An Overview and Analysis of Hybrid Encryption: The Combination of Symmetric Encryption and Asymmetric Encryption

Qixin Zhang
Computer Science and Engineering
NYU Tandon School of Engineering
New York, America
QZ2067@nyu.edu

2021 2nd International Conference on Computing and Data Science (CDS) | 978-1-6654-0428-0/21/$31.00 ©2021 IEEE | DOI: 10.1109/CDS52072.2021.00111

***Abstract*—In the current scenario, various forms of information are spread everywhere, especially through the Internet. A lot of valuable information is contained in the dissemination, so security issues have always attracted attention. With the emergence of cryptographic algorithms, information security has been further improved. Generally, cryptography encryption is divided into symmetric encryption and asymmetric encryption. Although symmetric encryption has a very fast computation speed and is beneficial to encrypt a large amount of data, the security is not as high as asymmetric encryption. The same pair of keys used in symmetric algorithms leads to security threats. Thus, if the key can be protected, the security could be improved. Using an asymmetric algorithm to protect the key and encrypting the message with a symmetric algorithm would be a good choice. This paper will review security issues in the information transmission and the method of hybrid encryption algorithms that will be widely used in the future. Also, the various characteristics of algorithms in different systems and some typical cases of hybrid encryption will be reviewed and analyzed to showcase the reinforcement by combining algorithms. Hybrid encryption algorithms will improve the security of the transmission without causing more other problems. Additionally, the way how the encryption algorithms combine to strength the security will be discussed with the aid of an example.**

Keywords*—*encryption algorithm, symmetric algorithm, asymmetric algorithm, hybrid encryption

I. Introduction

Nowadays, the amount of uploaded and downloaded data has dramatically increased to an unimaginable level. Data security incidents like information leakage and information tampering are increasingly growing. The huge transfer volume gives the attacker more opportunities to intercept data during transmission. However, if valuable data is intercepted, it can cause serious damage to individuals, companies, and governments. Thus, the protection of information has always been an issue worthy of attention. Effective strategies are necessary to protect data. Among many existing technologies, the data encryption method is a very reliable means of protecting data.

Data encryption is a kind of secret technology that both parties, the sender and receiver, in communication carry out special conversion of information according to agreed rules. According to certain rules, the message will be transferred between the plaintext and the ciphertext. The process from the plaintext to the ciphertext with specified function is called encryption; the process of recovering the original plaintext from the ciphertext by the receiver is called decryption. Encryption algorithms are often used in large amounts of data transmission and storage and they worked well in most cases. They are considered as an effective method to reduce the possibility of data leakage.

Traditionally, there are various encryption algorithms, such as AES, DES, and RSA. Those are very common encryption algorithms. However, any individual encryption algorithm is not strong enough to reduce the chance of being successfully cracked, since any of them has been studied thoroughly and attackers are already familiar with the vulnerabilities of these single algorithms. It makes attackers break easily and just spend a little time. In addition, different encryption algorithms have different focuses. Thus, people tend to use various combinations of several encryption algorithms in diverse fields

978-1-6654-0428-0/21/$31.00 ©2021 IEEE
DOI 10.1109/CDS52072.2021.00111

and applications for distinct needs.

There are many examples of the hybrid encryption method. In these papers, we will discuss the traditional method. This method combines algorithms from two different systems, and it always focuses on the improvement of security against from brute force attack. Dijesh et al. proposed a multi-layer encryption algorithm, consisting RSA and Fernet cipher encryption algorithm, which strengthens the security and efficiency of message delivery especially in electronic commerce [1]. This combination mainly aims at electronic commerce. For the two algorithms, RSA is a secure asymmetric encryption algorithm. Another component, Fernet encryption, is a strong algorithm in a symmetric encryption system. It is much stronger than RSA when there is no requirement for communication. These two encryption algorithms are chosen for higher security in electronic commerce. In another example of combining symmetric and asymmetric algorithms, Vashi et al. advocates the approach of using hybrid strategies [2]. The strategies consist of different symmetric and asymmetric encryption. This cryptographic strategy is used to protect the data in the medical field instead of using one technique to secure one data set. The result was tested with the help of a horizontally partitioned database table. This hybrid encryption method requires fewer pseudo-random numbers and has faster encryption/decryption speed, higher security, and strong system sensitivity.

Based on the combination of symmetric and asymmetric encryption, some adjustments for data integrity are made. Hash algorithms are added for further increasing the difficulty of attacking and ensuring the security of data transmission. Also, with the aid of hash algorithms, it ensures that the transmitted information package has not been broken by an attacker. Harba et al. proposed a method to protect data transferring through hybrid encryption techniques Advanced Encryption Standard, RSA, Hash-based Message Authentication Code (HMAC) to avoid exposure during data transferring [3]. In this paper, we will analyze the improved strength through the combination of three encryption algorithms. This combination makes it harder to be attacked by common methods, and this method also focuses on protecting passwords and credentials rather than only focusing on encryption. Similarly, Timothy et al. proposed a new security method by using a hybrid cryptosystem to solve the data security and privacy issues of cloud computing. This hybrid algorithm includes Blowfish symmetric algorithm, RSA and Secure Hash Algorithm 2 (SHA-2) [4]. This hybrid system will aim at transmission, specially, and it provides a higher difficulty level for unauthorized people or intruders. In the case of similar functions, different authors have proposed different combinations to strengthen a certain aspect. There is another similar example. AbdElnapi et al. combines RSA and AES with SHA256. This hybrid encryption method mainly improves the security of the cloud storage by achieving the integrity through SHA256 signature generation [5]. This combination has a similar function as the previous one, though different algorithms are chosen.

In other ways to be more secure and efficient, Sajay et al. states the importance of security of cloud data and proposes a hybrid encryption algorithm to improve security of cloud data. In this paper, homographic encryption and blowfish encryption are combined. This combination is a typical hybrid encryption, and it shows that a hybrid encryption is more efficient than other individual algorithms [6]. In addition to using traditional approaches to combine symmetric and asymmetric encryption algorithms, an author has a different view, combining two powerful asymmetric algorithms. Kanna et al. proposed a new identity-based hybrid encryption consisting of two asymmetric encryption algorithms, RSA and ECC, to enhance data security [7]. The new encryption system will be used to encrypt sensitive data, and the key will be protected by the proxy re encryption. This method focuses more on efficiency, so this method has higher speed of throughput and higher speed of encryption and decryption. In other ways, there are authors in two papers who did not choose to combine algorithms. They improved encryption algorithms by changing some details.

The combinations of algorithms are not the only choice. Although some algorithms have fatal weaknesses, they are not unsolvable. The weak parts can be modified to make the whole algorithm more difficult to crack. This happened to prove that the single algorithm of the past was no longer secure enough. We will prove that with the help of different cases. These cases show that the modified algorithms perform better than previous ones. Zodpe et al. proposed a new hybrid AES based on traditional AES with the help of the modified S-box. This improved AES was compared with the traditional AES encryption to show the proposed one has better performance, especially on security of data [8]. Its unique dynamic S-box and

initial key generated by PN Sequence Generator makes the algorithm invulnerable to brute force attack, and it also has higher key sensitivity, high throughput and utilizes less area. Lavanya et al. tends to show how the proposed encryption algorithm enhances the overall security. This proposed encryption algorithm is mainly based on AES and improved by small scales variations in the shift row transformation and key expansion unit [9]. This improved AES increases the confusion rate, is more secure, has better balance than AES, and has higher avalanche effect and larger hamming distance.

Due to the disadvantages of existing algorithms, the other authors are not satisfied with those algorithms. They have combined the existing technical characteristics to sum up a new encryption algorithm. For instance, Vuppala et al. proposed a new algorithm, FORTIS algorithm, to make the key more secure while the large key cannot stop the decryption by intruders. This new algorithm is compared with other excellent algorithms that do not encrypt the key generation [10]. According to the results of tests, this new algorithm encrypts the generated sub-key. It helps to avoid side-channel power attacks, and the number of glitches that represent the leakage power are reduced with a similar instruction performance that reduces the probability of being guessed.

All of the above data protection uses different encryption algorithms to secure data by combining or improving existing encryption algorithms. These combinations, improvements, and new algorithms indirectly proved that a single encryption algorithm has hidden safety issues, and those issues need to be cautiously considered. Before making changes, some typical algorithms need to be understood. To study which type of encryption algorithm is more secure or has more advantages in some respects, people need to learn about these common algorithms. In this paper, I will introduce some common encryption algorithms, and compare them to show the characteristics of these systems or algorithms. For example, symmetric encryption algorithms have fast computation speed, while asymmetric encryption algorithms are relatively more secure. Also, some classical hybrid algorithms proposed by other authors and the trend of using hybrid algorithms will be introduced.

The reminder of the paper is organized as follows. Section 2 reviews some typical algorithms from different systems. Then, Section 3 discusses related works and trend, and proposes a hybrid encryption algorithm. Section 4 summarizes the trend of hybrid encryption algorithm and restates the importance of it.

II. Backgrounds

The cryptography system can be divided into two categories: symmetric encryption algorithm and asymmetric encryption algorithm. These two encryption systems have their own characteristics, and they will be applied to distinct situations, according to different encryption and transmission demand and features of the algorithms.

A. Symmetric Encryption Algorithms

Symmetric encryption, also called private key encryption, refers to an encryption algorithm that uses the same key for both encryption and decryption. In the symmetric encryption algorithm, the data sender processes the plaintext, the original data, and the encryption key together with a special encryption and sends it out. After receiving the ciphertext, if the recipient wants to interpret the original text, it needs to decrypt the ciphertext using the used encryption key and inverse algorithm of the same algorithm to restore it to a readable plaintext. Also, in a symmetric encryption algorithm, the same keys are used. Both the sender and the receiver use the same key to encrypt and decrypt data. It requires that the decrypting party must know the secret key in advance.

This kind of encryption algorithms generally include three characteristics:

- It is easy to manage secret keys because the same secret key is used for both encryption and decryption.
- Symmetric encryption algorithms have very high efficiency and diversification, since there are less computation and relatively higher speed of encryption and decryption while processing. It makes it match diverse situations and is suitable for large data.

Specifically, there are some examples: DES, AES, Triple DES

a) Data Encryption Standard (DES) [11]

DES is a block encryption algorithm. Typical DES encrypts data in 64-bit blocks, and the same algorithm is used for both encryption and decryption. DES has high encryption and decryption speed and low resource consumption, but the security is not that high. It is commonly used to encrypt data

that has a large amount.

b) Advanced Encryption Standard (AES) [12]

AES is a symmetric block encryption technology that uses 128-bit blocks to encrypt data and provide higher encryption strength. The encryption table and decryption table of AES are separate, and support subkey encryption. This feature makes it better than some methods of decrypting with a special key. The AES algorithm supports any packet size and the initial time is fast. In particular, its parallelism can effectively utilize processor resources. In other words, high encryption and decryption speed, high security, low consumption and high flexibility are advantages of AES, making it popular in the application of cryptography.

c) Triple Data Encryption Algorithm(3DES)

3DES is a general term for triple data encryption algorithm block cipher. It is equivalent to applying the DES encryption algorithm three times to each data block. Due to the enhancement of computer computing capacity, the key length of the original DES cipher becomes easy to be cracked by brute force. 3DES is designed to provide a relatively simple method, that is, to avoid similar attacks by increasing the key length of DES. 3DES is much more secure than DES, however, it is lower and consumes more than DES, so people could use it to encrypt important and valuable data that has small amounts.

Although there are many advantages of a symmetric encryption system, it is not satisfactory and meets people's needs in some places.

Due to the same secret key used for both the receiver and sender in the transaction, the security cannot be guaranteed. To be more specific, once the secret key is intercepted by an attacker, no matter which party it is intercepted from, the entire transmission process is unsafe. It is because the attacker has already known the secret key that will be used to encrypt and decrypt the message.

Additionally, managing the secret keys is also troublesome. Every time each pair of users uses a symmetric encryption algorithm, they need to use a unique key that others do not know, so they may want to choose a new key for a new transmission. This will increase the number of keys possessed by both sender and receiver to grow exponentially. It makes the key management a burden on users.

Actually, not only is the number of keys difficult to manage, the size of the keys can also cause concerns. Symmetric encryption usually uses a relatively small key, generally less than 256 bits. Because the larger the key is, the stronger the encryption is, but the encryption and decryption would process slower. If you only use 1 bit as the secret key, then attackers can try to use 0 to decrypt it first. If not, then use 1 to solve. However, if the key is 1 MB, attackers may never be able to crack it, but the process of encryption and decryption takes a long time. The size of the key must take care of both security and efficiency, which is a trade-off, and the large size of keys also increases difficulty of key management.

B. Asymmetric Encryption Algorithms

Compared with the shortcomings that the key transmission process is insecure and easy to crack, asymmetric encryption provides a very secure method for data encryption and decryption. This system uses a pair of keys, a public key and a private key. The private key can only be safely kept by one party and cannot be leaked, while the public key can be sent to anyone who requests it. Asymmetric encryption uses the public key for encryption, while decryption requires the private key.

Asymmetric encryption algorithms have features:

- Asymmetric encryption algorithms are more secure and stronger, since attackers could not use the public key to decrypt the message.
- Asymmetric encryption algorithms have another function: digital signature.

Compared with symmetric encryption algorithms, asymmetric encryption algorithms are relatively cumbersome, the process of encryption and decryption takes a long time and is really slow. Thus, it is only suitable for encrypting a small amount of data each time.

RSA, ElGamal encryption, and ECC are some common asymmetric algorithms.

a) RSA [13]

RSA is designed by three mathematicians: Rivest, Shamir, and Adleman. The principle of the RSA public key cryptosystem uses numbers that are relatively prime. It is simple to find two large prime numbers, but it is extremely difficult to factorize their product. Thus, this algorithm is very reliable. The longer the key is, the harder it is to crack. However,

RSA has very low computation speed and high consumption.

b) ElGamal Encryption

ElGamal encryption algorithm is an asymmetric encryption algorithm based on Diffie-Hellman key exchange. It can be defined on any cyclic group G, and its security depends on the discrete logarithm problem on G. ElGamal encryption algorithm consists of three parts: key generation, encryption, and decryption. As an asymmetric cryptography system, ElGamal encryption algorithm is slow. This algorithm is usually used in hybrid systems. Encrypting the secret key by ElGamal algorithm and encrypting the message with symmetric algorithms would make it faster and safer.

c) Elliptic Curve Cryptography (ECC) [14]

ECC is a public key encryption system, based on elliptic curve mathematics. The main advantage of ECC is that in some cases it uses smaller keys than other methods like RSA, and it still provides comparable or higher levels of security. High security is one of its advantages. This algorithm has speed during encryption and decryption, and it requires less storage and broadband. However, compares with RSA, the computation is much more complex, so it makes it difficult in application, though it is much safer.

C. Comparison

They are both powerful encryption algorithms. However, these two kinds of encryption algorithm have different strengths and weaknesses. Symmetric encryption algorithms are more suitable for large-amount data, while asymmetric encryption algorithms are more usually utilized on small-size and more important data. Since the importance and size of data are not always single, people might try to combine the advantages of these two different systems to make a progress on security and efficiency. There is a table below, comparing these two cryptography systems.

TABLE I. DIFFERENT CHARACTERISTICS BETWEEN TWO SYSTEMS

	Symmetric encryption algorithm	**Asymmetric encryption algorithm**
Number of keys	Single secret key	Pair of keys
Category of key	The same two keys	Different two keys
Key management	Simple but not easy	Need digital certificate and reliable their party
speed	Very fast	Slow
security	High	Higher
Application	Encrypt data that has a large amount	Encrypt data that requires high confidentiality

III. DISCUSSION AND TREND OF HYBRID ENCRYPTION

A. Discussion of Hybrid Encryption

Hybrid encryption provides good protection against plaintext attacks and makes encryption stronger [5]. It is the combination of different encryption algorithms. There are various types of combinations. They might be the combination of algorithms from the same system or the algorithms from different systems. In this paper, the traditional type of hybrid encryption would be discussed. It is the combination of symmetric encryption and asymmetric encryption.

As mentioned before, both symmetric encryption and asymmetric encryption have their own advantages and disadvantages. Moreover, the hybrid encryption is more powerful in data protection and meets some operational processes or space requirements like computation speed and memory occupied by secret keys. Therefore, their special features can be used for diverse demands like the high demands of security. However, an individual encryption algorithm can no longer meet the needs of various aspects.

Hybrid encryption would be a good solution. The combination of strong algorithms increases the difficulty level of being decoded by intruders or some attacks like brute force attack. Also, it not only takes advantages from both two encryption systems, but also avoids their disadvantages. The combination of a symmetric algorithm and an asymmetric algorithm would be a typical case.

Using a symmetric algorithm to encrypt data can improve efficiency. However, the security of symmetric algorithms is slightly weaker than that of asymmetric algorithms. This problem is caused by the same key that will be used for encryption and decryption. If one part's key is exposed, it will directly lead to data disclosure because the attacker could recover the message with this key. So, if this problem can be solved, then this symmetric algorithm will be much more reliable than before.

Using asymmetric algorithms to encrypt the secret keys might be a great strategy. In general, although processing the

public key would take some time, encrypting the key with asymmetric encryption is much faster than encrypting a long message with it. Then, the secret keys are safer than before. Thus, the whole encryption benefits from the high speed of symmetric encryption and the high security of asymmetric encryption. Consequently, the data security will be improved a lot, and the computation time will not increase too much.

B. The Trend of Hybrid Encryption

There are some traditional methods about combining different encryption algorithms. Also, they are combined to achieve various goals.

In the paper [7], the author proposed a hybrid encryption algorithm, combining RSA and ECC. This is a combination of two asymmetric encryption algorithms to enhance the data security efficiency in cloud computing. The author compares this proposed hybrid algorithm with some identity-based encryption method through the test results. The result after the tests shows that it is more efficient, has higher speed of throughput, and has higher speed of encryption and decryption. Similarly, in the paper [6], the author combined homographic encryption and Blowfish encryption. Compared with some existing individual algorithms, this hybrid encryption behaves very well. The result shows it is more secure and efficient than other individual encryption algorithms, such as AES, DES, RSA, and MD5, and it performs better on storage.

In order to achieve other demands while encrypting, some special algorithms are chosen in the hybrid encryption method. In the paper [5], the hybrid encryption not only combines two algorithms. It adds hashing function to achieve a particular goal. It combines RSA and AES with SHA256 to improve the security of cloud storage. According to the test consequence, the proposed combination uses the strengthening of the asymmetric encryption and the speed of the symmetric encryption. At the same time, SHA256 generates signatures, achieving the integrity to improve the level of security in cloud data storage. To avoid data exposure, in the paper [3], the author came up with a combination of AES, RSA, and HMAC. The goal is to prevent data from disclosure. The combination of AES and RSA improves data security. Also, with the aid of HMAC, passwords and credentials are well protected.

C. Future Encryption

Both symmetric encryption algorithm and asymmetric encryption algorithm are powerful algorithms to protect data. Symmetric encryption algorithms can process faster, so they are usually chosen to encrypt data with large amounts. There is a specific example that chooses two algorithms to combine. The combination of ECC and AES might be a strong and efficient hybrid algorithm. Some typical algorithms from each system are compared in two tables below [15].

TABLE II. STRENGTH COMPARISON BETWEEN 3DES AND AES

Algorithm	Length of key	Strength
3DES-2	112	80~112
3DES-3	168	112
AES-128	128	128
AES-192	192	192
AES-256	256	256

It looks that AES is stronger when the key length is about the same, so AES is chosen as a part of the hybrid algorithm in this case. From other perspectives, AES has low demands for memory, and it supports variable packet length and key length. The packet length can be set to any multiple of 32 bits with a minimum of 128 bits and maximum of 256 bits. Also, the key length of AES is larger than that of DES. It can also be set to any multiple of 32 bits. The minimum value is 128 bits and the maximum value is 256 bits, so it is impossible to crack by exhaustive methods. All of those flexible designs make AES suitable for restricted and diverse environments. Moreover, it has good resistance to differential cryptanalysis and linear cryptanalysis.

Encrypting the public key of a symmetric algorithm will be a good method. In order to better protect the public key, a higher security level would be needed. So, an asymmetric algorithm is supposed to be chosen to protect the key from being leaked.

TABLE III. STRENGTH COMPARISON BETWEEN ECC AND RSA WITH DIFFERENT KEY LENGTH

Length of Key		Strength
ECC	***RSA***	
112	512	56
160	1024	80
224	2048	112
256	3072	128
384	7680	192
512	15360	256

After comparing the key length and the strength of RSA and ECC, it seems that ECC is more reliable with shorter key. Also, in this system, ECC would be more efficient than others, from a personal perspective. As stated before, the mathematical theory of the ECC algorithm is very profound and complicated, and it is difficult to implement in engineering applications, but its unit security strength is relatively high. Its deciphering or solving difficulty is basically exponential, and it is difficult for hackers to use the usual brute force to crack. One of the characteristics of the RSA algorithm is that its mathematical principles are relatively simple and easy to implement, but its strength is relatively low at the same time. Therefore, the ECC algorithm can provide a higher security strength than the RSA algorithm with less computing power. In addition, they key length of the ECC encryption algorithm is very short, which means that it takes up less storage space, lower CPU overhead and takes up less bandwidth than RSA. Thus, ECC could be chosen to encrypt the public key of AES algorithm in this paper.

This hybrid encryption algorithm consists of AES and ECC. AES algorithm will be used to encrypt the original message, while ECC algorithm will encrypt the public key of AES. This way could make effectively protection the public keys used by the sender and the receiver during data transmission. According to the features of these two algorithms, two parties could process the message fast. Moreover, ECC as an asymmetric algorithm has high level of security, and it is also faster and has less consumption than RSA. It makes ECC a better choice in asymmetric system.

IV. Conclusion

After reviewing and comparing some classical algorithms, we deduce that symmetric encryption is not as secure as asymmetric, while the computation speed of asymmetric encryption is not as fast as the former. However, in the current situation, the use of individual algorithms is not sufficient to ensure information security and efficiency. Then we propose hybrid encryption as a solution for the encryption algorithm in this paper. At the same time, some symbolic combination of algorithms is reviewed to show the strength of hybrid encryption algorithms. When the two are combined, the security of the information is strengthened without amplifying the disadvantages too much. Using asymmetric algorithms to protect the key of a symmetric algorithm could make the data safer, and it did not cause much more time. Also, combining existing algorithms could meet the special needs of the users. Through the comparison tables and the way of combination, hybrid encryption algorithms are relatively safer than a simple encryption algorithm. Thus, although hybrid encryption needs to be proven by more examples in various applications, hybrid encryption algorithms are a great strategy as a method of information protection. Among the many hybrid encryption algorithms, the combination of ECC and AES is a good example to strengthen the information security without increasing the burden of computation.

References

[1] D. P., S. S. Babu, and Y. Vijayalakshmi, "Enhancement of e-commerce security through asymmetric key algorithm," *Comput. Commun.*, vol. 153, no. January, pp. 125–134, 2020, doi: 10.1016/j.comcom.2020.01.033.

[2] D. Vashi, H. B. Bhadka, K. Patel, and S. Garg, "An Efficient Hybrid Approach of Attribute Based Encryption for Privacy Preserving Through Horizontally Partitioned Data," *Procedia Comput. Sci.*, vol. 167, no. 2019, pp. 2437–2444, 2020, doi: 10.1016/j.procs.2020.03.296.

[3] E. Salim and I. Harba, "www.etasr.com Harba: Secure Data Encryption Through a Combination of AES," *Technol. Appl. Sci. Res.*, vol. 7, no. 4, pp. 1781–1785, 2017, [Online]. Available: www.etasr.com.

[4] D. P. Timothy and A. K. Santra, "A hybrid cryptography algorithm for cloud computing security," *2017 Int. Conf. Microelectron. Devices, Circuits Syst. ICMDCS 2017*, vol. 2017-Janua, pp. 1–5, 2017, doi: 10.1109/ICMDCS.2017.8211728.

[5] N. M. M. AbdElnapi, F. A. Omara, and N. F. Omran, "A Hybrid Hashing Security Algorithm for Data Storage on Cloud Computing," *Int. J. Comput. Sci. Inf. Secur.*, vol. 14, no. 4, pp. 175–181, 2016, doi: 10.13140/RG.2.1.4103.3844.

[6] K. R. Sajay, S. S. Babu, and Y. Vijayalakshmi, "Enhancing the security of cloud data using hybrid encryption algorithm," *J. Ambient Intell. Humaniz. Comput.*, no. 2018, 2019, doi: 10.1007/s12652-019-01403-1.

[7] G. P. Kanna and V. Vasudevan, "Enhancing the security of user data using the keyword encryption and hybrid cryptographic algorithm in cloud," *Int. Conf. Electr. Electron. Optim. Tech. ICEEOT 2016*, pp. 3688–3693, 2016, doi: 10.1109/ICEEOT.2016.7755398.

[8] H. Zodpe and A. Sapkal, "An efficient AES implementation using FPGA with enhanced security features," *J. King Saud Univ. - Eng. Sci.*, vol. 32, no. 2, pp. 115–122, 2020, doi: 10.1016/j.jksues.2018.07.002.

[9] L. R and K. M, "Enhancing the security of AES through small scale confusion operations for data communication," *Microprocess. Microsyst.*, vol. 75, 2020, doi: 10.1016/j.micpro.2020.103041.

[10] A. Vuppala, R. S. Roshan, S. Nawaz, and J. V. R. Ravindra, "An Efficient Optimization and Secured Triple Data Encryption Standard Using Enhanced Key Scheduling Algorithm," *Procedia Comput. Sci.*, vol. 171, no. 2019, pp. 1054–1063, 2020, doi: 10.1016/j.procs.2020.04.113.

[11] Dey, S. Kumar and T. Nandy. A Symmetric Key Cryptographic Algorithm.

[12] M.G. Kumar,, A Survey on Current Key Issues and Status in Cryptography, (2016).

[13] R. L. Rivest, A. Shamir, and L. M. Adleman, "A method for obtaining digital signatures and public key cryptosystems," *Secur. Commun. Asymmetric Cryptosystems*, pp. 217–239, 2019.

[14] A. H. Koblitz, N. Koblitz, and A. Menezes, "Elliptic curve cryptography: The serpentine course of a paradigm shift," *J. Number Theory*, vol. 131, no. 5, pp. 781–814, 2011, doi: 10.1016/j.jnt.2009.01.006.

[15] E. Barker, "Recommendation for Key Management – Part 1: General," *NIST Spec. Publ. 800-57*, no. May, pp. 1–142, 2016, [Online]. Available: http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-57pt1r4.