East Journal of Applied Science
ISSN: 3079-9392
Volume 1, Issue 1
Publisher: East Publication & Technology
DOI: https://doi.org/10.63496/ejas.Vol1.Iss1.50

Cryptographic Techniques for Data Privacy Preservation: A Review

Hivi Kamal Ismael* [*1], Wafaa Mustafa Abduallah[2]

[1] Department of Information Technology, Technical College of Informatic-Akre, Akre University for Applied Science, Akre, Kurdistan, Iraq.
[2] Department of Information Technology, Technical College of Duhok, Duhok Polytechnic University, Duhok, Kurdistan, Iraq.
*Corresponding Author: hevi.kamal@auas.edu.krd

Received: 11/02/2025, **Revised**: 18/02/2025, **Accepted**: 22/02/2025, **Published**: 25/02/2025

***Abstract*:**

Protecting our personal and sensitive information is more important than ever in today's online world. Cryptographic techniques are key tools that use math to convert our data into secret codes, making sure only the right people can read it. These methods help keep our information safe from hackers and unauthorized access. This paper explores the crucial role of cryptographic techniques in preserving data privacy in the digital age. There are several types of cryptographic techniques. Symmetric-key encryption uses one key to both lock and unlock data, while asymmetric-key encryption uses two keys, one for locking and another for unlocking. More advanced methods, like homomorphic encryption, allow data to be used without being decrypted, keeping it secure even when it's being processed. Secure multi-party computation lets multiple people work with data together while keeping their own data private. These techniques are essential for protecting sensitive information in areas like healthcare, banking, and online communications. By using cryptography, organizations can meet legal requirements and prevent data breaches. Cryptography ensures that data stays private and hasn't been altered, which builds trust and security in our digital interactions. This paper covers these techniques and highlights their importance in our interconnected world.

***Keywords*: Cryptography, Data Privacy, Data Integrity, Symmetric-key Encryption, Asymmetric-key Encryption, Digital Signature.**

1. Introduction

In today's world, protecting our personal and sensitive information is more important than ever. With the rapid growth of digital technologies and the increasing reliance on online platforms, safeguarding data from cyber threats such as hackers and unauthorized access has become a critical priority. As more aspects of our daily lives, including communication, financial transactions, and healthcare services, are conducted online, ensuring the confidentiality, integrity, and authenticity of data is essential. To achieve this, cryptography, which employs advanced mathematical algorithms to secure information, serves as a vital tool in modern cybersecurity [1]. Cryptography plays a crucial role in maintaining data privacy by converting information into an unreadable format, known as ciphertext, that only authorized individuals can decipher [2]. This process ensures that sensitive information remains confidential and is protected from unauthorized access. Moreover, cryptography safeguards the integrity of data by detecting any unauthorized alterations. Through techniques such as digital signatures, cryptography also verifies the identity of individuals or systems involved in communication, ensuring that messages are genuine and have not been tampered with during transmission [3]. These features are essential for building trust in digital interactions and preventing malicious activities. The importance of cryptographic techniques extends across various sectors, including healthcare, banking, e-commerce, and government services [4]. In healthcare, for example, cryptography protects patients' medical records from unauthorized access, ensuring compliance with privacy regulations such as the Health Insurance Portability and Accountability Act (HIPAA). In the financial sector, encryption safeguards online transactions, preventing unauthorized access to sensitive financial information. Similarly, in e-commerce, cryptographic methods such as Secure Sockets Layer (SSL) and Transport Layer Security (TLS) protocols protect customers' payment details during online purchases. By implementing robust cryptographic measures, organizations can secure their data, safeguard individuals' privacy,

East Journal of Applied Science
ISSN: 3079-9392
Volume 1, Issue 1
Publisher: East Publication & Technology
DOI: https://doi.org/10.63496/ejas.Vol1.Iss1.50

and meet regulatory requirements for data protection [5]. This paper provides a comprehensive overview of various cryptographic methods that play a vital role in securing data in today's digital landscape. It explores symmetric-key encryption, where the same key is used for both encryption and decryption, offering high efficiency and speed. Additionally, the paper discusses asymmetric-key encryption, which uses a pair of keys-one public and one private-to ensure secure communication without the need to share a secret key. Beyond these traditional methods, the paper delves into advanced techniques such as homomorphic encryption, which enables computations on encrypted data without revealing the underlying information, and secure multi-party computation, which allows multiple parties to jointly process data while maintaining its confidentiality. The rest paper is structured as follows: Background theory is given in Section 2, giving the background knowledge and context. Section 3 gives a critical review of the literature, summarizing key studies and progress in the field. Section 4 discusses and contrasts the various methodologies, together with their strengths and limitations. Finally, the paper concludes with a summitry of the findings in Section 5.

2. Background Theory

2.1 Cryptography

Cryptography is a technique that relies on mathematics to secure information such as confidentiality, integrity, and entity authentication [1]. Cryptographic techniques are used for encoding by hiding or encoding data [2]. Encryption and decryption are important cryptography processes. Converting plaintext into ciphertext is called encryption and vice versa because decryption is converting ciphertext into plaintext. Figure 1. Shows working of Encryption and Decryption.

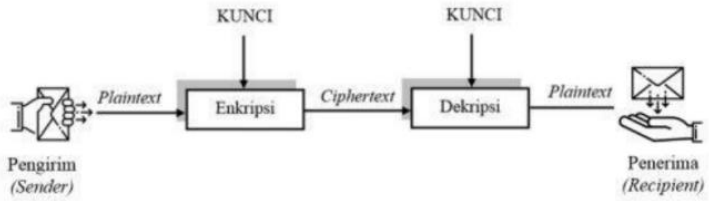

Figure 1. Working of Encryption and Decryption.

2.2 Symmetric-Key cryptography

If two parties are connected, they swap the confidential information known as the key with each other [3]. The sender encodes the message and the recipient also encodes it for encryption and decryption using identical, small key sizes. Before exchanging data, the transmitting parties must agree on a common protocol [1].

Data Encryption Standards (DES), a Triple-DES using a similar mystery key are all the different techniques used in SymmetricKey Encryption. Both parties achieve the balance as a traditional key to the mystery. The first message is referred to as plaintext, and ciphertext is the sender's coded message. The remote critical encryption work [4] is shown in Figure 2. The (3DES) Advanced Encryptions Standard (AES), IDEA and Blowfish are included in this plan.

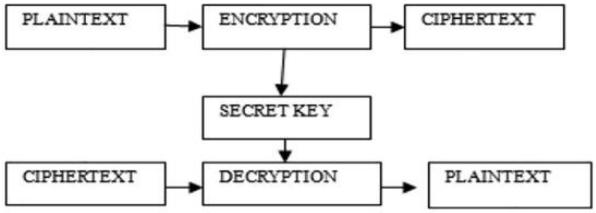

Figure 2. Private Key encryption.

East Journal of Applied Science
ISSN: 3079-9392
Volume 1, Issue 1
Publisher: East Publication & Technology
DOI: https://doi.org/10.63496/ejas.Vol1.Iss1.50

2.3 Asymmetric-Key cryptography

Public essential procedures enable customers to transmit securely without any mystery key being granted in advance. The approving party generates a leading pair (pk, sk) in this plan. The message is encoded using a public key pk and decoded using a private key [4] by the collector. The general essential encryption functioning is shown in Fig. 3. The public and private key pair used for this plan; (pk, sk). No data or key needs to be exchanged in advance. It appears to be the main topic of appropriation since the parties do not need to exchange a key in advance. But it depends on complex science, and slower than that, it is remarkably safe Encryption of private key [5]. RSA, ElGamal and Elliptical Curve Cryptography (ECC) are the different techniques used in asymmetric-key encryption.

2.4 Privacy Preserving

Data privacy encompasses several aspects, such as identity privacy, where the identity of users is kept confidential except for authorized entities; data privacy, where data remains confidential except for authorized users; and usage privacy, where user activities remain confidential except to authorized parties [6]. With the rapid expansion of the internet and information technology fields in recent years, measures to protect privacy have started to emerge in cyberspace [7]. Consequently, industry experts have initiated the development of innovative privacy solutions [8]. The initial focus was on understanding data preservation better and defining privacy-preserving methods. Challenges like power outages, hardware malfunctions, and network disruptions can lead to data failures in the Cloud. To address these issues, several strategies like randomization, micro-aggregation, and data condensing have been suggested to maintain data stream privacy. Additionally, developing a privacy-preserving method requires a unique approach that integrates essential privacy features. Nagaraj and Kumar [7] have suggested a four-component architecture for a privacy-preserving method, including a user engine, user interface, Cloud database, and rule engine. Another proposed solution for the email system is Pixelated, a privacy-preserving initiative. This consists of a user interface developed with a web application programming language and an email election engine. This design enables users to establish a secure connection with the server from their site, ensuring data confidentiality [9].

2.4.1 Privacy-Preserving Techniques

The primary obstacle in de-identification lies in figuring out how to share data that remains valuable for organizations, administrations, and companies to make well-informed decisions without revealing sensitive details about individuals. This involves finding methods that minimize the risk of exposing private information while still enabling statistical analysis and data mining activities. This balance between data privacy and utility has spurred efforts to either develop new privacy-preserving techniques (PPT) or improve upon existing ones. Willenborg and Waal [10] were pioneers in establishing guidelines for safeguarding microdata, proposing a classification system for PPT based on the characteristics of microdata. Their classification includes both non-perturbative methods, which reduce or suppress details, and perturbative methods, which alter data. Understanding the difference between these techniques is crucial when considering an intruder's perspective; perturbative methods might pique an intruder's interest due to the anomalies they introduce, enticing attempts to reconstruct original data. In contrast, non-perturbative methods do not create such inconsistencies. While these methods have been widely discussed and used in the past, other innovative PPT have emerged that likely belong in a separate category known as de-associative techniques. These techniques aim to sever the link between quasi-identifiers (QI) and sensitive attributes by either scrambling the sensitive values or splitting the data into two tables-one for QI attributes and the other for sensitive attributes. Additionally, the generation of synthetic data is another strategy for statistical disclosure control (SDC), aiming to produce artificial data that retains the properties of the original dataset [11]. A general overview of the main PPT is illustrated in Figure 3.

East Journal of Applied Science
ISSN: 3079-9392
Volume 1, Issue 1
Publisher: East Publication & Technology
DOI: https://doi.org/10.63496/ejas.Vol1.Iss1.50

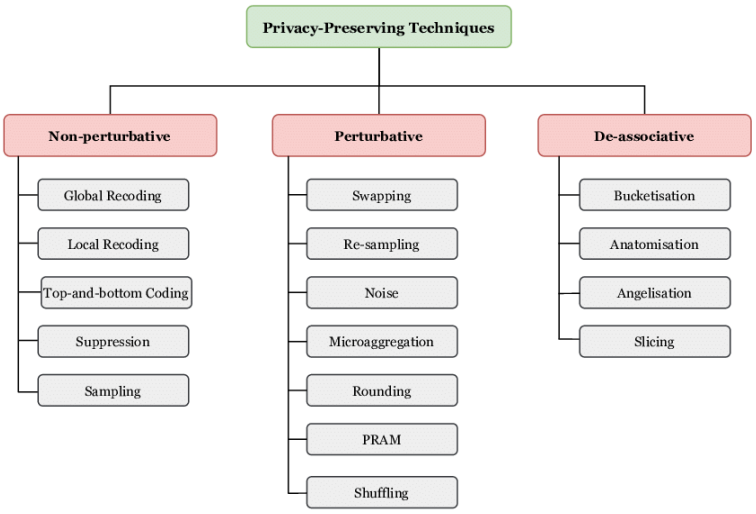

Figure 3. Taxonomy for privacy-preserving techniques in microdata.

2.4.2 Secure Cloud Communications

When the previous phase of anonymous authentication is a success, the consumer 'Ci' can upload their data to the cloud and can be downloaded, if there is a demand. Anonymous authentication allows people to access one's Web or FTP site's public parts without requiring them to enter a user name or password. Moreover, the data integrity can be secured with the symmetric cipher. And, the encryption and decryption are processed here with AES in the authentication phase. Here, ensuring secure cloud communication is developed by considering that the CSP is the third-party auditor in some cases. The malicious user can be one of the third-party auditors [12]. Hence, their illegal access to the cloud data is to be unsuccessful. Moreover, the overall process of cloud communication over in the proposed model of privacy-preserving is provided in Figure 4., the data taken from the model is computed, and then the computed data is again processed in application service via operation model for key generation. Meantime, the generated key is given to the CSP interface for third-party administration (TPA) via Access permission and data upload. A Third-Party Administrator (TPA) is a service company that, under the terms of a service agreement, performs several services to the insurance business. The TPA is primarily responsible for ensuring data integrity. It performs tasks such as producing hashes for encrypted blocks received from the cloud server, concatenating them, and generating signatures on them. It then analyzes both signatures to govern whether or not the information saved in the cloud has been tampered with. Further, the data from the TPA is given to the cloud consumer [13].

East Journal of Applied Science
ISSN: 3079-9392
Volume 1, Issue 1
Publisher: East Publication & Technology
DOI: https://doi.org/10.63496/ejas.Vol1.Iss1.50

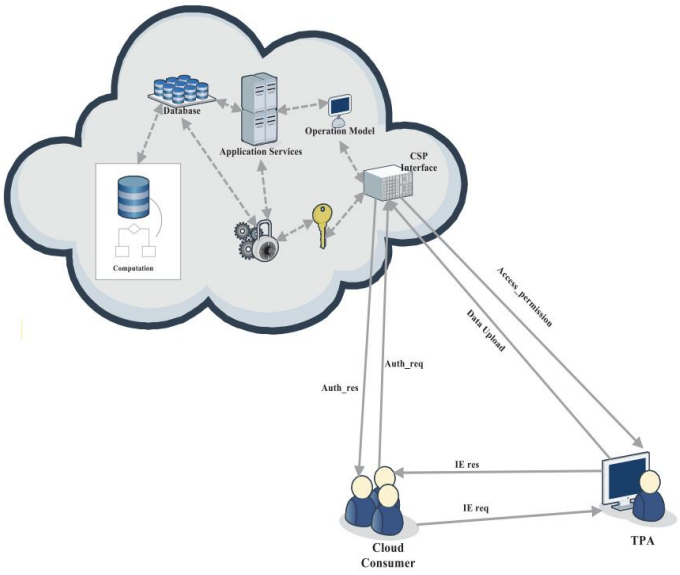

Figure 4. Model of privacy-preserved data security approach

2.5 Cryptographic Techniques for Data Privacy Preservation

2.5.1 Key Management

Proper management of cryptographic keys is essential for maintaining data privacy. Key generation, distribution, storage, and rotation are important aspects of key management to prevent unauthorized access to sensitive data [14].

2.5.2 Digital Signature

The digital signature is one scheme with cryptographic value by relying on the message and the message's sender. Digital signatures guarantee data integrity, detect changes or modifications to messages sent, and perform authenticity. Creating a signature on a message can be done by performing a digital signature with a hash function [2]. Figure 5. Shows digital signature scheme**.**

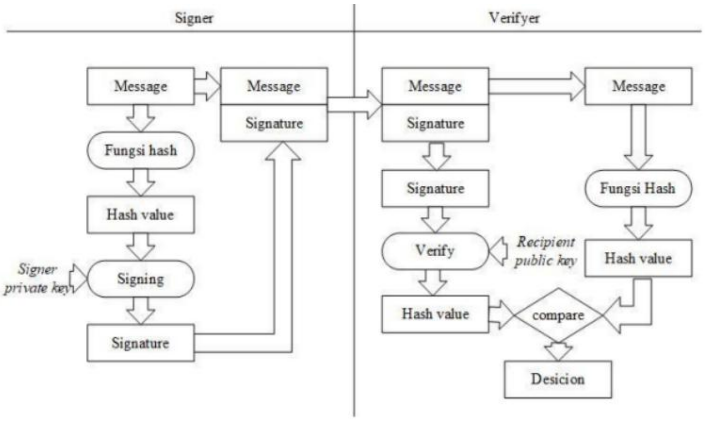

Figure 5. Digital Signature Scheme.

East Journal of Applied Science
ISSN: 3079-9392
Volume 1, Issue 1
Publisher: East Publication & Technology
DOI: https://doi.org/10.63496/ejas.Vol1.Iss1.50

2.5.3 Hash Function and Data Integrity

A hash function is often referred to as a one-way function. The hash function has long been used in the world of computer science. A hash function is a mathematical calculation that takes the variable length of an input string and converts it to a fixed length. The resulting output is commonly referred to as a hash value. Using a hash algorithm makes it easy to calculate the hash value on a message and makes it impossible to modify the message without composing the resulting hash value. The hash function can detect any modifications to the sent message. The hash function can guarantee data integrity based on specific settings [2]. Figure 6. Shows checking of message integrity.

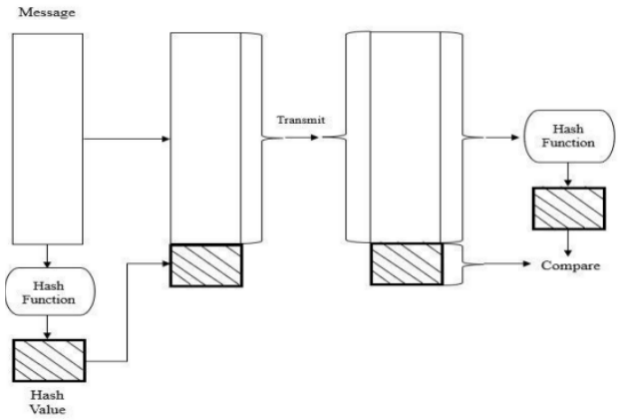

Figure 6. Message Integrity Checking.

2.5.4 Zero-Knowledge Proof (ZKP)

Zero-Knowledge Proof (ZKP), a cryptographic technique introduced in 1985 [15], enables a prover to demonstrate the correctness of a statement to a verifier without disclosing any information beyond the statement's validity. In the blockchain context, ZKP protocols like zk-SNARKs are widely utilized to ensure privacy by generating succinct proofs without divulging underlying data, facilitating functionalities such as decentralized coinmixing pools for enhanced privacy [16].

2.5.5 Homomorphic Encryption (HE)

Homomorphic Encryption (HE) stands as a pivotal cryptographic technique in blockchain development, allowing operations on encrypted data without exposing plaintext, thereby ensuring both confidentiality and data availability. With partial and fully homomorphic encryption, users can securely perform computations on encrypted data, preserving privacy while upholding computational efficiency [17]. Each of these privacy protection technologies plays a crucial role in enhancing data privacy on the blockchain, mitigating concerns associated with confidentiality and security [18].

2.5.6 Secure Multi-party Computation (SMPC)

Secure Multi-party Computation (SMPC) enables multiple participants to collaboratively process private data without disclosing individual inputs. Protocols like garbled circuits and secret sharing facilitate secure computation of functions while maintaining data privacy, ensuring that each participant only accesses their computed values [19].

East Journal of Applied Science
ISSN: 3079-9392
Volume 1, Issue 1
Publisher: East Publication & Technology
DOI: https://doi.org/10.63496/ejas.Vol1.Iss1.50

2.5.7 Data Encryption

Conventional data storage and sharing methods are vulnerable to various security threats [20][21], notably due to their dependence on centralized servers, rendering them susceptible to attacks and resulting in issues such as data leaks and tampering. Traditional encryption methods are inadequate to meet the escalating security requirements [22][23].

To address these challenges, privacy protection technology amalgamating artificial intelligence and blockchain has emerged. Leveraging distributed encryption algorithms substantially enhances the security and privacy protection level of data [18].

2.6 Access Control

Access control is pivotal in ensuring privacy protection by regulating access based on user identity and group membership to ensure only authorized users can access specific resources, thus protecting the system from unauthorized intrusion. Effective access control requires meticulous consideration and implementation of factors such as user authentication [24], authorization [25], and access policies [26]. Only through integrating these aspects can privacy and security be maintained within the system.

Digital Identity Technology (DIT) [27] emerges as a promising approach for IoT applications, providing secure access control and safeguarding device and data privacy. Wazid et al. [28] proposed access control policies based on digital identity technology and cryptographic primitives to enhance communication security among entities like drones, Ground Station Servers (GSS), and cloud servers. This approach ensures secure data sharing.

2.7 Data Protection

Data protection encompasses various measures such as access control, data encryption [27], data backup, and security auditing to prevent illegal access, tampering, or leakage of user data. Technologies like anonymization, data masking [29], data encryption, and data isolation shield data from unauthorized access and leakage. Encryption technologies like differential privacy protection [30], homomorphic encryption, hash algorithms , digital signature algorithms, and asymmetric encryption algorithms [29] ensure data confidentiality and prevent unauthorized access.

2.8 Network Security

Network security encompasses preventing network attacks, ensuring data confidentiality and integrity, and safeguarding systems from malicious software and network viruses. Various security measures, secure network architectures, and protocols must be implemented to achieve system security and reliability [18].

3. Literature Review

In recent years, various cryptographic techniques have been developed to enhance data privacy and security across different domains. These advancements aim to ensure confidentiality, integrity, and secure data processing without compromising performance.

Shanthi et al. [31] explored methods for enhancing data privacy in smart cyber-physical systems (SCPS), such as healthcare and smart cities. It detailed privacy preservation techniques like encryption, which was secure but computationally heavy, and perturbation methods like noise addition, which were simpler but might compromise data utility. Differential Privacy (DP) was discussed as a method that minimized privacy leaks but was limited by database size. The review also addressed challenges such as balancing privacy, utility, and scalability; enhancing

East Journal of Applied Science
ISSN: 3079-9392
Volume 1, Issue 1
Publisher: East Publication & Technology
DOI: https://doi.org/10.63496/ejas.Vol1.Iss1.50

DP for real-valued data; and developing robust privacy solutions for resource-constrained environments. It proposed a three-step process for maintaining data's spatial layout while ensuring privacy and demonstrated the effectiveness of this framework in maintaining data in various datasets, highlighting the need for tailored privacy-preserving solutions for SCPS-generated data.

M. Iezzi [32] provided a comprehensive review of how homomorphic encryption (HE) was applied in data science to enhance privacy while preserving data utility in enterprise applications. It traced the evolution of HE from its initial limited operational capabilities to the development of Fully Homomorphic Encryption (FHE) by Gentry in 2009, which allowed for unlimited computational operations on encrypted data. The paper discussed recent advancements in HE and its expansion into fields like medicine and finance, detailing various types of HE such as Partially Homomorphic Encryption (PHE), Somewhat Homomorphic Encryption (SWHE), and FHE. It highlighted their specific capabilities and limitations. The paper also illustrated the application of HE in real-world data science scenarios, such as in privacy-preserved predictions and machine learning models on encrypted data, showing improvements in computational efficiency and the development of HE libraries that aided in implementing data science algorithms securely. Despite significant progress, the paper identified ongoing challenges like computational overhead, the complexity of managing HE schemes, and the need for continued research to improve HE's efficiency and usability. Overall, the review underscored HE's role in transforming privacy-preserving data science, emphasizing its potential to securely manage sensitive data in collaborative settings.

Salim et al. [33] highlighted HE's ability to allow computations on encrypted data, thus preserving the functionality for analysis without needing decryption. The study detailed methods including Partially, Somewhat, and Fully Homomorphic Encryption, each offering different levels of computation freedom. Secret sharing was used to distribute tasks among virtual nodes securely, ensuring data privacy against untrusted cloud servers. Results indicated that these techniques enhanced data confidentiality and integrity, effectively protecting sensitive patient effect data from cyber threats and unauthorized access. The paper underscored the advantages of decentralizing computations and using edge computing resources to reduce latency, crucial for real-time healthcare applications. Overall, it presented a robust model for enhancing cybersecurity in healthcare technologies through advanced encryption and data handling strategies.

Maurya and Joshi [34] investigated two advanced privacy-preserving methods within data security. It discussed Group-Based Anonymization, which grouped individuals to maintain anonymity and data utility, balancing accessibility with privacy protection. Additionally, the Hybrid ECC Encryption Algorithm enhanced security in data transmissions by combining symmetric and asymmetric encryption, thus overcoming computational challenges of traditional ECC methods and strengthening defenses against unauthorized access. The study reviewed these methods' impact on data confidentiality and integrity, with the Hybrid ECC method showing lower computational costs and improved security over traditional methods. The findings emphasized the importance of sophisticated privacy-preserving methods for protecting sensitive information, significantly contributing to the discourse in data security.

Kaaniche and Laurent [35] provided a detailed review of cryptographic techniques that enhanced security and privacy in cloud storage. It discussed defense mechanisms like Homomorphic Encryption and Proxy Re-encryption, which enabled secure data handling and computations on encrypted data without exposure to unauthorized parties. The paper also analyzed security models that assessed the trustworthiness of cloud service providers and cryptographic models such as Attribute-Based Encryption and Homomorphic Encryption. Additionally, it covered techniques for verifying data integrity and availability, such as Proof of Data Possession and Proof of Retrievability, along with privacy-preserving methods like Searchable Encryption and Private Information Retrieval for secure query execution on encrypted data. While these methods significantly improved data security and privacy, challenges like managing complex encryption keys, maintaining regulatory compliance, and achieving efficient performance remained. The review highlighted the ongoing necessity to develop and implement robust cryptographic solutions to address both technical and regulatory challenges in cloud-related security.

East Journal of Applied Science
ISSN: 3079-9392
Volume 1, Issue 1
Publisher: East Publication & Technology
DOI: https://doi.org/10.63496/ejas.Vol1.Iss1.50

Catak et al. [36] examined cryptographic strategies for protecting sensitive data in big data systems. It discussed using homomorphic encryption to enable secure computations on encrypted data, facilitating cloud-based processing without compromising privacy. Various cryptographic models were evaluated, and novel privacy-preserving clustering methods using homomorphic encryption were introduced. These methods, designed for cloud platforms, reduced local processing demands. The study demonstrated that complex tasks like distance matrix calculations for clustering algorithms could be efficiently managed while keeping data encrypted. Performance was assessed using six evaluation metrics, showing the effectiveness of these methods. Overall, the paper highlighted the benefits of homomorphic encryption in maintaining data privacy and enabling complex big data analytics.

Su et al. [37] analyzed privacy-preserving techniques in machine learning, focusing on homomorphic encryption (HE) and its integration with AI. It explored methods like HE, which allowed operations on encrypted data, and Secure Multi-Party Computing, which enabled joint computations without data sharing. Order Preserving Encryption (OPE) maintained data order post-encryption for comparisons. Federated Learning Models trained algorithms across decentralized devices, sharing only model updates to enhance privacy. Dense State Computing Models used HE for complex encrypted data computations, aimed at secure cloud applications. Privacy-Preserving Federated Learning encrypted data locally before uploading it to a central server, protecting sensitive information during transmission and storage. The study tested these techniques using the Pima and Heart Disease UCI datasets, showing their effectiveness in safeguarding privacy. Results indicated that HE and secure multi-party computation allowed secure predictive analytics, with minor accuracy losses due to encryption-related computational costs. Overall, combining HE with AI and machine learning proved to be a viable solution for secure, privacy-preserving data analysis in various applications, highlighting the need for further research to enhance these methods' efficiency and scalability.

Chen et al. [38] provided a detailed literature review on IoT data security. It focused on the efficiency and robustness of symmetric encryption methods, particularly AES, in securing IoT data. It examined deep packet inspection (DPI) techniques that allowed data traffic to be inspected without compromising encryption. The paper evaluated security models that applied symmetric cryptography to maintain data confidentiality and integrity in IoT networks, including those that combined symmetric encryption with other cryptographic methods. It also introduced techniques for inspecting encrypted traffic without decryption, such as pattern matching and anomaly detection, and discussed key management strategies essential for IoT security. The study demonstrated that AES could secure IoT traffic with minimal performance impact and showed the feasibility of efficient encrypted traffic inspection. The results confirmed that these cryptographic techniques provided strong security guarantees, preventing unauthorized access and protecting data privacy. Overall, the paper highlighted the effectiveness of symmetric cryptographic techniques for privacy-preserving traffic inspection in IoT and called for further research to enhance these methods.

Singh et al. [39] reviewed privacy-preserving techniques in machine learning, focusing on homomorphic encryption (HE) and AI integration. HE allowed encrypted data operations without decryption, ensuring secure data outsourcing and analysis. The review also covered secure multi-party computing for joint data computations without sharing, and Order Preserving Encryption (OPE) for maintaining data order post-encryption. It evaluated Federated Learning Models, which trained algorithms on decentralized devices with shared model updates, and Dense State Computing Models for complex encrypted data computations in cloud applications. Privacy-preserving federated learning was introduced, where data was encrypted locally before central server upload, protecting information during transmission and storage. Experimental designs using datasets like the Pima and Heart Disease UCI datasets showed the methods' effectiveness in protecting privacy. HE and secure multi-party computation allowed secure predictive analytics with minor accuracy losses. The combination of HE and machine learning was shown to be a viable solution for secure data analysis in various applications, highlighting the need for further research to enhance efficiency and scalability.

Mondal and Goswami [40] provided an analysis of methods, models, techniques, and results for cloud security. It discussed the use of homomorphic cryptosystems for secure data operations without decryption and honeypot schemes for encryption and decryption, ensuring secure data access. Various Intrusion Detection Systems (IDS)

East Journal of Applied Science
ISSN: 3079-9392
Volume 1, Issue 1
Publisher: East Publication & Technology
DOI: https://doi.org/10.63496/ejas.Vol1.Iss1.50

models that employed multiple encryption techniques and attribute-based encryption were explored. The evaluation included decision trees and machine learning algorithms for classifying and predicting attacks. The preprocessing stage involved removing missing values and redundant data, with GLCM used for feature extraction. Gradient fuzzy K-means clustering and CNN classification were applied to identify attack types. The methods demonstrated high accuracy and effectiveness in detecting and classifying attacks, validating the efficacy of the honeypot cryptographic scheme. The study highlighted that combining cryptographic techniques with machine learning enhanced cloud security, data privacy, and intrusion detection, emphasizing the importance of advanced cryptographic schemes and AI integration. A summary of the key studies discussed in this section, including techniques, key results, advantages, and disadvantages, is presented in Table 1.

Table 1. Summary of Literature Review

Authors & Reference	Techniques	Key Results	Advantages	Disadvantages
Shanthi et al. [31]	Encryption, Perturbation, Differential Privacy	Effective in maintaining spatial data layout	Balances privacy, utility, scalability; tailored for SCPS data	DP limited by database size; encryption computationally heavy
M. Iezzi [32]	Homomorphic Encryption (PHE, SWHE, FHE)	HE libraries developed, improved computational efficiency	Applicable in diverse fields, secures sensitive data	Computational overhead, managing HE schemes complex
Salim et al. [33]	Homomorphic Encryption, Secret Sharing	Enhanced data confidentiality and integrity	Decentralizes computations, reduces latency, crucial for real-time healthcare	Complex encryption management
Maurya and Joshi [34]	Group-Based Anonymization, Hybrid ECC Encryption	Improved security and lower costs	Sophisticated privacy-preserving, balances accessibility and privacy protection	Traditional ECC methods computationally challenging
Kaaniche and Laurent [35]	Homomorphic Encryption, Proxy Re-encryption, Various Cryptographic Models	Enhanced cloud storage security	Secures data handling and computations, various cryptographic models assessed	Complex key management, regulatory compliance, performance issues
Catak et al. [36]	Homomorphic Encryption, Privacy-Preserving Clustering Methods	Effective big data analytics while preserving privacy	Reduces local processing demands, maintains data privacy in cloud-based processing	Need for further improvement in efficiency
Su et al. [37]	Homomorphic Encryption, Secure Multi-Party Computing, Federated Learning	Effective in safeguarding privacy	Supports complex computations on encrypted data, integration with AI	Minor accuracy losses, needs further research on scalability and efficiency
Chen et with. [38]	AES, Deep Packet Inspection (DPI)	Efficient encrypted traffic inspection	Strong security guarantees, minimal performance impact	Need for enhanced methods
Singh et al. [39]	Homomorphic Encryption, Secure	Secure predictive analytics	Protects data during transmission and storage, integrates	Scalability challenges, minor accuracy losses

East Journal of Applied Science
ISSN: 3079-9392
Volume 1, Issue 1
Publisher: East Publication & Technology
DOI: https://doi.org/10.63496/ejas.Vol1.Iss1.50

	Multi-Party Computing, Federated Learning		with machine learning	
Mondal and Goswami [40]	Homomorphic Cryptosystems, Honeypot schemes, IDS models	High effectiveness in detecting and classifying attacks	Combines cryptographic techniques with machine learning, enhances cloud security	Advanced cryptographic schemes and AI integration required

4. Discussion

Studying cryptographic techniques shows how important they are for keeping data private and secure online. The reviewed literature highlights significant advancements in privacy-preserving techniques across various domains. Shanthi et al. [31] explored methods for enhancing data privacy in smart cyber-physical systems (SCPS), detailing encryption and perturbation methods, and addressing the balance between privacy, utility, and scalability. M. Iezzi [32] traced the evolution of homomorphic encryption (HE) and its applications in data science, emphasizing its role in preserving data utility while enhancing privacy. Salim et al. [33] highlighted the use of HE and secret sharing in healthcare, demonstrating improved data confidentiality and integrity. Maurya and Joshi [34] examined Group-Based Anonymization and Hybrid ECC Encryption, showing improved security and lower computational costs. Kaaniche and Laurent [35] reviewed cryptographic techniques in cloud storage, focusing on homomorphic encryption and proxy re-encryption, while addressing challenges like key management and regulatory compliance. Catak et al. [36] discussed cryptographic strategies for big data, demonstrating the effectiveness of homomorphic encryption in maintaining data privacy. Su et al. [37] analyzed privacy-preserving techniques in machine learning, combining HE with AI for secure data analysis. Chen et al. [38] reviewed IoT data security, emphasizing symmetric encryption methods like AES and techniques for inspecting encrypted traffic. Singh et al. [39] focused on HE and AI integration for secure data outsourcing and analysis in machine learning. Finally, Mondal and Goswami [40] discussed methods for cloud security, validating the efficacy of honeypot cryptographic schemes and machine learning models. Overall, these studies underscore the importance of advanced cryptographic techniques and their integration with AI to enhance data privacy and security across various applications.

5. Conclusion

This paper has delved into various cryptographic techniques crucial for maintaining data privacy. The exploration covered symmetric-key encryption, which uses a single key for both encryption and decryption, and asymmetric-key encryption, which employs a pair of keys for enhanced security. Advanced methods like homomorphic encryption and secure multi-party computation were also discussed, highlighting their ability to process encrypted data without compromising privacy. Cryptographic techniques play an essential role in protecting sensitive information across different sectors such as healthcare, banking, and online communications. These methods not only ensure data privacy but also maintain data integrity, which is vital for building trust in digital interactions. By employing these techniques, organizations can meet legal and regulatory requirements, preventing data breaches and unauthorized access. In conclusion, the importance of cryptography in safeguarding our digital world cannot be overstated. As technology continues to evolve, so too must our cryptographic methods to address new challenges and threats. Continuous research and development in cryptography will ensure that our data remains secure, private, and integral, fostering a safer digital environment for all.

References

[1] S. Vollala, N. Ramasubramanian, U. Tiwari, S. Vollala, N. Ramasubramanian, and U. Tiwari, “Modular Exponential Techniques,” *Energy-Efficient Modul. Exponential Tech. Public-Key Cryptogr. Effic. Modul. Exponential Tech.*, pp. 67–83, 2021.

Volume 1, Issue 1
Publisher: East Publication & Technology
DOI: https://doi.org/10.63496/ejas.Vol1.Iss1.50

[2] R. Bahri, M. Budiman, and B. Nasution, "Sign-Then-Encrypt Scheme with Cramer-Shoup Cryptosystem and Dissanayake Digital Signature," no. Icaisd 2023, pp. 131–138, 2024, doi: 10.5220/0012444900003848.

[3] M. S. Lydia, M. A. Budiman, and D. Rachmawati, "Factorization of Small Rprime RSA Modulus Using Fermat's Difference of Squares and Kraitchik's Algorithms in Python," 2021.

[4] D. Kumar Sharma, N. Chidananda Singh, D. A. Noola, A. Nirmal Doss, and J. Sivakumar, "A review on various cryptographic techniques & algorithms," *Mater. Today Proc.*, vol. 51, no. xxxx, pp. 104–109, 2021, doi: 10.1016/j.matpr.2021.04.583.

[5] W. Li, X. Chang, A. Yan, and H. Zhang, "Asymmetric multiple image elliptic curve cryptography," *Opt. Lasers Eng.*, vol. 136, p. 106319, 2021.

[6] Y. I. Alzoubi, A. Al-Ahmad, and H. Kahtan, "Blockchain technology as a Fog computing security and privacy solution: An overview," *Comput. Commun.*, vol. 182, pp. 129–152, 2022.

[7] A. Mishra, T. S. Jabar, Y. I. Alzoubi, and K. N. Mishra, "Enhancing privacy-preserving mechanisms in Cloud storage: A novel conceptual framework," *Concurr. Comput. Pract. Exp.*, vol. 35, no. 26, pp. 1–21, 2023, doi: 10.1002/cpe.7831.

[8] L. Kuang, S. Tu, Y. Zhang, and X. Yang, "Providing privacy preserving in next POI recommendation for Mobile edge computing," *J. Cloud Comput.*, vol. 9, pp. 1–11, 2020.

[9] A. Alzahrani, T. Alyas, K. Alissa, Q. Abbas, Y. Alsaawy, and N. Tabassum, "Hybrid approach for improving the performance of data reliability in cloud storage management," *Sensors*, vol. 22, no. 16, p. 5966, 2022.

[10] L. Willenborg and T. De Waal, *Elements of statistical disclosure control*, vol. 155. Springer Science & Business Media, 2012.

[11] V. Torra, *A Guide to Data Privacy*. Springer, 2022.

[12] S. Rani, P. Bhambri, A. Kataria, A. Khang, and A. K. Sivaraman, *Big Data, Cloud Computing and IoT: Tools and Applications*. CRC Press, 2023.

[13] S. Stewart Kirubakaran, V. P. Arunachalam, S. Karthik, and S. Kannan, "Towards Developing Privacy-Preserved Data Security Approach (PP-DSA) in Cloud Computing Environment," *Comput. Syst. Sci. Eng.*, vol. 44, no. 3, pp. 1881–1895, 2023, doi: 10.32604/csse.2023.026690.

[14] S. Ahmad, S. Mehfuz, and J. Beg, "Hybrid cryptographic approach to enhance the mode of key management system in cloud environment," *J. Supercomput.*, vol. 79, no. 7, pp. 7377–7413, 2023.

[15] M. M. Islam, "Exploring the Applications of Artificial Intelligence across Various Industries," *J. Artif. Intell. Gen. Sci. ISSN*, pp. 3006–4023, 2024.

[16] S. Akter, "Investigating State-of-the-Art Frontiers in Artificial Intelligence: A Synopsis of Trends and Innovations," *J. Artif. Intell. Gen. Sci. ISSN*, pp. 3006–4023, 2024.

[17] M. Sarker, "Revolutionizing healthcare: the role of machine learning in the health sector," *J. Artif. Intell. Gen. Sci. ISSN 3006-4023*, vol. 2, no. 1, pp. 36–61, 2024.

[18] A. Intelligence, G. Science, J. Home, C. Author, and H. Padmanaban, "Privacy-Preserving Architectures for AI / ML Applications : Methods , Balances , and Illustrations Harish Padmanaban Site Reliability Engineering lead and Independent Researcher Article History : Received : Accepted : Introduction :," vol. 3, no. 01, 2024.

[19] H. Padmanaban, "Revolutionizing Regulatory Reporting through AI/ML: Approaches for Enhanced Compliance and Efficiency," *J. Artif. Intell. Gen. Sci. ISSN 3006-4023*, vol. 2, no. 1, pp. 71–90, 2024.

Volume 1, Issue 1
Publisher: East Publication & Technology
DOI: https://doi.org/10.63496/ejas.Vol1.Iss1.50

[20] J. G. C. Ramírez, "Natural Language Processing Advancements: Breaking Barriers in Human-Computer Interaction," *J. Artif. Intell. Gen. Sci. ISSN 3006-4023*, vol. 3, no. 1, pp. 31–39, 2024.

[21] P. C. Harish Padmanaban and Y. K. Sharma, "Optimizing the Identification and Utilization of Open Parking Spaces Through Advanced Machine Learning," *Adv. Aer. Sens. Imaging*, pp. 267–294, 2024.

[22] H. P. PC, "Compare and analysis of existing software development lifecycle models to develop a new model using computational intelligence".

[23] N. G. Camacho, "Unlocking the Potential of AI/ML in DevSecOps: Effective Strategies and Optimal Practices," *J. Artif. Intell. Gen. Sci. ISSN 3006-4023*, vol. 3, no. 1, pp. 106–115, 2024.

[24] M. A. Bappy, M. Ahmed, and M. A. Rauf, "Exploring the Integration of Informed Machine Learning in Engineering Applications: A Comprehensive Review," *Manam Rauf, Md Abdur, Explor. Integr. Inf. Mach. Learn. Eng. Appl. A Compr. Rev. (February 19, 2024)*, 2024.

[25] M. Sarker, "Towards Precision Medicine for Cancer Patient Stratification by Classifying Cancer By Using Machine Learning," *J. Sci. Technol.*, vol. 3, no. 3, pp. 1–30, 2022.

[26] M. N. Uddin, M. A. Bappy, M. F. Rab, F. Znidi, and M. Morsy, "Recent Progress on Synthesis of 3D Graphene, Properties, and Emerging Applications," 2024.

[27] M. A. Bappy and M. Ahmed, "ASSESSMENT OF DATA COLLECTION TECHNIQUES IN MANUFACTURING AND MECHANICAL ENGINEERING THROUGH MACHINE LEARNING MODELS," *Glob. Mainstream J. Business, Econ. Dev. Proj. Manag.*, vol. 2, no. 04, pp. 15–26, 2023.

[28] S. Ness, M. Sarker, M. Volkivskyi, and N. Singh, "The Legal and Political Implications of AI Bias: An International Comparative Study," *Am. J. Comput. Eng.*, vol. 7, no. 1, pp. 37–45, 2024.

[29] J. Xu, H. Wang, Y. Zhong, L. Qin, and Q. Cheng, "Predict and Optimize Financial Services Risk Using AI-driven Technology," *Acad. J. Sci. Technol.*, vol. 10, no. 1, pp. 299–304, 2024.

[30] X. Yafei, Y. Wu, J. Song, Y. Gong, and P. Lianga, "Generative AI in Industrial Revolution: A Comprehensive Research on Transformations, Challenges, and Future Directions," *J. Knowl. Learn. Sci. Technol. ISSN 2959-6386*, vol. 3, no. 2, pp. 11–20, 2024.

[31] R. Shanthi, M. D. Babu, N. Kousika, C. Vijayaraj, S. B. Choubey, and S. Sambooranalaxmi, "Advanced Privacy-Preserving Framework Using Homomorphic Encryption and Adaptive Privacy Parameters for Scalable Big Data Analysis," *Int. J. Intell. Syst. Appl. Eng.*, vol. 12, no. 11s, pp. 160–165, 2024.

[32] M. Iezzi, "Practical Privacy-Preserving Data Science with Homomorphic Encryption: An Overview," *Proc. - 2020 IEEE Int. Conf. Big Data, Big Data 2020*, no. i, pp. 3979–3988, 2020, doi: 10.1109/BigData50022.2020.9377989.

[33] M. M. Salim, I. Kim, U. Doniyor, C. Lee, and J. H. Park, "Homomorphic encryption based privacy-preservation for IoMT," *Appl. Sci.*, vol. 11, no. 18, 2021, doi: 10.3390/app11188757.

[34] A. Maurya and M. Joshi, "Exploring Privacy-Preserving Strategies: A Comprehensive Analysis of Group-Based Anonymization and Hybrid ECC Encryption Algorithm for Effective Performance Evaluation in Data Security," *Int. J. Intell. Syst. Appl. Eng.*, vol. 12, no. 13s, pp. 517–527, 2024.

[35] N. Kaaniche and M. Laurent, "Data security and privacy preservation in cloud storage environments based on cryptographic mechanisms," *Comput. Commun.*, vol. 111, pp. 120–141, 2017, doi: 10.1016/j.comcom.2017.07.006.

[36] F. O. Catak, I. Aydin, O. Elezaj, and S. Yildirim-Yayilgan, "Practical implementation of privacy preserving clustering methods using a partially homomorphic encryption algorithm," *Electron.*, vol. 9, no. 2, 2020, doi: 10.3390/electronics9020229.

Volume 1, Issue 1
Publisher: East Publication & Technology
DOI: https://doi.org/10.63496/ejas.Vol1.Iss1.50

[37] G. Su, J. Wang, X. Xu, Y. Wang, and C. Wang, "The Utilization of Homomorphic Encryption Technology Grounded on Artificial Intelligence for Privacy Preservation," *Int. J. Comput. Sci. Inf. Technol.*, vol. 2, no. 1, pp. 52–58, 2024, doi: 10.62051/ijcsit.v2n1.07.

[38] D. Chen *et al.*, "Privacy-Preserving Encrypted Traffic Inspection with Symmetric Cryptographic Techniques in IoT," *IEEE Internet Things J.*, no. September, 2022, doi: 10.1109/JIOT.2022.3155355.

[39] P. Singh, M. Masud, M. S. Hossain, and A. Kaur, "Blockchain and homomorphic encryption-based privacy-preserving data aggregation model in smart grid," *Comput. Electr. Eng.*, vol. 93, no. September 2020, p. 107209, 2021, doi: 10.1016/j.compeleceng.2021.107209.

[40] A. Mondal and R. T. Goswami, "Enhanced Honeypot cryptographic scheme and privacy preservation for an effective prediction in cloud security," *Microprocess. Microsyst.*, vol. 81, 2021, doi: 10.1016/j.micpro.2020.103719.