A Dual-Layer Approach: Combining Lightweight and Dynamic RSA for Enhanced Data Security

Balaji R
School of Computer Science and Engineering
Vellore Institute of Technology
Chennai, TamilNadu, India
balaji.r2021@vitstudent.ac.in

Sriraam C
School of Computer Science and Engineering
Vellore Institute of Technology
Chennai, TamilNadu, India
sriraam.c2021@vitstudent.ac.in

Lionel Donato L
School of Computer Science and Engineering
Vellore Institute of Technology
Chennai, TamilNadu, India
lioneldonato.l@vitstudent.ac.in

Krithin Ragav
School of Computer Science and Engineering
Vellore Institute of Technology
Chennai, TamilNadu, India
krithin.ragav2021@vitstudent.ac.in

Kanthimathi S
School of Computer Science and Engineering
Vellore Institute of Technology
Chennai, TamilNadu, India
kanthimathi.s@vit.ac.in

***Abstract*— Security is an important aspect for both individuals and business data. Security has been studied extensively by many researchers. Still, security gaps or threats are increasing, and data protection is a primary issue. An effective lightweight hybrid cryptographic algorithm with two layers of encryption is presented in this paper. A new effective, lightweight cryptographic algorithm named ASCON-128 is used in the first layer, and a Dynamic RSA Technique is used in the second layer. Both symmetric and asymmetric cryptography features are offered by this approach. The proposed algorithm's performance is evaluated using metrics such as execution time, throughput rate, delay, and latency. A higher level of security, a faster encryption execution times, reduced memory usages, and improved throughput were observed in the proposed algorithm when compared to widely used cryptographic systems. The results are shown by the experimental findings.**

Keywords - Security, RSA, Lightweight hybrid cryptography, ASCON-128

I. INTRODUCTION

Data transfer applications are vital for communication and collaboration, making the security and integrity of transmitted information crucial. Traditional encryption techniques often struggle to balance security and efficiency, particularly in real-time data transfer. To address this, a novel hybrid cryptographic algorithm that combines lightweight and traditional methods is proposed. Both symmetric and asymmetric algorithms are integrated by the proposed algorithm, enhancing security, and optimizing performance. This combination leverages the strengths of both types to mitigate their limitations, delivering improved security and efficiency in data transfer scenarios.

Unlike conventional approaches that rely solely on either symmetric or asymmetric encryption, a layered approach is employed by the proposed hybrid algorithm. This dual-layer integration ensures a more secure and efficient encryption process, suitable for a variety of data transfer applications.

The first layer of the proposed algorithm includes ASCON 128-bit encryption, a lightweight symmetric authenticated encryption algorithm known for its efficiency and robust security. ASCON's design is made ideal for constrained environments, such as IoT devices, where resource efficiency is paramount. Additionally, the encryption process is adjusted by the dynamic RSA method as the second layer based on input data characteristics, improving encoding and decoding times. By storing pre-computed values of frequently occurring data, computational overhead is reduced.

Performance evaluations demonstrate that computational time and time complexity are significantly improved by the proposed algorithm compared to existing methods. Experimental results showcase a substantial improvement in time complexity and computational time, validating the practicality and robustness of the proposed algorithm.

By combining the benefits of ASCON's lightweight, efficient design with the robust security features of dynamic RSA, a significant step forward in cryptographic research and its practical applications is represented by the proposed hybrid algorithm. This combination has the potential to address the critical needs in data transfer security, ensuring that both performance and protection are not compromised.

This paper has been divided into 8 sections. Section 1 is meant to serve as an overview containing an introduction to the proposed algorithm. Different studies that are linked to the research are outlined in Section 2. The proposed algorithm is explained in an elaborate manner in Section 3. The simulation environment is described in Section 4. The findings and comments are summarized in Section 5. Conclusions and recommendations for future research are suggested in the final section i.e. Section 6.

II. RELATED WORKS

A novel lightweight homomorphic cryptographic algorithm specifically designed for cloud computing environments was introduced by Thabit, et al., showcasing an innovative approach that marries efficiency with security to address the critical need for robust data protection in cloud services [1]. A significant advancement in the field of cryptography is represented by this work, offering a solution that is both efficient and secure for cloud-based applications.

Authors Krishnadoss, Pradeep, et al. [2] proposed a dynamic method aimed at reducing time complexity in RSA encryption and decryption processes was unveiled, highlighting the importance of adaptive encryption techniques in enhancing the practicality of RSA for real-time applications. By introducing a dynamic approach, contributions are made by this research to the ongoing efforts to optimize cryptographic algorithms for better performance and security.

A novel data security algorithm that leverages genetics techniques and logical-mathematical functions was proposed by the authors in this study [3], showcasing the potential of interdisciplinary methods in enhancing cryptographic security within cloud computing. This innovative approach demonstrates how combining different fields of study can lead to breakthroughs in cryptography, offering new ways to protect sensitive data in cloud environments.

A comprehensive overview of research [4] trends in RSA-based asymmetric cryptography techniques was provided by authors Mohd Saiful Adli, et. al., underscoring the role of RSA in securing digital communications and highlighting both developments and challenges within RSA cryptography. The importance of staying informed about the latest trends and advancements in cryptographic techniques to ensure effective data protection strategies is emphasized by this overview.

Within the healthcare industry, homomorphic encryptions play an important role. This study [5] by authors Munjal, Kundan, and Rekha Bhatia emphasizes its potential to enhance privacy and efficiency in secure data processing and analytics. By focusing on the healthcare sector, the practical applications of homomorphic encryption are highlighted by this review.

A study by authors of [6] introduced an innovative approach to enhancing the security of Ad-hoc On Demand Vector (AODV) routing protocol using Elliptic Curve Cryptography (ECC) and Ant Colony Optimization (ACO). This research focuses on improving the security aspects of wireless ad-hoc networks, particularly against black hole attacks, by integrating ECC for secure key exchange and ACO for optimizing route selection.

An efficient hybrid cryptography algorithm was introduced by authors Hoobi and Mayes M, designed to improve security across various digital platforms by combining cryptographic primitives for enhanced security [7]. The trend towards hybrid cryptographic solutions is exemplified by this algorithm, offering a balanced approach that leverages the strengths of different encryption methods to protect sensitive information across a wide range of applications.

Authors Mohammed, et. al. conducted a performance evaluation comparing RSA, ElGamal, and Paillier partial homomorphic encryption algorithms was conducted offering valuable insights into efficiency and security trade-offs among these algorithms [8]. Through this comparative analysis, guidance is aimed to be provided to practitioners in selecting the most suitable cryptographic solutions for specific applications, considering factors such as computational efficiency and security requirements.

The necessity of integrating security measures with timing considerations in safety-critical industrial cyber-physical systems was discussed in the study [9], emphasizing the importance of timing predictability alongside security. The multifaceted nature of security in industrial applications is highlighted by this discussion, where both the integrity of data and the timely execution of operations are considered very important.

Authors Dobraunig, et al. introduced a study introducing Ascon v1.2, a lightweight authenticated encryption and hashing algorithm [10], marking a significant contribution to the field of cryptography. This algorithm is particularly notable for its efficiency and security, making it well-suited for applications in memory constrained environments.

Xoodyak, a lightweight cryptographic algorithm was designed for efficiency and security in constrained environments, by authors Daemen, Joan, et al, addressing the growing need for cryptographic solutions that are both powerful and resource-friendly [11]. This introduction of Xoodyak represents a significant advancement in lightweight cryptography, catering to the demands of modern applications that require secure communication channels without compromising on performance.

The paper titled “Fast generation of RSA keys using smooth integers” [12] was by authors Dimitrov, Vassil, Luigi Vigneri, and Vidal Attias. It presents a novel method for accelerating RSA key generation and enhancing the performance of cryptographic systems. This method simplifies the key generation process, making RSA encryption more accessible and efficient for a wider range of applications.

RSA acceleration utilizing parallelization was proposed in the study [13], showcasing how parallel processing can significantly enhance the efficiency of RSA encryption and decryption processes. This innovation leverages computational resources to streamline cryptographic operations, reducing latency in secure communications.

An improvement to the RSA algorithm using Euclidean techniques was presented by authors [14] Lizy .et .al, enhancing its efficiency and contributing to ongoing efforts to refine cryptographic techniques. By incorporating mathematical optimizations, this work advances the state-of-the-art RSA encryption, offering a more streamlined approach to data security.

Cloud computing, while offering scalability and efficiency, faces significant security challenges including data breaches, unauthorized access, and cyber-attacks [15]. To mitigate these risks, organizations should adopt strong authentication measures like multi-factor authentication (MFA), ensure data encryption, keep systems updated with the latest security patches, segment networks for better isolation, and conduct regular security assessments. Additionally, employee training on cloud security best practices and vendor due diligence are crucial for maintaining a secure cloud environment.

III. PROPOSED METHODOLOGY

This section focuses on the methodology of the proposed cryptographic algorithm, an improved variation of the one proposed in an earlier study. The first layer is ASCON, a new and effective light-weight cryptographic algorithm and the second layer consists of a Dynamic RSA algorithm, which has an improved run-time compared to the traditional RSA. This Hybrid Cryptographic Algorithm offers both symmetric and asymmetric cryptographic features, which improves the data security and maintains confidentiality. The following subsections describe the proposed algorithm.

A. Description

The proposed algorithm, features two encryption layers. The primary layer is the ASCON-128 algorithm, renowned for

its lightweight attributes, symmetric-key foundation and follows Feistel architecture. Second layer is the Dynamic RSA algorithm. Fig. 1 displays the flow of the algorithm. The process begins with the sender sending a plain text. This plain text is first encrypted by ASCON-128 encryption and the resulting cipher text is given as input to Dynamic RSA layer.

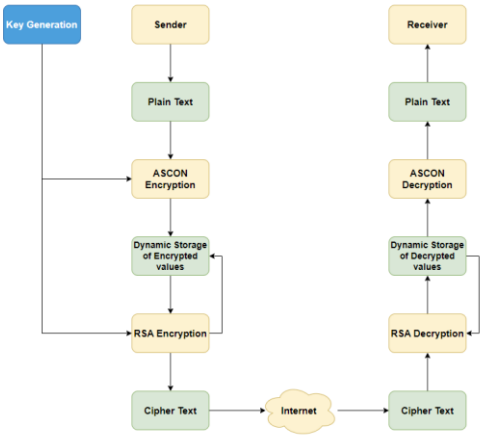

Fig. 1. Block diagram of the proposed hybrid algorithm

The second layer has dynamic properties i.e. it stores the values it is encrypting into a storage. If the same value is encountered again, instead of performing the complex RSA calculation again, the encrypted value is simply substituted from the storage. This saves computational resources while also providing the same output as normal RSA. The result is the required cipher text that has been encrypted in both the layers.

The decryption process also follows a similar approach where new cipher text values are stored and when the same is encountered, it directly extracts the corresponding plain text from the storage.

B. Key Generation Process

Keys are an important component of any cryptographical algorithm. Hence, it is crucial to generate a strong key through techniques such as diffusion and confusion. A strong key makes encryption harder to break, improves security, and makes it less likely for attackers to figure out the key.

Keys corresponding to ASCON is generated with the help of random library in python. Firstly, A random number is generated using this library and a 128-bit key is generated by using a random function. In Addition, We generate a 128-bit nonce before the encryption process takes place.

In RSA key generation, two large prime numbers are chosen randomly. Their product forms the modulus of the RSA key pair. The Euler's totient function is computed, and a public exponent is selected, typically a small prime number. The public key is formed with the modulus and the public exponent. Finally, the private exponent is calculated as the modular multiplicative inverse of the public exponent. The public key is shared, while the private key is kept secret, ensuring secure communication and data integrity.

C. Encryption

In the proposed algorithm, ASCON-128 encryption bit is used for the first level encryption and Dynamic RSA encryption for the second level encryption as the encryption process unfolds in two stages.

1) First Level Encryption (ASCON-128 bit Encryption)

The plaintext message is encoded using ASCON-128 bit encryption algorithm. ASCON encrypts the plaintext message, generating ciphertext which serves as the input for the next encryption stage.

2) Second Level Encryption (Dynamic RSA Encryption)

The ciphertext from the first level encryption is encrypted using Dynamic RSA encryption. RSA's public key, which was dynamically generated for this session, is used for encryption. The RSA encryption process transforms the ASCON encrypted ciphertext into a 2-level encrypted ciphertext, ensuring additional security to the data.

D. Decryption

The two step decryption process has first step being decryption using Dynamic RSA Decryption and then by ASCON-128 Decryption.

1) Second Level Decryption (Dynamic RSA Decryption):

The ciphertext is decrypted using Dynamic RSA algorithm. RSA's private key is used for encryption, is used for decryption. The RSA decryption process converts the encrypted ciphertext back into the original plaintext, recovering the data from the second encryption layer.

2) First Level Decryption (ASCON-128 bit Decryption):

The derived plaintext from the second level decryption is decrypted using ASCON-128 bit decryption algorithm. ASCON decrypts the derived plaintext, recovering the original plaintext message encrypted.

IV. Simulation Environment

The proposed algorithm, aimed at improving data security in data transfer applications, was simulated, and implemented on a Lenovo IdeaPad L340 laptop. Equipped with an Intel Core i5-9300H processor, the laptop provided robust computational power for intensive algorithmic processing. Complementing the processor, the inclusion of a GTX1650 GPU accelerated graphics processing tasks, crucial for image rendering and analysis.

The laptop's 8GB of RAM allowed seamless transitions between algorithm development, testing, and evaluation tasks. Utilizing Python 3.9 within Jupyter Notebook, developers harnessed the versatility of Python's scientific computing libraries, such as NumPy for code execution. The interactive environment of Jupyter Notebook provided a user-friendly interface for iterative algorithm refinement and experimentation.

V. Results And Discussions

Several experiments are conducted to evaluate the proposed algorithm’s quality, compared to traditional lightweight encryption algorithms and symmetric/asymmetric key encryption algorithms. In the following sub-sections, we talk about different parameters considered and how the proposed algorithm performs when in comparison with existing NELC hybrid algorithm, light-weight algorithms, and symmetric/asymmetric algorithms.

A. Execution Time

Another metric to consider for evaluating a cryptographic algorithm is the execution time. The overall time taken to encrypt or decrypt a given piece of data is known as the cryptographic execution time.

Execution time is the algorithm's overall time to complete the execution and the processes. Execution time has two times- encryption and decryption time. Encryption time is the overall time the code takes to convert the original message into the cipher text. Decryption time is the time taken by the algorithm to convert the encrypted message back into the original message. Upon observing Fig. 2, we can find that the proposed algorithm is faster than the existing NELC hybrid algorithm.

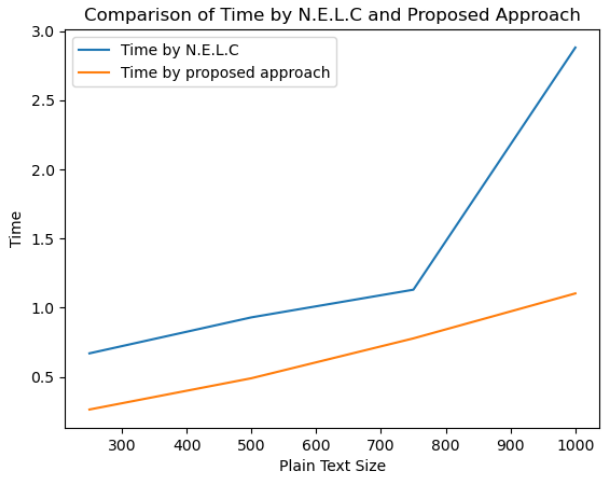

Fig. 2. Execution Time Comparison of proposed algorithm with NELC algorithm

B. Throughput

The throughput rate is used to evaluate the algorithm's efficacy. Throughput is directly proportional to its performance. It means higher the performance, the higher the throughput. The formula for calculating throughput for an algorithm is shown in (1).

Throughput = Plain Text Size/Encoding Time (1)

The throughput comparison of the proposed algorithm with NELC hybrid algorithm is shown in Fig. 3.

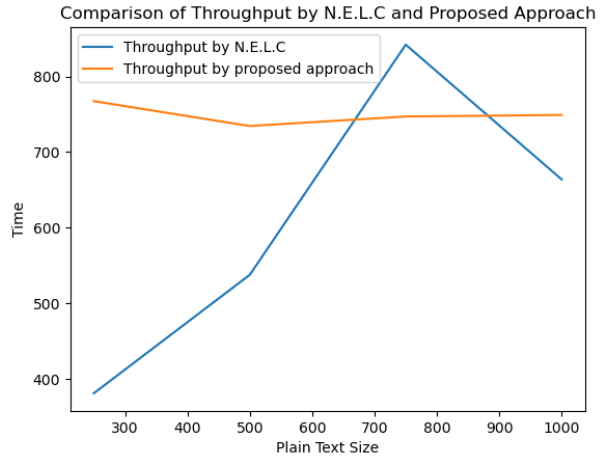

Fig. 3. Throughput Comparison of proposed algorithm with NELC algorithm

C. Delay and Latency

In cryptography, delay and latency play crucial roles in determining the efficiency of an encryption algorithm. Delay implies the time taken for a message to travel from the sender to the receiver, while latency represents the time delay incurred during the processing of the message.

The proposed algorithm's delay and latency characteristics were evaluated through comprehensive testing. Multiple experiments were conducted, varying the input sizes and types of data. Each experiment was repeated five times to ensure statistical reliability. Fig. 4 graphically represents the Delay and Latency of the proposed algorithm.

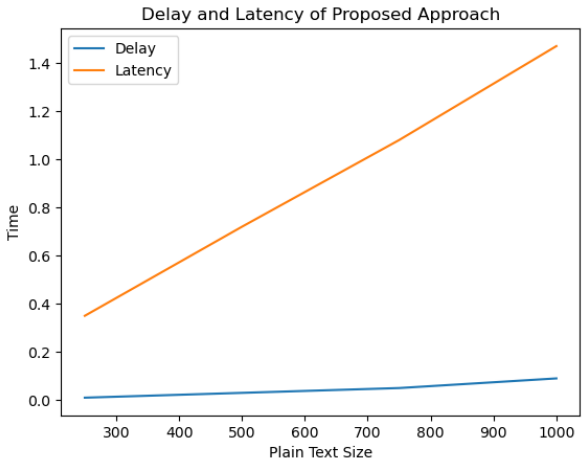

Fig. 4. Delay and Latency of the proposed algorithm

D. Benchmarking proposed algorithm

The algorithm's evaluation is done using text files of different sizes. The experiment is performed five times on each file size and has been tabulated in Table I. It shows the average execution time (in milliseconds) for text files. Table I also presents the average delay and latency values obtained from the experimental tests. It illustrates the delay in message transmission and the latency introduced during the encryption and decryption processes across different file sizes. The results of throughput analysis are shown in Table I.

TABLE I. COMPLEXITY ANALYSIS OF PROPOSED ALGORITHM

Plaintext Size (kB)	Enc Time (s)	Throughput (Kb/s)	Delay (s)	Latency (s)
255	0.32	767.34	0.35	0.01
500	0.68	734.43	0.72	0.03
750	1	747.01	1.08	0.06
1000	1.33	749.06	1.47	0.09
Average	0.83	749.46	0.905	0.04

E. Comparative study of proposed algorithm with traditional symmetric and asymmetric algorithms

The proposed algorithm is compared to traditional symmetric and asymmetric encryption algorithms frequently used for securing information in data sharing scenarios. The comparative study was based on factors such as Structure, Key size, Execution Time, No of Possible Keys, Block Size, Cipher Type and Security strength. These evaluation metrices are shown in Table II.

TABLE II. COMPARATIVE STUDY OF PROPOSED ALGORITHM WITH ASYMMETRIC AND SYMMETRIC ALGORITHMS

	AES [21]	BLOWFISH [22]	SIT [23]	HOMOMORPHIC RSA [24]	HOMOMORPHIC ELGAMAL [24]	PROPOSED ALGORITHM
Structure	SP	Feistel	Feistel + SP	Modular Exponentiation	Modular Exponentiation	SP + Modular Exponentiation
Algorithm	Symmetric	Symmetric	Symmetric	Asymmetric	Asymmetric	Symmetric + Asymmetric
Key size (bits)	128	64	64	Random	Random	128
Block size (bits)	128, 192, 25	32-448	64	512, 1024	512, 1024	128
Key space analysis (bits)	2128, 2192, 2256	232-2448	264	Random	Random	212
Deposit of keys	Yes	Yes	Yes	No	No	Yes
No of round(s)	10, 12, 14	16	5	Random	Random	18
Encryption Process	Moderate	Moderate	Faster	Faster	Moderate	Faster
Decryption Process	Moderate	Moderate	Moderate	Faster	Moderate	Faster
Power consumption	Low	Low	Moderate	High	High	Moderate
Security	Secure	Secure	Secure	Secure	Secure	Moderately Secure

TABLE III. COMPARATIVE STUDY OF PROPOSED ALGORITHM WITH LIGHTWEIGHT ALGORITHMS.

	HIGHT [16]	SEA [17]	LED [18]	RC6 [19]	NLCA [20]	**Proposed Algorithm**
Structure	Feistel	Feistel	Feistel	Feistel	Feistel + SP	**SP**
Layer(s)	1	1	1	1	1	**2**
Block size (bits)	64	48, 96, 144	64, 128	128	128, 256	**128**
Key size (bits)	128	48, 96, 144	64, 128	128. 192, 256	128, 256	**128**
No of Round Possible key(s)	32	Variable	Variable	20	4	**18**
Average time (s)	2.5	4.2	2.9	2.63	1.89	**0.8364**
Security rate	Secure	Secure	Secure	Secure	Secure	**Highly secure**

F. Time Complexity

The proposed algorithm features a 128-bit key size. This mean there are 2^128 possible keys. An attacker using brute-force attacks has to find the right key out of all the possible keys. As a result, the time needed to find the right key is 2^128, which is very large but considered constant on average. In practice, the proposed algorithm is as complex as AES but more efficient because it avoids the repeated steps of each round found in AES and other similar algorithms.

G. Comparative study of the proposed algorithm with light-weight hybrid cryptographic algorithms

The proposed algorithm is put through a comparative analysis with light-weight algorithms. The parameters used for the evaluation are Mathematical Operations, Key Length, Block Size, Execution time, Cipher Type, Possible Key and Security strength. The results are tabulated in Table III.

VI. CONCLUSION

Amidst the growing popularity of remote connectivity and data storage solutions, there is a pressing need for enhanced data security measures. This research introduces a Lightweight Hybrid Cryptographic Algorithm that employs a two-layer encryption approach to improve data security. The first layer utilizes a novel 128-bit lightweight algorithm called ASCON, while the second layer incorporates a modified RSA with dynamic properties to enhance encryption and decryption times. The proposed algorithm shows promise for future applications, offering significantly improved outcomes in various data transfer scenarios and bolstering overall security. Future work can address issues related to storing pre-computed values for dynamic RSA, as improper management or protection of these values could pose a security risk, potentially allowing attackers to exploit them.

Abbreviation	Expansion
RSA	Rivest-Shamir-Adleman
SEA	Scalable Encryption Algorithm
HIGHT	High Security and Light Weight
RC6	Rivest Cipher 6
SIT	Simple Internet Transactions
AES	Advanced Encryption Standard
N.E.L.C	Novel Effective Lightweight Cryptographic algorithm

REFERENCES

[1] Fursan Thabit, Ozgu Can, Sharaf Alhomdy, Ghaleb H. Al-Gaphari, Sudhir Jagtap, A Novel Effective Lightweight Homomorphic Cryptographic Algorithm for data security in cloud computing, International Journal of Intelligent Networks, Volume 3, 2022, Pages 16-30, ISSN 2666-6030, https://doi.org/10.1016/j.ijin.2022.04.001.

[2] Krishnadoss, Pradeep, et al. "Dynamic Approach for Time Reduction in RSA Algorithm through Adaptive Data Encryption and Decryption." *International Journal of Intelligent Engineering & Systems* 17.4 (2024).

[3] Thabit, Fursan, Sharaf Alhomdy, and Sudhir Jagtap. "A new data security algorithm for the cloud computing based on genetics techniques and logical-mathematical functions." *International Journal of Intelligent Networks* 2 (2021): 18-33.

[4] Mohamad, Mohd Saiful Adli, Roshidi Din, and Jasmin Ilyani Ahmad. "Research trends review on RSA scheme of asymmetric cryptography techniques." Bulletin of Electrical Engineering and Informatics 10.1 (2021): 487-492.

[5] Munjal, Kundan, and Rekha Bhatia. "A systematic review of homomorphic encryption and its contributions in healthcare industry." Complex & Intelligent Systems 9.4 (2023): 3759-3786.

[6] Kanthimathi, S., and P. Jhansi Rani. "An efficient packet dropping attack detection mechanism in wireless ad-hoc networks using ECC based AODV-ACO protocol." *Wireless Networks* (2022): 1-13.

[7] Hoobi, Mayes M. "Efficient hybrid cryptography algorithm." Journal of Southwest Jiaotong University 55.3 (2020).

[8] Mohammed, Saja J., and Dujan B. Taha. "Performance evaluation of RSA, ElGamal, and paillier partial homomorphic encryption algorithms." *2022 International Conference on Computer Science and Software Engineering (CSASE)*. IEEE, 2022.

[9] Mubeen, Saad, Elena Lisova, and Aneta Vulgarakis Feljan. "Timing predictability and security in safety-critical industrial cyber-physical systems: A position paper." *Applied Sciences* 10.9 (2020): 3125.

[10] Dobraunig, C., Eichlseder, M., Mendel, F. *et al.* Ascon v1.2: Lightweight Authenticated Encryption and Hashing. *J Cryptol* **34**, 33 (2021). https://doi.org/10.1007/s00145-021-09398-9 [11] Daemen, Joan, et al. "Xoodyak, a lightweight cryptographic scheme." (2020).

[12] Dimitrov, Vassil, Luigi Vigneri, and Vidal Attias. "Fast generation of RSA keys using smooth integers." *IEEE Transactions on Computers* 71.7 (2021): 1575-1585.

[13] Liu, Jun-Jie, Kang-Too Tsang, and Yu-Hui Deng. "A variant RSA acceleration with parallelisation." *International Journal of Parallel, Emergent and Distributed Systems* 37.3 (2022): 318-332.

[14] Lizy, R. Felista Sugirtha. "Improvement of RSA algorithm using euclidean technique." *Turkish Journal of Computer and Mathematics Education (TURCOMAT)* 12.3 (2021): 4694-4700.

[15] Thabit, Fursan, et al. "Exploration of security challenges in cloud computing: Issues, threats, and attacks with their alleviating techniques." *Journal of Information and Computational Science* 12.10 (2020).

[16] Hong, Deukjo, et al. "HIGHT: A new block cipher suitable for low-resource device." *Cryptographic Hardware and Embedded Systems-CHES 2006: 8th International Workshop, Yokohama, Japan, October 10-13, 2006. Proceedings 8*. Springer Berlin Heidelberg, 2006.

[17] Huang, Shih-I., and Shiuhpyng Shieh. "SEA: Secure Encrypted-Data Aggregation in Mobile Wireless Sensor Networks." *2007 International Conference on Computational Intelligence and Security (CIS 2007)*. IEEE, 2007.

[18] Bansod, Gaurav, Nishchal Raval, and Narayan Pisharoty. "Implementation of a new lightweight encryption design for embedded security." *IEEE Transactions on Information Forensics and Security* 10.1 (2014): 142-151.

[19] Rivest, R., et al. "The RC6 Block Cipher. First Adv. Encryption… (1998)."

[20] Thabit, Fursan, et al. "Exploration of security challenges in cloud computing: Issues, threats, and attacks with their alleviating techniques." *Journal of Information and Computational Science* 12.10 (2020).

[21] Wright, Marie A. "The advanced encryption standard." *Network Security* 2001.10 (2001): 11-13.

[22] M.N. Valmik, P.V.K. Kshirsagar, Blowfish algorithm, IOSR J. Comput. Eng. (2014), https://doi.org/10.9790/0661-162108083.

[23] Usman, Muhammad, et al. "SIT: a lightweight encryption algorithm for secure internet of things." *arXiv preprint arXiv:1704.08688* (2017).

[24] Jabbar, Ihsan, and Saad Najim. "Using fully homomorphic encryption to secure cloud computing." *Internet of things and cloud computing* 4.2 (2016): 13-18.