International Journal of Environmental Sciences
ISSN: 2229-7359
Vol. 11 No. 8, 2025
https://theaspd.com/index.php

Comprehensive Survey of the Cryptographic Framework for Data Security Using Graph Theory Protocol

NVSS. Prabhakar[1], Talari Surendra[2*], R. Hari Kishore[3], K. Chittibabu[4]
[1,2]Department of Mathematics & Statistics, GSS, GITAM Deemed to be University, Visakhapatnam – Andhra Pradesh, India, prabhakar.nedunuri@gmail.com & surendrabw.t@gmail.com
[3]Assistant Professor, Department of Mathematics, Vasavi College of Engineering, Ibrahimbagh, Hyderabad, Telangana – 500 031, India. kishore.rh6@gmail.com
[4]Lecturer in Mathematics, Govt. Degree College, Mummidivaram- 533216, Dr.B.R.Ambedkar Konaseema District, A.P., India. kchittibabu@gmail.com
Corresponding author: surendrabw.t@gmail.com

Abstract
In the modern digital world, ensuring the confidentiality, authenticity, and integrity of sensitive data has become increasingly critical due to the growing prevalence of cyberattacks and privacy breaches. Traditional cryptosystems face mounting challenges from both advanced classical computing and emerging quantum computing capabilities, which threaten to compromise existing encryption frameworks [11]. To address these concerns, this paper presents a series of advanced cryptographic models incorporating graph theory, identity-based encryption. The proposed systems aim to enhance the security, efficiency, and resilience of digital data protection systems.
Keywords- *Encryption, Cryptographic models, graph theory, Edwards curves, Certificateless public key encryption, Lattice-based techniques.*

INTRODUCTION TO DATA SECURITY

Data security is all about keeping digital information safe from unauthorized access, corruption, theft, or loss at every stage of its lifecycle [19]. In our current digital age, where so much sensitive data is stored and sent electronically, making sure that data is secure has become incredibly important [1].

The need for strong data security measures comes from various potential threats we face today [21]. These threats can range from the physical theft of devices and hardware failures to natural disasters and cyber-attacks like hacking, phishing, and malware. Each of these situations carries the risk of data loss or compromise, highlighting just how crucial it is to have thorough security strategies in place [7].

At the heart of data security are the key principles of confidentiality, integrity, and availability—often referred to as the CIA triad [23]. Confidentiality means that only authorized individuals can access certain information, keeping it safe from unauthorized disclosure [13]. Integrity focuses on ensuring that data remains accurate and complete, so it isn't changed during storage or transmission. Finally, availability makes sure that authorized users can reliably access the information whenever they need it.

Beyond the basics of the CIA triad, concepts like accountability and non-repudiation are also really important. Accountability helps us trace actions related to data back to the individuals responsible, making it easier to perform audits and ensure compliance. Non-repudiation gives us the reassurance that someone can't later deny having signed a document or sent a message, which is crucial for maintaining legal and transactional trust [2].

To really implement strong data security measures, organizations need to blend both technical and administrative controls. On the technical side, this includes tools like encryption, firewalls, intrusion detection systems, and access controls, all aimed at keeping data safe from unauthorized access and cyber threats. On the administrative side, it involves creating policies, procedures, and training programs that steer organizational behavior and help ensure everyone follows security protocols.

To sum up, data security is an intricate field that's crucial for keeping information safe in our ever-more digital landscape. By following fundamental principles and putting in place robust security strategies, organizations can protect their data from a wide range of threats, making sure it stays confidential, intact, and accessible.

The first study introduces a novel cryptographic method based on Crypto Bipartite Graph Theory (CBGT) integrated with a Modified Diffie–Hellman (m-DH) key exchange algorithm. This system secures communication by leveraging the structural characteristics of bipartite graphs, where the encryption keys are selected using an improved Teacher Learning Based Optimization (iTLBO) technique. This approach improves encryption robustness without sacrificing decryption efficiency. Data is then exchanged securely

using the enhanced m-DH algorithm, which incorporates Euler's coefficient and modulo inverse for private key generation. Simulation results demonstrated that this proposed system significantly outperforms traditional methods such as DES, AES, Blowfish, and RSA, particularly in encryption and decryption time, throughput, and execution efficiency.

1.2 Data Security Techniques

These days, data security is essential. Online attacks are growing in number in tandem with the expansion of online transactions. Certain strategies are developed to safeguard data transmission in order to prevent hacking or unwanted access. These methods are:

1) Cryptography

Some consider cryptography a science of protecting information through conversion into an unreadable format, which assures that only the authorized parties would have access to contents in original form [10]. The conversion process consists of:

- **Encryption:** Encryption refers to algorithms and keys that switch plain text (unencrypted data, or an unencrypted file) into unreadable form (ciphertext).
- **Decryption:** Reverting ciphertext back to plaintext using corresponding keys.

Cryptography plays a critical role in safeguarding data confidentiality, integrity, and authenticity. It automatically associates with different security protocols, such as SSL or TLS, for secure web communications and end-to-end encryption for messaging applications.

2) Steganography

Steganography entails hiding a message or file or image inside another medium such that no one would suspect the existence of the hidden message. While cryptography is intended to obscure the content of a message, steganography serves to hide the very existence of the message. Well-known techniques comprise embedding text into an image or audio file by altering insignificant bits, making detection very difficult without analytical tools. More often than not, this technique is combined with cryptography, thereby providing an additional level of security.

3) Digital Watermarking

Digital watermarking is the procedure of embedding a unique identifier or code into digital content of any kind, such as pictures, sound, or video, to claim ownership, authenticate, or track distribution [5]. These watermarks may either be:

- **Visible:** Clearly noticeable marks, like logos or text overlays.
- **Invisible:** Embedded within the content in a manner imperceptible to human senses but detectable by specialized software.

Digital watermarking represents a copyright protection measure, a means of forensic tracking, and verification of integrity of digital media. This prevents unauthorized copying and distribution, thus making it possible for concerned content creators or rights holders to exercise some control over their intellectual properties.

1.3. Cryptography

The fundamental premise of a cryptography system is to encode data or information so that an unauthorized person cannot fully comprehend its meaning and the information is kept confidential. Using cryptography to send data over an unprotected channel, like the internet, or making sure that unauthorized users cannot decipher what they are viewing in the event that they have obtained the data are two of its most popular applications.

The process of hiding the plaintext is called "encryption," and the encrypted plaintext is called "ciphertext." In cryptography, the hidden information is typically referred to as "plaintext." A collection of guidelines referred to as "encryption algorithms" carry out this operation. An "encryption key," which is supplied to the encryption algorithm as input along with the data, is typically used in the encryption process. With the right "decryption key," the receiving party can recover the data using a "decryption algorithm".

1.3.1. Types of Cryptography

Cryptography was initially done by hand using manual methods. Although the implementation was improved in the early days, the fundamental architecture remained mostly unchanged. Nowadays, as everything is dependent on technology and computers, cryptography is likewise done via computers to protect our data. Symmetric key [6] cryptography and asymmetric key cryptography are two methods of

using computers to carry out operations and algorithms [8,9]. Basically, there are two kinds of cryptography depending on how the system performs encryption and decryption [4]:

- Symmetric Key Cryptography
- Asymmetric Key Cryptography

1.3.2. Symmetric Key Cryptography

Another name for symmetric key cryptography is shared key or secret-key cryptography. Both the sender and the recipient use the same key for encryption and decryption in this kind of system. The key is self-certified, which is in accordance with the self-certification procedure. It is necessary to communicate the key in secret. The attacker can quickly decipher the encrypted message if it is compromised. Because it offers speedier service while consuming fewer resources, this kind of encryption approach is necessary. To date, symmetric key cryptography has been described by a number of different algorithms. These include Blowfish, DES, 3DES, and AES.

1.3.3. Asymmetric Key Cryptography

With this process, we will encrypt it using the public key of the recipient, but decrypt it through the private key belonging to the recipient [3,15]. This feature denotes the use of digital signatures to certify the keys rather than the self-certification approach. Thus, this secure system provides superior authentication with better practicality when privacy is maintained. Encryption like this can be done through various methods of doing so, including the Digital Signature Algorithm, Diffie-Hellman, ECC, and RSA.

1.3.4. Modern Cryptography Concepts

In a nutshell, modern cryptography will be the science behind secure digital communications, such as privacy, data integrity, authentication, and non-repudiation mechanisms [16]. It is actually the opposite of classical cryptography, which only used simple substitution and transposition techniques, going as far as specifying mathematically complex public key mechanisms and digital certificates to keep information exchanges safe over open and untrusted networks. In addition to envelopes that also define other protocols and standards for securing data in real time, sensitive environments like financial systems, health care, e-governance, and cloud systems include many others. Public Key Infrastructure (PKI) within Certificateless Public-key Cryptography, each proposes resolutions on several issues, such as key management and identity assurance, in distributed systems [22].

1.3.5. Known-Plaintext Attack

In a Known-Plaintext Attack (KPA), the attacker has at least one pair: plaintext and corresponding ciphertext. Then by analyzing these known pairs, the attacker will try to get hold of the encryption key or predict how other plaintext messages would be encrypted, compromising future communications.

1.3.5 Chosen-Plaintext Attack

In a Chosen-Plaintext Attack (CPA), the attacker can select arbitrary plaintexts and obtain their corresponding ciphertexts under an unknown key. This access allows the attacker to study the encryption process and potentially deduce the secret key or find patterns that lead to partial or full decryption of other messages.

1.3.6 Man-in-the-Middle Attack

A Man-in-the-Middle (MITM) Attack involves an adversary secretly intercepting and possibly altering communication between two parties without their knowledge. The attacker can eavesdrop, modify, or inject false messages, making it seem as though the two legitimate parties are communicating securely when, in reality, the attacker controls the conversation.

1.3.7 Side-Channel Attack

A Side-Channel Attack exploits physical or implementation-related information leaked during the encryption or decryption process, such as timing information, power consumption, electromagnetic emissions, or even sound. By analyzing these side effects, attackers can infer secret keys or sensitive data without directly breaking the cryptographic algorithm itself.

1.3.8 Brute Force Attack

A Brute Force Attack involves systematically trying every possible key combination until the correct one is found. While it guarantees success if enough time and computational power are available, strong encryption algorithms with sufficiently large key spaces make brute-force attempts computationally infeasible in practice.

1.4. Existing Public Key Cryptosystems and Limitations

Public key cryptosystems form the backbone of modern secure communications, enabling key exchange, digital signatures, and secure encryption. Many existing cryptosystems are broadly accepted, yet each one has limitations in security, efficiency, and resistance to newer quantum threats. The main systems are:

1.4.1 RSA-Based Cryptosystems

RSA (Rivest–Shamir–Adleman) is one of the earliest and most widely used public key algorithms. It relies on the computational difficulty of factoring large composite numbers. RSA supports encryption, digital signatures, and secure key exchange. However, it requires large key sizes (2048 bits or more) for adequate security, leading to slower performance. Additionally, RSA is highly vulnerable to quantum attacks using Shor's algorithm.

1.4.2 Elliptic Curve Cryptography

Elliptic Curve Cryptography (ECC) is a more efficient replacement for the RSA processor, since it achieves almost similar security with smaller key sizes. The complexity of the elliptic curve discrete logarithm problem (ECDLP) is how ECC got its name. Wire communication issues, particularly internet applications, mobile devices, and IoT, commonly favor ECC. All the same, it would not perform well in a quantum environment while ECC has demonstrated excellent performance. Side-channel attacks can still exploit implementation errors [17, 24].

1.4.3 Lattice-Based Cryptography

It uses the intractability of lattice problems like the shortest vector problem to build encryption and signature schemes. Among the post-quantum families of encryption, it is considered the strongest because of its robustness against classical as well as quantum adversaries. However, typical lattice schemes suffer from larger ciphertext and key sizes, which affect performance as well as storage efficiency.

1.4.4 Limitations in Existing Approaches

Most cryptosystems currently in operation have proven strong against threats from traditional computing, but they often suffer from limitations concerning scalability and efficiency, disadvantage them in terms of quantum resilience. RSA and ECC can both be broken by quantum algorithms such as Shor's, whereas lattice-based schemes are quantum-safe but have some associated costs in terms of larger keys and higher computational complexity. Key management, secure implementations, and protection against side-channel attacks continue to haunt public key infrastructures as one of the biggest challenges.

1.5. Motivation for the Study

This essay traces the growth of information assurance. During the present digital age, the spiraling usage of digital media in terms of text, image, audio, and video has tremendously increased worries about the security of sensitive information in transit across open, unsecured networks worldwide or the Internet. The unauthorized access, theft, and manipulation risks seem to be continually mounting, and thus there is a need for the development of highly robust and secure communication frameworks. Cryptographic techniques have stood for long as the base for protecting the confidentiality and integrity of data as well as privacy in enabling secure message exchanges using encryption keys. In fact, encryption in attaining or making data secure has always been a basic requirement across numerous applications in real life, including financial services applications, health or healthcare applications, military communication applications, and those applications based on cloud infrastructures.

Nonetheless, conventional identity authentication methods have mostly depended upon certificate-based infrastructures that complicate operations, adding possible security weaknesses and limitations to scalability. Cryptographic systems must now prove resilient against quantum-capable adversaries; hence the need has been most critical.

1.5.1. Contributions of the Proposed Schemes

The key contribution of this study is the design of a novel encryption scheme that synergistically combines graph-theoretic encryption strategies with evolutionary optimization for key selection and an enhanced key exchange protocol, resulting in a highly secure, efficient, and scalable cryptographic system suitable for safeguarding sensitive digital data against emerging security threats.

1.6 Summary

This chapter effectively introduces data security. The significance of data security in defining the modern digital architecture systems is brought out with respect to the role that data security plays in safeguarding sensitive information. Fundamental data security principles, which include confidentiality, integrity, availability, authentication, and non-repudiation, are discussed alongside threats that targets the information, such as ciphertext-only, brute-force, and side-channel attacks. It also addresses traditional and contemporary data protection mechanisms like cryptography and steganography plus some digital watermarks, focusing on cryptography, which is described in two broad approaches: symmetric and asymmetric schemes with public key infrastructures, moving next to advanced paradigms such as Isogeny-based cryptography and DNA-based identity encryption. Furthermore, it identified the limitations of widely used cryptosystems like RSA, ECC, and lattice-based cryptography against modern and quantum threats. To overcome these challenges, the proposed research integrating Isogeny-based Edwards curves, DNA-based identity encryption, and a tri-level certificateless handshake mechanism was introduced, along with its motivation, objectives, contributions, and the overall structure of the thesis. Building on this foundation, the next chapter conducts an extensive literature survey, critically analyzing existing models, identifying their strengths and limitations, and pinpointing research gaps to justify the relevance and novelty of the proposed encryption framework.

2. LITERATURE

2.1. Overview

Cyber warfare encryption techniques are the most important of the several data security techniques developed to counter the increasing threats of cyber-attacks. By converting plaintext into ciphertext and limiting access to the data to those who are authorized to interact with or change it, it safeguards sensitive information. Since Claude Shannon's groundbreaking research in 1949, cryptography has made significant strides. These methods consist of hash functions, symmetric cryptography, and asymmetric cryptography. A single key is used for both encryption and decryption in symmetric cryptography. Code-based cryptography has been increasingly understood by researchers through examinations of current advances that demonstrate its important usage in encryption, identity, and signature systems. Research acknowledges the value of code-based cryptography in digital signatures, encryption, and decryption. Hash-based encryption, which is frequently used in signature systems, is being thoroughly investigated for post-quantum security due to the intrinsic immutability of hash functions. The document provides a description of various hash-based signature schemes, potential ways to improve existing ones, and their many advances.

2.2 Related Works based on Cryptography and Computer Security

This section presents the current methodologies surrounding data security in a data sharing environment and their pros and cons as follows:

Poriye, Monika, and Shuchita Upadhyaya. (2023), had focused on introducing a security framework that included a DNA congruent technique for securing data being transmitted by sensor nodes in a wireless sensor network (WSN). The encryption and decryption of a WSN's data by two nodes was part of this process. Their DNA congruence enabled similar processes such as with DNA encoded information and functionality [14]. The framework included also data compression taking into account the limitations of WSNs. The actual data was hybridized with fake data to enhance security with respect to data sharing.

Kavitha, S., et al. (2024), had showed they have analyzed an encryption scheme involving Gaussian Graceful labeling and an Nth degree truncated polynomial ring unit (NTRU). Through this technique, the vertices of a graph were given unique labels, producing a series of Gaussian integers. The NTRU technique provides effective key exchange and increased security. Integers P, a, and b were necessary for the communication encryption procedure, where P was the greatest prime number in the vertex labeling. All other recipients receive messages from the sender, but the original recipients were the vertex labels with the biggest prime number coefficient. NTRU encryption and decryption employ clustering method

based on abecedarian probability scheme and a polynomial algebraic mixing scheme. The creation of polynomial rings used for decryption and encryption in NTRU was influenced by the selection of relatively prime numbers p and q, with particular selections and characteristics intended to guarantee scheme security.

Roy, Animesh, et al. (2025), had utilized Henon Logistic Crossed Couple Map (HLCML) in conjunction with federated learning and chaos-based encryption to improve security of medical photographs that were kept on cloud servers. The encryption approach was non-interactive, employs weighted parameters in every aggregation step, and provides robust privacy protection through the use of semi-synchronous and differential privacy mechanisms. It was based on chaos-based algorithms. Numerous simulations show how resilient the algorithm was to different challenges, with a noise multiplier of ϵ = 0.25 providing robust privacy protection and 85% convergence in privacy improved FL rounds with 100 communication rounds. The framework's average accuracy on noni.i.d. Medical datasets was 94.3% while using MobileNetV2 CNN. The HLCML-based encryption reduces computational cost to 0.0143 seconds each round while safeguarding weight parameters and preventing potential data leaks. Medical data security had advanced significantly as a result of theoretical and empirical findings that support potential to improve privacy for healthcare organizations and provide robust performance in non-i.i.d. situations.

2.3 Research Gap

The analysis indicates that, following an extensive review of the literature from numerous research articles, the weaknesses in the earlier studies are identified. Data transmission is less secure when symmetric key-based data encryption is used since the secret key could be easily found [12]. Consequently, a system's overall security will be jeopardized. Integrity, confidentiality, and verification issues cannot all be resolved simultaneously using the conventional cryptographic approach. The literature pays insufficient attention to the efficacy of important management practices, which are crucial for maintaining security in practical deployments. Furthermore, not enough study has been done to determine how resistant current cryptographic techniques are to novel assaults. Public-key encryption offered both data encryption and private search capabilities in the cryptosystem area. Traditional schemes, however, were susceptible to internal attacks.

3. Proposed approach

3.1 Overview

Sharing private information through an unprotected channel increases the risk of privacy violations because the data can be stolen by unauthorized parties. Thus, creating a cryptosystem that guarantees the security requirements for integrity, confidentiality, and validity of transmitted data is both required and unavoidable. To ensure data integrity during user-to-user communication, this research suggests a novel graph-based cryptosystem. In this proposed work, the data is secured using a method called crypto bipartite graph theory (CBGT). These innovations exploit the unique properties of bipartite graphs to strengthen communication security. However, the CBGT might be vulnerable to cryptographic attacks due to the random selection of keys, thus threatening security. In this system, the key is defined as a collection of edges connecting vertices from two different groups. To ensure a secure and optimal selection of these edges, we employ an improved teacher learning-based optimization technique (iTLBO) designed to elevate encryption security without compromising the efficacy of decryption. Furthermore, the key exchange relies on a modified Diffie-Hellman (m-DH) algorithm that achieves enhanced security by leveraging Euler's coefficient and the modulo inverse, both of which serve to modify how private keys are generated. In many respects, this newly proposed method has been shown by experiments to be far better than the traditional techniques such as AES, Blowfish, Rivest–Shamir–Adleman (RSA), and Data Encryption Standard (DES) in the decryption time, encryption time, throughput, and overall execution time. The simulations for the study using Python were performed.

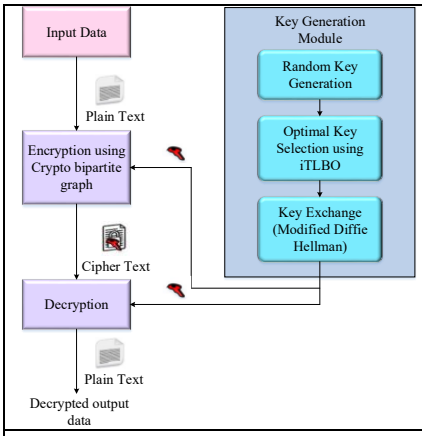


Figure 3.1: Proposed scheme model

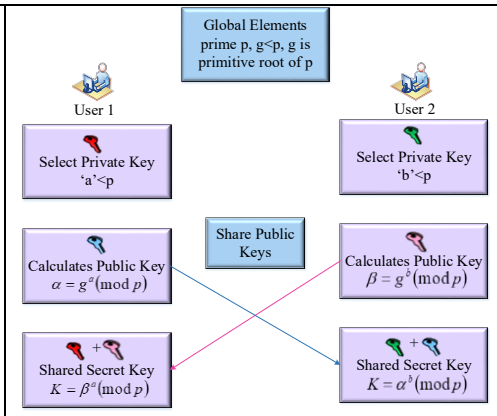


Figure 3.2: Key exchange procedure

3.2 Key Exchange Using the Modified Diffie–Hellman Algorithm (m-DH)

Algorithm 1: m-DH key exchange

Begin

Randomly Generate Large prime numbers p, q, Y and g

$0 < g < p, 0 < g < q, p \neq q \text{ and } g < Y$

Here 'p' and 'q' are large and unique prime numbers that are than base than the base generator value g.

Note:

'p' and 'g': secret and known for User I and User 2.

X and g are global components.

Calculate n and $\phi(n)$

$n = p \times q$

$\phi(n) = (p-1) \times (q-1)$

Generate a random co-prime 'e' for the public key. User 1 and User 2 concur that the co-primes are: $(\phi(n) > e), (\phi(n), e > 1)$.

User 1's actions

Chooses $a < Y$

Calculates $d_1 = e^{-1} (\text{mod}\, \varphi(n))$

Calculates Public key $\alpha = g^a (\text{mod}\, Y)$

Public key encryption of α

$C_1 = \alpha^e (\text{mod}\, n)$

Decrypting received message $\beta = R_t = C_2 d_1 (\text{mod}\, n)$

Secret key calculation

$K_1 = \beta^a (\text{mod}\, Y) = g^{ba} (\text{mod}\, Y)$

User 2's actions

Chooses $b < Y$

Calculates $d_2 = e^{-1} (\text{mod}\, \varphi(n))$

Calculates Public key $\beta = g^b (\text{mod}\, Y)$

Public key encryption of β

$C_2 = \beta^e (\text{mod}\, n)$

Decrypting received message $\alpha = R_2 = C_1 d_2 (\text{mod}\, n)$

Secret key calculation $K_2 = \alpha^b (\text{mod}\, Y) = g^{ab} (\text{mod}\, Y)$

$K_1 = g^{ba} (\text{mod } Y) = g^{ab} (\text{mod } Y) = K_2 = K$, which is secret key shared between the users

End

The suggested model's total process flow, including key creation, data encryption, key exchange, and decryption, is depicted in Figure 3.3.

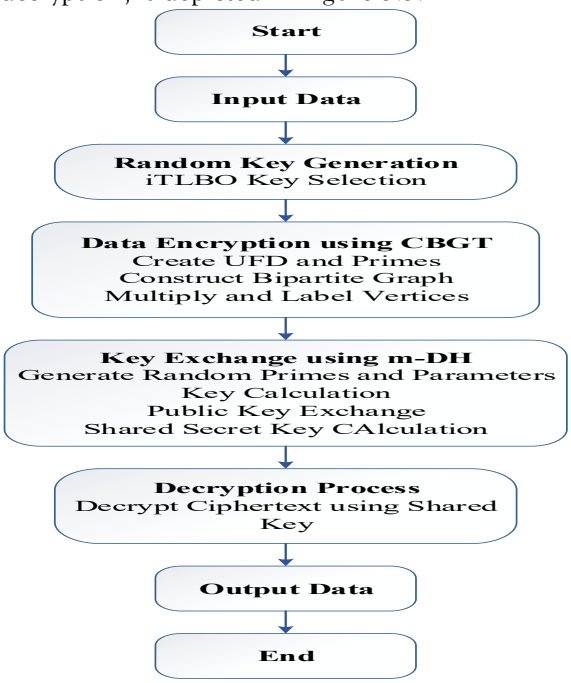
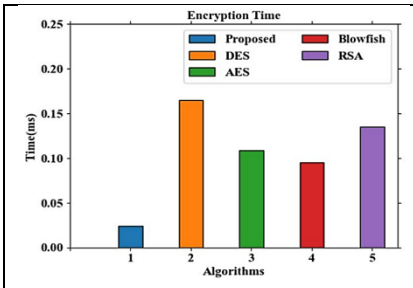


Figure 3.3: The proposed model overall process flow

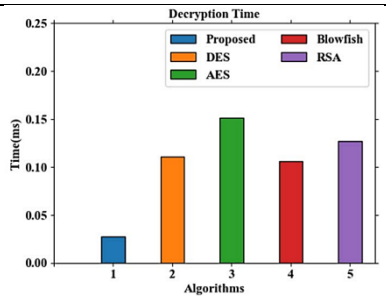
3.3 RESULTS AND DISCUSSION

This section uses simulation and experimental results to assess the effectiveness of the suggested cryptosystem technique for data encryption and decryption. The suggested model is implemented using the Python platform. Table 3.1 lists the parameters that were used to put the suggested cryptosystem into practice.

Here, Figure 3.4 compares the suggested method's encryption and decryption times to those of the other methods now in use.



(a)



(b)

Figure 3.4: (a) Encryption time and (b) decryption time graph

The two graphs of encryption and decryption times compared to the current methods, such as DES, AES, Blowfish, and RSA (Poduval Arjun et al., 2021), are displayed in Figure 3.4. The time required for decryption is consistently longer than the time required for encryption when comparing these two plots. Figure 3.5 shows how long it takes to decrypt modest quantities of data.

The execution time of the suggested CBGT in comparison to the current methods is shown in Figure 3.6.

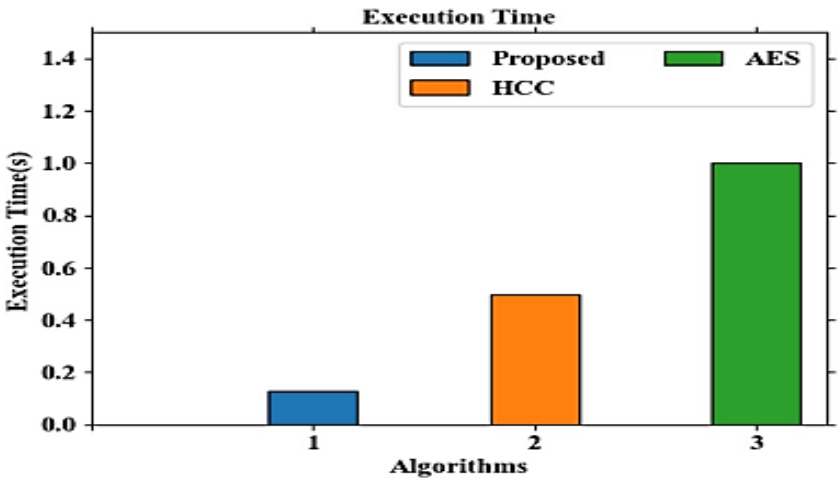


Figure 3.6: Execution time of the proposed approach

The time needed to finish the full suggested CGBT procedure is displayed in Figure 3.6, which also contrasts it with alternative methods like AES and HCC (Hazzazi, Mohammad Mazyad et al., 2023). In this case, the suggested CGBT is faster than AES and HCC.

3.4 Summary

This research brings about a new cryptography system that ensures the speed of data processing along with very high levels of security application, namely, graph theory. A random key generator creates the keys in the first place and then while iTLBO is being applied on these keys, the best picks of the keys are chosen. Simply, encryption based on the crypto-bipartite graph is proposed for data security along with the best-chosen secure keys. In contrast, a modified Diffie-Hellman algorithm is used to perform the key exchange. Finally, the encryption functions are reversed to decode the encrypted data. To improve encryption, the suggested cryptosystem makes use of meta-heuristic optimization-based key selection and the structural characteristics of bipartite graphs. Comparing the suggested CBGT-based cryptosystem to the current DES, AES, Blowfish, and RSA-based techniques, the findings reveal a lower encryption time of 0.0156 ms, a decryption time of 0.0468 ms, and a greater throughput of 288,573.63 bytes/sec. These validation findings thus demonstrate the effectiveness of the proposed cryptosystem. Future research will examine the possibilities of sophisticated graph-theoretic techniques to reduce computational overhead and speed up encryption. For increased security, future advancements might potentially investigate dynamic key updates based on graph modifications.

3.5 DISCUSSION

This section explains how the suggested and current model compare, obtaining the results shown in Table 4.9. The offered paradigm suggests superior data security and privacy when related to alternative models. The effective public key cryptosystem based on DNA-based identity encryption and isogenies of non-supersingular Edwars curves is noteworthy for its innovative cryptography, especially when post-quantum considerations are taken into account. The suggested model uses Identity Based Encryption (IBE), where a user's identity is treated as the public key, to simplify the laborious tasks of key management and distribution. This is in contrast to the methods in [28], [29], and [30], which focus on particular use cases like Digital Twin ecosystems, vehicular ad hoc networks, and intelligent neural network systems. Because of a special DNA encoding procedure that converts the DNA sequence into plaintext before encryption, increasing obfuscation, this streamlined procedure not only increases complexity but also enhances security. Furthermore, the suggested model performed better than others in terms of encryption, decryption, key generation, and CPU usage, making it one of the safest and most scalable solutions that can be applied to many different domains, particularly cloud computing and Internet of Things devices [20]. However, the cited studies do not incorporate such a broad range of cryptographic methods or approaches, and as a result, they do not explain how they might be applied to general security issues.

This work employs a sophisticated key generation procedure in conjunction with efficient encryption. When employing Edward's curves in IBE, a TA chooses a non-supersingular curve, like Ed25519, and uses it to create a master private key and public parameters. The TA generates a unique private key using the master key and each user's identity, which is then securely transmitted to the user for key extraction. To improve security, the DNA encoding procedure is finished before encryption. First, a mapping

approach is used to convert the plaintext message into a DNA sequence. The suggested model is contrasted with other models in the findings section in terms of encryption, decryption, setup time, and other factors. 1.7536 ms for search time, 2.1784 ms for key creation, 2.5672 ms for key retrieval, 4.2502 ms for data encryption, 1.1318 s for data access, and 4.0424% for CPU utilization were the outcomes attained by the suggested methodology. To progress the security of the suggested model and to further prioritize attack detection and cloud security, the research plans to incorporate a more sophisticated encryption model in the future.

3.6 RESULTS AND DISCUSSION

The results of the experimental assessment of suggested approach are shown in this section. The proposed model is simulated using CloudSim and implemented on a Python platform. A 64-bit operating system, an x64-based processor, and an Intel(R) Core(TM) i7-9700 CPU running at 3.20GHz with 16 GB of RAM make up the system. Neither a pen nor a touch input device are needed. When evaluating the performance of the proposed method, we didn't just look at cryptographic execution time, throughput, decryption time, avalanche effect, encryption time, setup time, and CPU utilization. It also considered some other factors as well. The proposed model was compared with Lattice-Based Certificateless Public Key Encryption (L-bCPUK), the elliptic curve digital signature algorithm (ECDSA), RSA, AES, ElGamal, and more. Moreover, we provided an extensive security analysis that illustrates how it defends against different attacks.

The study presented here has made an important breakthrough in data protection: the Tri-level Handshake Lattice-Based Certificateless Public Key Encryption technique. Using the lattice-based nature of cryptography helps to find a solutions to some of the gaps in encryption exploits left by quantum computing, and removes digital certificates. The three-level protocol provides mutual authentication between the two parties, while HKDF along with HMAC provides key management and secure key derivation. The 3HLB-CLPKE architecture of the recommended method delivers an extremely good level of performance across a variety of critical parameters. A total calculation time of 560 ms is recorded, which is an improvement over the previous model in every respect. The calculated handshake time is longer at 151 ms before moving on to key creation at 127 ms, and encryption takes 143 ms while decryption takes about 139

4. CONCLUSION

Across independent yet complementary studies, this paper has validated great accomplishments in encryption strength and system performance for maximum effectiveness regarding the integrity and confidentiality of data while in transit or storage.

The first study affirmed a strong cryptographic system using Crypto Bipartite Graph Theory (CBGT), whereby the security of encryption is enhanced through graph-structured selection of keys. On the other hand, iTLBO-the algorithm for optimized key selection-impressively contributes to bringing forth encryption resilience toward cryptographic attacks without jeopardizing the processing speed. Performance testing proved that this system allowed the least encryption and decryption times together with a comparatively high throughput for standard methods.

5. Future Scope

The current paper brings forward elaborate cryptographic framework addressing contemporary difficulties faced in securing data: the graph-theoretical cryptosystem that uses bipartite graphs and modified Diffie–Hellman key exchange for securing communications; This model indicate improvements in the aspects of encryption efficiency, system throughput, key management, and attack resilience.

Thus, future research directions on their basis would be:

1. An advanced cryptographic method in the graph-theoretic sense can be investigated for the purpose of reducing computation overhead and possibly increasing encryption speed in very large distributed networks.
2. The integration of dynamic key update mechanisms based on real-time graph changes can be investigated to further enhance the adaptability and security of encrypted communications.

REFERENCES

[1] Ahmad, Shahnawaz, and Shabana Mehfuz. "Efficient time-oriented latency-based secure data encryption for cloud storage." Cyber Security and Applications 2 (2024): 100027.

[2] Aliyari Boroujeni, Ahmad, Reza Pourgholi, and Seyed Hashem Tabasi. "A new improved teaching–learning-based optimization (ITLBO) algorithm for solving nonlinear inverse partial differential equation problems." Computational and Applied Mathematics 42, no. 2 (2023): 99.
[3] Al-Riyami, Sattam S., and Kenneth G. Paterson. "Certificateless public key cryptography." In International conference on the theory and application of cryptology and information security, pp. 452-473. Berlin, Heidelberg: Springer Berlin Heidelberg, 2003.
[4] Al-Shabi, Mohammed Abdulhameed. "A survey on symmetric and asymmetric cryptography algorithms in information security." International Journal of Scientific and Research Publications (IJSRP) 9, no. 3 (2019): 576-589.
[5] Balamurugan, Chithralekha, Kalpana Singh, Ganeshvani Ganesan, and Muttukrishnan Rajarajan. "Code-based post-quantum cryptography." (2021).
[6] Bariant, Augustin. "Analysis of AES-based and arithmetization-oriented symmetric cryptography primitives." PhD diss., Sorbonne Université, 2024.
[7] Bokhary, Syed Ahtsham Ul Haq, Athar Kharal, Fathia M. Al Samman, and Ameni Gargouri. "Efficient graph algorithms in securing communication networks." Symmetry 16, no. 10 (2024): 1269.
[8] Cai, Wentian, and Huijun Yao. "A secure transmission method of network communication data based on symmetric key encryption algorithm." Wireless Personal Communications 127, no. 1 (2022): 341-352.
[9] Elkana Ebinazer, Silambarasan, Nickolas Savarimuthu, and S. Mary Saira Bhanu. "ESKEA: enhanced symmetric key encryption algorithm based secure data storage in cloud networks with data deduplication." Wireless Personal Communications 117 (2021): 3309-3325.
[10]El-Latif, Ahmed A. Abd, Janarthanan Ramadoss, Bassem Abd-El-Atty, Hany S. Khalifa, and Fahimeh Nazarimehr. "A novel chaos-based cryptography algorithm and its performance analysis." Mathematics 10, no. 14 (2022): 2434.
[11]Fernandez-Carames, Tiago M., and Paula Fraga-Lamas. "Towards post-quantum blockchain: A review on blockchain cryptography resistant to quantum computing attacks." IEEE access 8 (2020): 21091-21116.
[12]Hazzazi, Mohammad Mazyad, Sasidhar Attuluri, Zaid Bassfar, and Kireet Joshi. "A novel cipher-based data encryption with Galois field theory." Sensors 23, no. 6 (2023): 3287.
[13]Kahate, Sandip A., and Atul D. Raut. "An Enhanced Data Confidentiality in Online Social Networks Using Quantum Key Management with a Blockchain Approach." In 2023 14th International Conference on Computing Communication and Networking Technologies (ICCCNT), pp. 1-6. IEEE, 2023.
[14]Karthiga, S., and E. Murugavalli. "DNA Cryptography." International Research Journal of Engineering and Technology 5, no. 3 (2018): 3987-3991.
[15]Kavitha, S., G. Jayalalitha, and K. Sivaranjani. "Enhanced Security in Public Key Cryptography: A Novel Approach Combining Gaussian Graceful Labeling and NTRU Public Key Cryptosystem." EAI Endorsed Transactions on Internet of Things 10 (2024).
[16]Kościelny, Czesław, Mirosław Kurkowski, and Marian Srebrny. Modern cryptography primer. Springer Verlag, 2013.
[17]Kumar, Sanjay, and Deepmala Sharma. "A chaos-based image encryption scheme using elliptic curve cryptography and genetic algorithm." Artificial Intelligence Review 57, no. 4 (2024): 87.
[18]Lalem, Farid, Abdelkader Laouid, Mostefa Kara, Mohammed Al-Khalidi, and Amna Eleyan. "A novel digital signature scheme for advanced asymmetric encryption techniques." Applied Sciences 13, no. 8 (2023): 5172.
[19]Leiss, Ernst L. Principles of Data Security. Springer Science & Business Media, 2012.
[20]Liu, Guijiang, Haibo Xie, Wenming Wang, and Haiping Huang. "A secure and efficient electronic medical record data sharing scheme based on blockchain and proxy re-encryption." Journal of cloud computing 13, no. 1 (2024): 44.
[21]Manzoor, Atif, Amjad Hussain Zahid, and Malik Tahir Hassan. "A new dynamic substitution box for data security using an innovative chaotic map." IEEE Access 10 (2022): 74164-74174.
[22]Maurer, Ueli. "Modelling a public-key infrastructure." In Computer Security—ESORICS 96: 4th European Symposium on Research in Computer Security Rome, Italy, September 25–27, 1996 Proceedings 4, pp. 325-350. Springer Berlin Heidelberg, 1996.
[23]Moniz, Paulo Miguel Santos. "Confidentiality, Integrity and Non-Repudiation in Smartgrids." Master's thesis, Universidade de Lisboa (Portugal), 2011.
[24]Nithisha, J., and P. Jesu Jayarin. "A secured storage and communication system for cloud using ECC, polynomial congruence and DSA." Wireless Personal Communications 126, no. 2 (2022): 949-974.