International Journal of Engineering Technology and Management Sciences
Website: ijetms.in Issue: 2 Volume No.9 March - April – 2025
DOI:10.46647/ijetms.2025.v09i02.012 ISSN: 2581-4621

THE ROLE OF AI IN IMPROVING ENCRYPTION IN DATA PRIVACY: A HYPOTHETICAL APPROACH

[1]N Keerthi Reddy, [2]K Venkateswari, [3]N Veeralahari, [4]M Pavithra, [5]Dr. G Thippanna
Dept. of CSE, [1-4] 3rd CSE, [4] Professor, Dr. KV Subbareddy Institute of Technology

ABSTRACT
In the digital era, ensuring data privacy has become a paramount concern, particularly as cyber threats continue to grow in complexity. Cryptography [1] plays a vital role in protecting sensitive information, but traditional approaches are increasingly facing challenges in the face of evolving attack strategies. Artificial Intelligence (AI) offers innovative solutions to enhance data privacy within cryptographic systems. This abstract explores how AI can be leveraged to strengthen cryptographic methods and address the challenges of data privacy. AI-based techniques, such as machine learning algorithms, can improve encryption processes by automating key generation, detecting vulnerabilities in cryptographic protocols, and enabling adaptive responses to real-time security threats. Additionally, AI enhances privacy-preserving technologies like homomorphic encryption, differential privacy, and secure multi-party computation by optimizing their efficiency and ensuring more robust protection of sensitive data. AI can also assist in identifying patterns in potential attacks, allowing systems to preemptively adapt and safeguard against breaches. While AI's integration into cryptography offers numerous advantages, it also introduces ethical concerns, particularly when AI-driven cryptanalysis can be used for malicious purposes. Therefore, it is crucial to establish frameworks that govern the responsible use of AI in cryptographic applications.
Keywords: Cryptography, Symmetric Key, Asymmetric Key, Generate AI, AI Models.

1. INTRODUCTION

In today's digital landscape, the convergence of Artificial Intelligence (AI) and cryptography has ushered in transformative advancements in data privacy protection. As AI technologies permeate various aspects of daily life, from predictive analytics to personalized experiences, the imperative to safeguard personal and sensitive information has intensified. Traditional data protection mechanisms face challenges in keeping pace with the sophistication of AI-driven data processing and potential vulnerabilities. This intersection of AI and data privacy has led to the emergence of Privacy-Enhancing Technologies (PETs)[2], which aim to bolster data security while maintaining the utility of data for analytical purposes.

Privacy-Enhancing Technologies (PETs):

PETs are a suite of tools and methodologies designed to protect individual privacy by minimizing data exposure during processing and analysis. These technologies enable organizations to extract valuable insights from data without compromising the confidentiality of personal information. Notable PETs include:

- **Homomorphic Encryption:** Allows computations to be performed on encrypted data, producing results that, when decrypted, match the outcome of operations performed on the original data. This ensures that sensitive information remains confidential throughout the processing phase.
- **Federated Learning:** Enables machine learning models to be trained across decentralized devices holding local data, without exchanging the actual data. This approach preserves data privacy by keeping raw data localized while still benefiting from collective model training.
- **Secure Multi-Party Computation (SMPC):** Facilitates collaborative computations among multiple parties holding private data, ensuring that each participant's data remains confidential and is not exposed to others during the computation process.

International Journal of Engineering Technology and Management Sciences
Website: ijetms.in Issue: 2 Volume No.9 March - April – 2025
DOI:10.46647/ijetms.2025.v09i02.012 ISSN: 2581-4621

- **Differential Privacy:** Incorporates controlled random noise into data analysis outputs, making it difficult to identify individual data entries. This technique allows organizations to share aggregate data insights without revealing information about specific individuals.

The integration of AI with these PETs enhances their effectiveness by automating the detection of privacy risks, optimizing encryption algorithms, and identifying patterns that may indicate potential data breaches. For instance, AI-driven anomaly detection systems can monitor data access patterns to identify and mitigate unauthorized attempts to access sensitive information. Moreover, AI can assist in the development of quantum-resistant cryptographic algorithms, preparing data security infrastructures for the emerging threats posed by quantum computing.

However, the deployment of AI in data privacy[3] enhancement also raises critical considerations. The dual-use nature of AI means that the same technologies can be employed for malicious purposes, such as de-anonymizing data or breaching encryption. Therefore, establishing robust ethical guidelines and regulatory frameworks is essential to govern the use of AI in this domain, ensuring that advancements in data privacy do not inadvertently introduce new risks.

2. LITERATURE SURVEY

2.1. Cryptography

Cryptography[1] is a learning method used to provide secure communication and protect data from any attacks on the data. In order to ensure confidentiality, integrity, authenticity, and non-repudiation, it entails developing and evaluating methods that stop illegal access to data.

➢ Making sure that only people with permission can view and access the data is known as **confidentiality**.

➢ **Integrity**: Confirming that information has not been changed or tampered with while being transmitted or stored.

➢ Verifying the identity of the parties communicating is known as **authentication**.

➢ Ensuring that the sender cannot retract the veracity of their communication is known as **non-repudiation**.

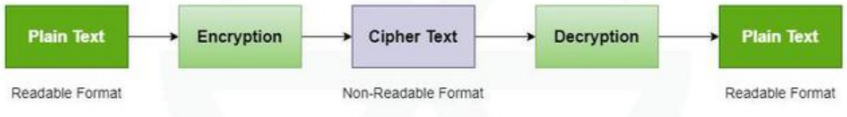

Fig-1 Mechanism of Cryptography.

2.2. Types of Cryptography-

Cryptography is the process to encrypt the data by using different keys into unreadable formats which are can't accessed by unauthorized users. Key is a technical format which is a piece of information used to encrypt and decrypts the data. There are two types of keys, and one is No key based, A single secret key that encrypts and decrypts data is called **Symmetric Key (Private Key)**, two keys one is shared and another one is private key used to encrypt and decrypt the data is known as **Asymmetric Key,** and another approach is **No key** based encrypts the data.

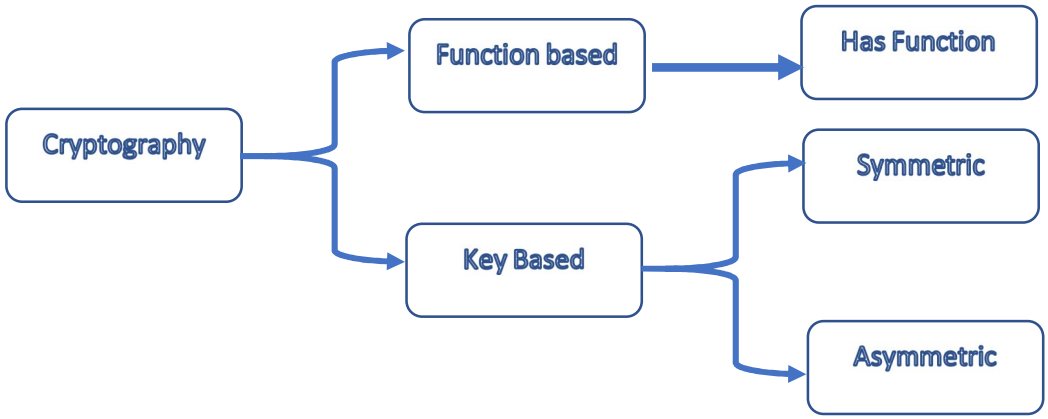

Fig-2: Classification of Cryptography approach

International Journal of Engineering Technology and Management Sciences
Website: ijetms.in Issue: 2 Volume No.9 March - April – 2025
DOI:10.46647/ijetms.2025.v09i02.012 ISSN: 2581-4621

A. Symmetric Key Cryptography

Symmetric key cryptography[4], also known as secret-key cryptography, is a type of encryption where the same key is used for both encryption and decryption.

General Steps for Symmetric Key Cryptography:

1. **Key Generation**:
   - A secret key is generated, which will be used by both the sender and the receiver for encryption and decryption. This key must be kept secure and shared only between trusted parties.
2. **Encryption**:
   - The plaintext (original data) is processed using the encryption algorithm along with the secret key, resulting in ciphertext (encrypted data). The ciphertext is then sent to the receiver.
3. **Transmission**:
   - The encrypted data (ciphertext) is securely transmitted to the receiver over the communication channel.
4. **Decryption**:
   - Once the receiver receives the ciphertext, they use the same secret key with the decryption algorithm to convert the ciphertext back into the original plaintext.

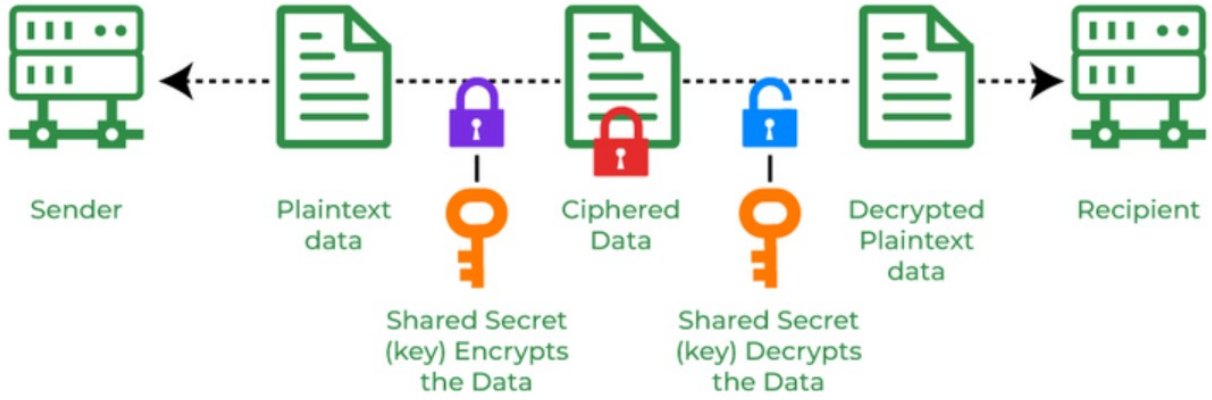

Fig-3 Mechanism of Symmetric Key Cryptography.

B. Asymmetric Key Cryptography

Asymmetric cryptography [5] (also known as public-key cryptography) is a technique that uses two keys: a public key and a private key. The public key is used for encryption, while the private key is used for decryption.

Key Points of Asymmetric Cryptography:

- **Public Key**: This key is shared with anyone who wants to send a message securely. It is used for encrypting data.
- **Private Key**: This key is kept secret by the recipient. It is used for decrypting the encrypted data.

Fig-4 Mechanism of Symmetric Key Cryptography.

International Journal of Engineering Technology and Management Sciences
Website: ijetms.in Issue: 2 Volume No.9 March - April – 2025
DOI:10.46647/ijetms.2025.v09i02.012 ISSN: 2581-4621

C. **Hash Functions**

For this approach No keys are used. Fixed length hash values are calculated according to simple text. This makes it impossible to restore simple text content. Many operating systems use hash functions to encrypt passwords.

3. METHODOLOGY

3.1. AI role in Cryptography

Artificial Intelligence (AI) is playing an increasingly important role in cryptography by enhancing both security mechanisms and the ability to break cryptographic systems. Its impact is seen in various areas, such as encryption, decryption, key management, and cryptographic attacks. Below is the key roles AI can play in cryptography:

a. **Cryptanalysis and Attacking Cryptographic Systems**

AI techniques, particularly **machine learning (ML)** [6] and **deep learning** [7], can be used for cryptanalysis, which is the study of breaking cryptographic algorithms and deciphering encrypted messages without knowing the key. AI can help automate and improve the efficiency of attacks such as:

- **Side-Channel Attacks**: These attacks exploit physical information leaked during encryption processes (e.g., power consumption, electromagnetic radiation) to deduce the secret key. Machine learning models can analyze the patterns in the leaked data and identify the key faster than traditional methods.
- **Key Recovery Attacks**: AI can enhance brute-force attacks by identifying patterns or characteristics in cryptographic systems that could be exploited to reduce the search space for possible keys.
- **Predicting Weaknesses**: AI algorithms can help detect weaknesses or predict vulnerabilities in encryption schemes that are harder to identify through manual cryptanalysis, making cryptanalysis more efficient.
- **Breaking Captchas**: AI models, especially those based on deep learning, have shown the ability to crack image- and audio-based CAPTCHAs, which are often used to distinguish humans from bots and provide a form of cryptographic protection.

b. **Enhancing Cryptographic Algorithms**

AI can also be used to strengthen cryptographic techniques, both in terms of encryption methods and key management:

- **Optimizing Cryptographic Algorithms**: AI can optimize cryptographic algorithms by fine-tuning parameters, identifying more efficient algorithms, and improving the speed of cryptographic processes without sacrificing security.
- **AI-Driven Random Number Generation**: Strong encryption depends on the quality of random numbers (for generating keys). AI-based models can generate more unpredictable and secure random numbers by detecting and avoiding patterns in pseudo-random number generators (PRNGs) that attackers could exploit.
- **Designing New Cryptographic Protocols**: AI can aid in designing new cryptographic protocols that are harder to break. For instance, AI can automate the process of testing new encryption algorithms for vulnerabilities and weaknesses by simulating a wide range of attack scenarios.

c. **Automating and Improving Key Management**

Key management (generating, distributing, storing, and destroying keys) is one of the most critical components of any cryptographic system. AI can help automate and secure key management processes:

- **Key Generation and Distribution**: AI can help generate cryptographic keys that are more secure and resistant to attacks. AI systems can also help distribute keys securely across networks by optimizing the communication paths and reducing vulnerabilities.
- **AI-Based Key Management Systems**: AI-based systems can monitor key usage and predict key expiration or compromise, automatically rotating keys when necessary to ensure optimal security.

DOI:10.46647/ijetms.2025.v09i02.012 ISSN: 2581-4621

AI can also identify abnormal access patterns or usage behaviors associated with potential insider threats or key compromise.

d. **Post-Quantum Cryptography**

Quantum computing [8] poses a significant threat to traditional cryptographic algorithms like RSA and ECC, which could be broken by quantum algorithms such as Shor's algorithm. AI can assist in the development of **post-quantum cryptography (PQC)**:

- **Designing Quantum-Resistant Algorithms**: AI can assist in analyzing quantum-safe algorithms to identify potential weaknesses or help optimize their performance, ensuring that cryptographic systems can remain secure in the face of quantum computing.
- **AI-Enhanced Quantum Cryptography**: AI can improve quantum key distribution (QKD), where quantum mechanics principles are used for secure key exchange. AI could enhance the speed and accuracy of QKD systems, making them more robust against errors or noise in the quantum channels.

e. **AI in Homomorphic Encryption**

Homomorphic encryption is an advanced cryptographic technique that allows computations to be performed on encrypted data without decrypting it. AI can be useful in enhancing this type of encryption:

- **Efficient Homomorphic Encryption**: AI techniques can help optimize homomorphic encryption [9] by finding more efficient ways to perform operations on encrypted data. This could reduce computational overhead and make homomorphic encryption more practical for real-time applications, such as cloud computing and machine learning on encrypted data.
- **AI on Encrypted Data**: Homomorphic encryption allows AI models to train and operate on encrypted data without revealing the underlying information. This ensures that privacy is maintained while still benefiting from AI's capabilities in data analysis.

f. **AI for Cryptographic Protocol Validation and Verification**

AI can help automate the testing and verification of cryptographic protocols, ensuring their security and correctness:

- **Protocol Analysis**: AI systems can be used to simulate attacks on cryptographic protocols and analyze their responses. This can help identify vulnerabilities that might not be apparent through manual analysis.
- **AI-Based Formal Verification**: AI can assist in the formal verification of cryptographic protocols, where the correctness of the algorithm is mathematically proven. AI can enhance the verification process by exploring possible edge cases and attack scenarios.

g. **AI in Blockchain and Distributed Ledgers**

Blockchain technology relies heavily on cryptographic mechanisms, such as hashing and digital signatures, to ensure security and immutability. AI can contribute in several ways:

- **AI for Enhancing Blockchain Security**: AI can monitor blockchain networks for malicious activity, fraud, or security threats. It can also predict potential attacks or identify abnormal patterns that may indicate a compromise in cryptographic functions.
- **Optimizing Consensus Algorithms**: Blockchain systems use cryptographic consensus algorithms (like Proof of Work or Proof of Stake) to validate transactions. AI can help optimize these algorithms, making them more efficient, secure, and scalable.
- **AI for Smart Contracts**: AI can automate the security auditing of smart contracts, which rely on cryptographic mechanisms to execute automatically. AI models can detect vulnerabilities or coding flaws that could be exploited by attackers.

h. **AI in Secure Communication**

AI can enhance secure communication protocols and technologies that use cryptography:

- **AI-Based Intrusion Detection Systems (IDS)**: AI can monitor network traffic and detect anomalies that may indicate attempts to break cryptographic protocols. By learning from patterns of normal and abnormal behavior, AI-driven IDS can quickly detect potential security breaches.

International Journal of Engineering Technology and Management Sciences
Website: ijetms.in Issue: 2 Volume No.9 March - April – 2025
DOI:10.46647/ijetms.2025.v09i02.012 ISSN: 2581-4621

- **Improved Encryption Techniques for IoT Devices**: Internet of Things (IoT) devices often have limited computational power, making traditional encryption challenging. AI can help design lightweight cryptographic protocols tailored for these devices, balancing security and resource efficiency.

i. **AI for Password Security**

AI can contribute to enhancing password security and authentication processes:

- **AI-Based Password Generation and Strength Analysis**: AI can help users generate stronger passwords and analyze the strength of existing passwords, identifying weak patterns or common password choices that could be vulnerable to attacks.
- **Behavioral Biometrics**: AI can be used in combination with cryptographic methods to enhance authentication. For example, behavioral biometrics (such as keystroke dynamics, typing speed, or mouse movements) can be combined with cryptographic techniques to provide stronger multi-factor authentication (MFA).

AI-generated key cryptography refers to using artificial intelligence to enhance or develop cryptographic systems, particularly in the generation and management of cryptographic keys. Here are some potential AI-driven algorithms and techniques that can be applied in cryptography:

3.2. TEXT Encryption using AI generated Symmetric Key

AI-Generated Key Creation Algorithm

Step 1: Initialize Key Generation Environment

- **Input parameters**: AI-based key generation will require some randomness or seed input (e.g., entropy from user input, system-level noise).
- **AI model**: Use a neural network, genetic algorithm, or reinforcement learning model designed to generate high-entropy, cryptographically strong keys.

Step 2: Train AI Model (Optional)

- For more sophisticated key generation, you can train the AI model on previous cryptographic patterns or known weaknesses in existing cryptography to avoid them in future keys.
- The goal is to ensure the AI learns to generate keys that are highly random and resistant to cryptanalysis techniques.

Step 3: Generate the Symmetric Key

- **Input random data**: Feed a source of high-entropy random data (e.g., system noise, hardware RNG) into the AI model.
- **Key creation**: The AI model processes this input to generate a key that is secure and random, following cryptographic principles.
- The AI could also use advanced techniques like deep learning to detect and avoid patterns in key generation that could compromise security.

Step 4: Post-process Key for Symmetry

- Ensure the key is in a usable format, such as a 128-bit or 256-bit string for AES encryption.
- Apply any required transformations to ensure the key meets the desired format for the cryptographic system (e.g., a binary or hexadecimal key).

3.3. Image Encryption Using AI generated Asymmetric Key

AI-Generated Asymmetric Key Creation Algorithm

Step 1: Define the Asymmetric Cryptography System

- **System choice**: Choose the underlying asymmetric encryption system (e.g., RSA, ECC).
- **Input parameters**: Define parameters like key length (e.g., 2048-bit for RSA, 256-bit for ECC).
- **AI model**: Use AI models like neural networks or genetic algorithms to assist in key generation, ensuring randomness and reducing predictability.

Step 2: Train AI Model (Optional)

- The AI can be trained to identify cryptographic weaknesses, ensuring generated keys avoid such patterns.
- The model could learn to identify weaknesses in prime number generation (for RSA) or vulnerabilities in elliptic curve parameters (for ECC).

International Journal of Engineering Technology and Management Sciences
Website: ijetms.in Issue: 2 Volume No.9 March - April – 2025
DOI:10.46647/ijetms.2025.v09i02.012 ISSN: 2581-4621

Step 3: Generate the Key Pair

- **Public and private key relationship**: Ensure the AI-generated keys maintain the necessary mathematical relationship (e.g., for RSA: e*d ≡ 1 (mod φ(n)), where e is the public exponent and d is the private key).

A. **For RSA Key Pair Generation**:

- Use AI to assist in selecting two large prime numbers p and q.
- The product of these primes (n = p * q) forms part of the public key.
- Compute φ(n) = (p-1)*(q-1).
- Choose a public exponent e such that 1 < e < φ(n) and gcd(e, φ(n)) = 1.
- Use AI to compute the private exponent d such that e*d ≡ 1 (mod φ(n)).

B. **For ECC Key Pair Generation**:

- Use AI to help select secure curve parameters, ensuring resistance to known attacks (e.g., side-channel attacks).
- The private key is a randomly chosen integer d from the range [1, n-1] (where n is the order of the curve).
- The public key is computed as Q = d * G, where G is the base point of the elliptic curve.

Step 4: Validate the Key Pair

- Perform standard cryptographic checks to ensure the key pair is valid and secure (e.g., checking for weak keys, ensuring public-private key relationships hold).

C. **Encryption and Decryption Using AI-Generated Keys**

Step 5: Encrypt Data Using the AI-Generated Public Key

- Use the public key to encrypt the plaintext message. The encryption algorithm varies depending on the system:
  - **For RSA**: ciphertext = (plaintext^e) % n.
  - **For ECC**: Encrypt using the public key Q, with the message represented as a point on the elliptic curve.

Step 6: Decrypt Data Using the AI-Generated Private Key

- The recipient uses their private key to decrypt the ciphertext:
  - **For RSA**: plaintext = (ciphertext^d) % n.
  - **For ECC**: Decrypt the elliptic curve point back to the original message.

AI-generated key cryptography involves applying artificial intelligence to both the generation and management of cryptographic keys, enhancing the security and efficiency of cryptographic systems. By leveraging neural networks, reinforcement learning, genetic algorithms, and other AI techniques, it is possible to design more robust and adaptive cryptographic systems capable of resisting current and emerging threats.

4. CONCLUSION

We are engineering graduation students, expressed our thoughts and this is a short article titled How AI interacts with cryptography concepts.

The integration of Artificial Intelligence (AI) into cryptographic systems represents a pivotal advancement in enhancing data privacy within our increasingly digital society. AI-driven techniques such as homomorphic encryption, federated learning, secure multi-party computation, and differential privacy offer robust solutions to protect sensitive information while maintaining its utility for analysis and decision-making. However, the dual-use nature of AI necessitates careful consideration of ethical and security implications, as malicious applications of AI could undermine the very privacy protections these technologies aim to establish. Therefore, it is imperative to develop and enforce ethical guidelines and regulatory frameworks that govern the use of AI in cryptography, ensuring that the pursuit of technological advancement does not compromise individual privacy rights or societal trust. By balancing innovation with responsibility, AI can significantly contribute to the fortification of data privacy in cryptographic applications, paving the way for a more secure and trustworthy digital future.

DOI:10.46647/ijetms.2025.v09i02.012 ISSN: 2581-4621

REFERENCES

1. Thippanna G, A Re-Examine on Assorted Digital Image Encryption | Algorithm's Techniques, Biostat Biometrics Open Acc J. ISSN: 2573-2633, 2018; 4(2): 555633. DOI: 10.19080/BBOAJ.2018.04.555633, PP: 31-38,
2. Simon Fondrie's Technology Blog-Teitler, Office of Technology February 1, 2024, Keeping Your Privacy Enhancing Technology (PET) Promises.
3. https://www.jdsupra.com/legalnews/managing-data-security-and-privacy-6030039/
4. G Thippanna, Dr T Bhaskara Reddy, Dr S Kiran, Image Masking and Compression Using user Private Key Generation, International Journal of Emerging Trends & Technology in Computer Science (IJETTCS), 2014/9, Volume 3 (5), PP 262-266.
5. Leighton Johnson, Chapter 11 - Security component fundamentals for assessment, Academic Press, Security Controls Evaluation, Testing, and Assessment Handbook (Second Edition)2020, Pages 471-536, https://doi.org/10.1016/B978-0-12-818427-1.00011-2
6. Isonkobong Christopher Udousoro, Machine Learning: Review, Semiconductor Science and Information Devices | Volume 02 | Issue 02 | October 2020, DOI: https://doi.org/10.30564/ssid.v2i2.1931
7. Hussein Abdel-Jaber, Disha Devassy, Azhar Al Salam, Lamya Hidaytallah and Malak EL-Amir, A Review of Deep Learning Algorithms and Their Applications in Healthcare, *Algorithms* 2022, *15*(2), 71; https://doi.org/10.3390/a15020071
8. Aayush Joshi etc, Breaking RSA Encryption Using Quantum, Computer, International Journal of Research and Analytical Reviews © 2022 IJRAR May 2022, Volume 9, Issue 2, www.ijrar.org (E-ISSN 2348-1269, P- ISSN 2349-5138).
9. Kavya Joshi etc, Homomorphic Encryption: A Comprehensive Review, Journal of Emerging Technologies and Innovative Research (JETIR), © 2023 JETIR August 2023, Volume 10, Issue 8 www.jetir.org(ISSN-2349-5162), www.jetir.org.