pp. 121-136, 2017.
2. J. Singh, T. Pasquier, J. Bacon, H. Ko and D. Eyers, "Twenty Security Considerations for Cloud-supported Internet of Things," IEEE Internet of things Journal, vol. 3, pp. 126-134 2016.
3. X. Huang, P. Craig and H. Y. Lin, "SecIoT: A Security Framework for the Internet of Things," IEEE Internet of things Journal, vol. 9, pp. 3083-3094, 2015.
4. M. Mohammadi, M. Aledhari, A. Al-Fuqaha, M. Guizani and M. Ayyash, "Internet of Things: A Survey on Enabling," IEEE Explore, vol. 2, pp. 138-142, 2015.
5. L. Atzori, A. Iera and G. Morabito, "The social internet of things (siot)– when social networks meet the internet of things: Concept, architecture and network characterization," Computer Networks, vol. 56, pp. no. 3594-3608, 2012.
6. R. Zejun, L. Xiangang, Y. Runguo and Z. Tao, "Security and privacy on internet of things," in Electronics Information and Emergency Communication (ICEIEC), 7th IEEE International Conference, July 2017, pp. 150-156.
7. Z. Zhang and Q. Wen, "Application of dynamic variable cipher security certificate in internet of things," in International Conference on Cloud Computing and Intelligent Systems (CCIS), July 2012, pp. 203-209.
8. K. Zhao and L. Geo, "A survey on the internet of things security," in International Conference on Computational Intelligence and Security (CIS), August – 2013, pp. 663-667.
9. H. Suo, W. Zou, and C. Liu, "Security in the Internet of Things: A Review," IEEE International Conference on Computer Science and Electronics Engineering, March 2012, pp. 23-25.
10. T. Nguyen and K. Laurent, "Survey on Secure Communication," Protocols for the Internet of Things. Ad Hoc Networks, vol. 32, pp. 17- 31, 2015.
11. A. Arseni, S. Halunga, S. Fratu and O. Vulpe, "Analysis of the Security Solutions Implemented in Current Internet of Things Platforms," in IEEE Conference on Grid, Cloud & High Performance Computing in Science, Romania, October 2015, pp. 28-30.
12. A. Tahir, M. Maier and A. Fernando, "A novel IC Metric based framework for securing the Internet of Things," in IEEE International Conference on Consumer Electronics, August 2016, pp. 469-470.
13. C. Zhang and C. Liu, "A Novel Approach to IoT Security Based on Immunology," in Ninth International Conference on Computational Intelligence and Security, August 2013, pp. 316-322.
14. C. Zhou, "Multimedia traffic security architecture for the internet of things," IEEE Explore, vol. 25, pp. 35-40, 2011.
15. Rose, "Security meets nanoelectronics for Internet of things," in International Great Lakes Symposium on VLSI, May 2016, pp. 356-362.
16. L. Santos, F. Guimaraes and C. Rodrigues, "A DTLS based security architecture for the Internet of Things," in IEEE Symposium on Computers and Communication, 2015, pp. 482-486.
17. T. Stepanova and P. Zegzhda, "Achieving Internet of Things security via providing topological sustainability," in International Conference on Science and Information, London, 2015, pp. 356-364.
18. L. Seitz, D. Sitenkov and G. Selander, "S3K: Scalable Security with Symmetric Keys—DTLS Key Establishment for the Internet of Things," IEEE Transactions on Automation Science and Engineering, vol. 13, pp. 896 - 902, 2016.
19. J. S. Kumar and D. R. Patel, "A Survey on Internet of Things: Security and Privacy Issues," International Journal of Computer Applications, vol. 90, 2014.
20. E. Bertino, S. R. Hussain and O. Chowdhury, "5G Security and Privacy: A Research Roadmap," CCC White Paper, vol. 4, pp. 356-365, 2020.
21. N. Li, M. Lyu, D. Su and W. Yang, "Differential Privacy: From Theory to Practice," Synthesis Lectures on Information Security, Privacy and Trust, pp. 129-138, 2016.
22. M.L. Damiani, E. Bertino and C. Silvestri, "The PROBE Framework for the Personalized Cloaking of Private Locations," Transactions on Data Privacy, Vol. 3, pp. 123-148, 2010.
23. G. Ghinita, K. Nguyen, M. Maruseac and C. Shahabi, "A Secure Location based Alert System with Tunable Privacy-Performance Trade-off," IEEE Access, Vol. 3, pp. 156-162, 2020.
24. R. Paulet, G. Kaosar, X. Yi and E. Bertino, "Privacy-Preserving and Content-Protecting Location Based Queries," IEEE Transactions on Knowledge and Data Engineering, Vol. 26, pp. 1200-1210, 2014.
25. M.I. Sarfraz, M. Nabeel, J. Cao, E. Bertino, "DBMask: Fine-Grained Access Control on Encrypted Relational Databases," Transactions on Data Privacy, Vol. 9, pp. 187-214, 2016.
26. M. Nabeel, E. Bertino, "Privacy Preserving Delegated Access Control in Public Clouds," IEEE Transactions on Knowledge and Data Engineering, Vol. 26, pp. 2268-2280, 2014.
27. S.H. Seo, M. Nabeel, X. Ding and E. Bertino, "An Efficient Certificateless Encryption for Secure Data Sharing in Public Clouds," IEEE Transactions on Knowledge and Data Engineering, Vol. 26, pp. 2107-2119, 2014.
28. B. Carminati, E. Ferrari and M. Viviani, "Security and Trust in Online Social Networks," Synthesis Lectures on Information Security, Privacy, and Trust, Vol. 6, pp. 163-172, 2021.
29. H. Gunasinghe and E. Bertino, "RahasNym: Protecting against Linkability in the Digital Identity Ecosystem," 35th IEEE International Conference on Distributed Computing Systems, USA, June 2015, pp. 365-375.
30. H. Gunasinghe, A. Kundu, E. Bertino, H. Krawczyk, S. Chari, K. Singh and D. Su, "PrivIdEx: Privacy Preserving and Secure Exchange of Digital Identity Assets," in The World Wide Web Conference, USA, May 2019, pp. 456-461