Find out the innovative techniques of data sharing using cryptography by systematic literature review

Anik Sen [a, *], Rasel Ahmed [a, *], Samiha Hossain [a], Sazzad Hossain Tasnim [a, *], Tanvir Ahmed [a]

[a] Faculty of Science & Technology, American International University-Bangladesh, AIUB, 408/1, Kuratoli, Khilkhet, Dhaka 1229, Bangladesh.

Corresponding author email: aniksen360@gmail.com; raselahmed1337@gmail.com; sazzadaiub1@gmail.com

Author email: hsamiha2020@gmail.com; tanvir.ahmed@aiub.edu

Abstract: Secure data sharing is crucial for protecting sensitive information, and the use of cryptographic protocols, such as the Secure Shell (SSH) protocol, provides an efficient way to achieve this. Found a novel proposed authentication system that combines cryptography and machine learning techniques to ensure secure data sharing within a federated cloud services environment. Their approach involves mutual authentication to establish trust between cooperating entities, threat detection using machine learning algorithms, and cryptography-based key agreement for secure data exchange. They evaluated different classifiers and found that LR, KNN, and DT achieved higher accuracy in malware prediction. Founded another approach where a data-sharing scheme for cloud storage that emphasizes security and efficiency. They introduced a secure cloud storage model utilizing a semi-trusted third party (STTP) for user management, key management, and data processing. By combining a hybrid encryption scheme with a re-encryption protocol, they ensured data confidentiality, unforgeability, and user-centricity. These studies highlight the importance of cryptography in secure data sharing and propose innovative techniques to enhance security and efficiency in data sharing.

Keywords: cryptography, secure data, SSH, efficient way, cryptography.

1. Introduction

The emergence of the smart grid has brought about significant advancements in information digitization. However, it has also given rise to crucial concerns regarding security and privacy [26]. These concerns encompass various issues such as the absence of shared authentication among communicating parties, the potential for multiple cyber-attacks, unauthorized access to services, and the disclosure of confidential information to unauthorized entities. Therefore, before granting access to individuals, whether they are computers or people, it is essential to verify their identity and validate permission and control policies based on their identification. User identity is validated through digital signatures, while authorization ensures that the person has the necessary authority to access shared resources [27].

Data transmission and communication always require encryption [28]. The use of encryption and decryption is critical in maintaining information security as data transmission and reception are vulnerable to external attacks. To enhance security, data is converted into encoded messages through encryption and then restored to its original form through decryption [29]. Several cryptographic algorithms have been proposed to ensure secure data transmission and information sharing. These algorithms can be categorized as either symmetric or asymmetric cryptographic techniques [30].

A digital signature, generated through a cryptographic process, device, or electronic record, serves as a means to validate the authenticity and legality of a message. Unlike a digital certificate, a digital signature serves as a digital counterpart to a handwritten signature or a stamped seal, offering enhanced protection against interference and spoofing in communication networks. Digital signatures provide additional assurances regarding the source, integrity, and location of an electronic document, activity, or communication, while also confirming the signer's authorization. These signatures are part of digital signature technologies that employ keys and encryption algorithms to sign documents [31].

Furthermore, this study aims to identify efficient methods of data sharing through cryptography using a systematic literature review (SLR).).

2. Machine Learning Based Authentication for Secure Data-Sharing

Singh and Saxena, (2022) worked on an authentication system utilizing cryptography and machine learning is employed to ensure secure data-sharing within a federated cloud services environment. They told that Mutual authentication that ensures security is an essential necessity when it comes to exchanging priceless organizational data among cooperating entities within a federated cloud setting. This study introduces an improved mutual authentication protocol by combining cryptography and machine learning techniques at a trusted cloud server, aiming to overcome limitations in online data sharing. The proposed approach involves proper registration, threat detection using machine learning and cryptography-based key agreement for secure data exchange during session establishment and password change. Among the various classifiers used, SVM showed the lowest performance, while LR, KNN, and DT achieved higher accuracy, with DT outperforming SVM, KNN, and LR in malware prediction by 1–1.5%; the ensemble classifier, Random Forest or Bagging Classifier, demonstrated an equivalent accuracy of 99.61% as reported by the Voting Classifier combining LR and KNN. The limitation is that their focus was exclusively on online data sharing within a multi-cloud environment [1].

3. Secure and efficient data sharing

Luo et al, 2019 researched a data-sharing scheme for cloud storage that focuses on security and efficiency. The scheme is built upon c hybrid encryption. They said that people are becoming more worried about security issues like data confidentiality and user privacy because they don't fully trust cloud service providers. Their aim to propose a secure cloud storage model utilizing a semi-trusted third party (STTP) for user managertificatesment, key management, and data processing. It also aims to introduce a low-computation certificate-less hybrid encryption scheme and develop a simplified key derivation method through partial iteration to enhance user key management. They created a secure data sharing scheme by combining the suggested CL-HSC scheme and a re-encryption protocol, ensuring that it meets the requirements of confidentiality, unforgeability, and user-centricity. The result is a comprehensive solution for securely sharing data. One limitation to address is the secure sharing of data with multiple recipients [2].

4. Secure data by secure shell protocol

Kumar (2015) presented an encrypted data-sharing methodology for a cloud environment following a decentralized way to prevent various types of cyberattacks. the author made some assumptions in this paper which is users can only read/write data, not anyone else or not even cloud administrators. All sorts of communication between users and the cloud will be secured by secure shell protocol(SSH). The author also used Bilinear pairings on elliptic curves and also Bilinear pairing on elliptic curves groups are used because it determines the complexity of pairing operations. The author mentioned the future work which will be on authenticating or verifying the users without revealing who they are to protect the privacy. [11].

5. Various ways of data sharing

Adee and Mouratidis, (2022) conducted their research on developing a Dynamic Four-Step Data Security Model for data in cloud computing, which relies on the integration of cryptography and steganography. They said that cloud computing is a field that is growing quickly. It enables users to easily utilize computer system resources, such as data storage and computational power, without having to handle them directly. The main objective of this research paper is to improve the level of data security and privacy in cloud computing environments. The goal is to address various security and privacy concerns that exist in cloud computing, such as data loss, data manipulation, and data theft. Through this study, the aim is to accomplish the following objectives. A dynamic four-step model was created to secure cloud data. It combines hybrid encryption, LSB steganography, and identity-based encryption. Users can back up decryption results, and minimizing picture distortion increases data concealment in images. Their limitation lies in the need for further research in order to enhance the integration and ensure enhanced security measures for multimedia data [3].

Xie et al., 2023 developed an enhanced attribute access control scheme that utilizes blockchain technology and elliptic curve cryptography. This scheme is designed to facilitate efficient and secure data sharing among multiple authorities. They mentioned, the pressing need to securely and effectively share data among various Internet of Things enterprises is growing more crucial due to the swift advancements in Internet of Things technology. The aim of this paper is to utilize IPFS as a distributed storage platform to address the issues of privacy leakage, single point of failure, and repeated storage found in centralized storage. Additionally, the paper proposes a data sharing scheme based on consortium blockchain and improved attribute encryption to enhance distribution and transparency in the sharing process. Furthermore, the adoption of the ECC-improved MA-CPABE encryption

algorithm resolves the problem of centralized attribute distribution and reduces the time and resource consumption in encryption and decryption. Finally, the use of Hyperledger Fabric chaincode technology enables data upload, query, and access, restricting access to privacy information only to users who meet the data owner's access control conditions. This paper presents a Fabric blockchain-based scheme for multi-authority attribute access control, enhancing traditional data sharing with secure storage, distributed access control, and transparency. Experimental results demonstrate improved performance, security, and practicality compared to other approaches. Their limitation lies in effectively implementing and maintaining efficient and secure access control policies and dynamic update mechanisms for attribute authentication in blockchain-based data sharing schemes [4].

Adeniyi et al., 2022 explored the utilization of RSA and ElGamal cryptographic algorithms combined with hash functions to ensure secure sharing of sensitive data. They said that with the rise of connected devices, the amount of transmitted data is increasing day by day. This has given rise to new challenges in terms of information security, such as unauthorized access to users' credentials and sensitive information. This study aims to implement RSA and ElGamal cryptographic algorithms using hash functions for security and integrity. Additionally, it seeks to establish data integrity in cryptographic procedures through sender and receiver validation. The study's outcomes will benefit the control of cryptographic operations between the sender and receiver. This study addresses security concerns in distributed data by focusing on encryption/decryption for data protection. It examines RSA and ElGamal algorithms for enhancing information security and implements the SHA-256 hash function for data integrity. The approach ensures security and control over users' sensitive data, making it suitable for secure data sharing systems. One limitation of the study is that while it emphasizes the importance of encryption/decryption and the use of RSA and ElGamal algorithms for information security, it does not specifically address the implementation of secure submission, storage, and extraction operations for maximum protection of sensitive data in the sharing system.One limitation of the study is that while it emphasizes the importance of encryption/decryption and the use of RSA and ElGamal algorithms for information security, it does not specifically address the implementation of secure submission, storage, and extraction operations for maximum protection of sensitive data in the sharing system [5].

Rana et al.,2022 conducted a survey on lightweight cryptography in IoT networks. They said that with the arrival of cutting-edge technology, the Internet of Things has enabled the linking of countless devices capable of gathering immense amounts of data. This paper explores recent advancements in lightweight cryptography (2019-2020) and conducts a comparative analysis of state-of-the-art algorithms. It evaluates protocols based on factors like block size, key length, gate area, technology value, encryptions/decryptions, latency, and throughput, highlighting the requirements for lightweight cryptography ciphers. Their result indicates that two types of algorithms were discovered based on the key arrangement: symmetric and asymmetric cryptography. Currently, commonly used symmetric algorithms in IoT security are block ciphers and stream ciphers. However, these algorithms are not suitable for effectively securing communications in IoT systems with limited resources. The security problem is a crucial concern for IoT and has not been adequately tackled in current network protection research. Therefore, there is a need to develop a lightweight cryptographic algorithm specifically designed to secure resource-constrained IoT architecture. The increasing patterns of attacks on IoT networks necessitate research focused on enhancing lightweight ciphers. Limitations of current research include the need for reducing the size of encryption keys, exploring the use of more commonly occurring dynamic keys, decreasing the block size, simplifying the rounds involved, and creating uncomplicated key schedules for the development of lightweight block ciphers. Additionally, future efforts should prioritize the optimization of the internal state, minimization of key size, and effective initialization of vectors when designing lightweight stream ciphers[6].

Song et al.,2011 proposed a novel communication protocol that seamlessly integrates steganography and cryptography methods, ensuring enhanced security. They carried out research on a new approach that combines steganography and cryptography, enabling encryption and concealment simultaneously. The method proposed is based on the widely-used LSB matching technique in steganography and employs Boolean functions commonly used in cryptography. This protocol offers ease of implementation and requires less computational effort compared to previous methods while maintaining a high level of security. The proposed secure communication protocol is limited to grayscale images and lacks compatibility with colored images. It relies on specific steganography and cryptography techniques, limiting its flexibility with other methods. The protocol claims simultaneous encryption and hiding but lacks detailed information on computational efficiency and visual quality preservation. Additionally, its robustness against advanced steganalysis techniques is uncertain due to the lack of supporting evidence or experimentation results[7].

Upadhyaya, S. (2015) focuses on data security in WSNs. DNA cryptography is utilized for secure communication and computation. The paper proposes an algorithm that combines DNA cryptography with SSL for secure

information exchange in wireless sensor networks. They suggested a method that involves utilizing DNA cryptography alongside a secure socket layer (SSL) to establish a highly secure channel for exchanging information during communication and data transmission. The SSL protocol incorporates the DNA concept for encryption, providing three levels of security in WSN. Their proposed system assigns key pairs and digital certificates before deploying sensor nodes, addressing the energy consumption issue. Public key and certificate sharing is done securely via SSL, reducing computation overhead and improving energy efficiency. Promising results are anticipated, and implementation of the algorithm for encryption and decryption is underway. One potential limitation of the proposed system is that assigning key pairs and digital certificates before deploying sensor nodes may introduce security risks if the keys or certificates are compromised during deployment. Additionally, the use of SSL for public key and certificate sharing may introduce additional computational overhead on the network. The effectiveness of the solution in reducing energy consumption and computation time will also depend on the specific hardware and network capabilities of the sensor nodes. Further evaluation and testing are necessary to assess the overall performance and scalability of the system[8].

Rahmani et al.,2023 worked on creating Encryption as a Service (EaaS) to serve as an effective remedy for cryptography concerns within cloud environments. They have been engaged in the exploration of efficient utilization of computing resources to minimize expenses while processing extensive data. The demand for a network of shared resources over a large geographical area, offering scalability, substantial computational power, and the ability to store data on location-independent storage systems, has given rise to the emergence of cloud computing. Their objective is to demonstrate that by combining control and management of cryptography, EaaS can address the issues related to client and server-side encryption and also reduce operational expenses.[9]

Senapati et al.,(2023) worked on the implementation of quantum communication featuring RLP quantum resistant cryptography within the realm of industrial manufacturing. The main focus of this paper is to demonstrate the successful application of quantum theory in achieving secure data transfer between industrial production facilities, specifically in highly restricted areas such as Air and Defense production units. It showcases the optimal results obtained from utilizing quantum communication in the context of industrial manufacturing. They worked on to explore how advanced technologies, digital twins, and quantum cryptography can be utilized in industrial operations to safeguard smart factories, data centers, shop floors, and other manufacturing facilities. In today's digital era, the success of enterprise businesses heavily relies on the implementation of smart technologies such as AI, ML, quantum computing, sensors, IIoT, edge technologies, 5G, and the SAP S/4HANA cloud database. Protecting operational data, information, and security in manufacturing is of utmost importance for achieving a prosperous enterprise.The establishment of a secure communication path between the source and target in a quantum computer poses numerous limitations. Challenges arise in the communication network for quantum key distribution (QKD) due to limitations in secreting key rate (SKR), distance size, timeline, costs, and the security of information transmission from the source to the destination. Notable limitations in implementing QKD involve hardware constraints, key rates, and cost factors. The outcome of this study explored different elements of quantum communication and information theory, including quantum cryptography and various protocols related to quantum key distribution (QKD). Such advancements have the potential to enhance production efficiencies in industrial manufacturing and optimize the implementation of digital transformation strategies in the context of Industry 4.0 [10].

Mahendra et al. (2022) used Novel Data Authentication in the cloud service to provide more security and to get the trust from the users without compromising information. The author performed a plan with some sample against cipher attack to ensure the security to achieve less encryption time. According to the author, the proposed algorithm which is blowfish algorithm that takes less time to encrypt data than the data encryption standard process. The authors also provided the standard error mean value of both such as for blowfish algorithm is .01733 and for data encryption standard is .03005[12].

Gupta et al. (2023) analyzed about since the number of online social platforms are increasing along with the amount of users and also the scale of storing information also increases. so, its challenging to sharing individual user data to others. The author proposed two approaches in this paper, one of them was securely sharing one user data to other users without compromising privacy and another approach was any user can allow specific accounts to share their data without providing any credintials for certain times. The author said that the proposed techniques is diff than the existing one which is on online website and also said that its possible to accomplish goal if the session auth saving process and cryptography encryption algorithm integrate together to share user data [13].

Vat et al., (2022) wanted to build a technique to increase the security for storing data in the cloud using threshold cryptography and encryption. the authors proposed a technique with the concept of threshold cryptography to

secure the data before uploading into cloud storage with modified version of RSA algorithm and RSA algorithm helps to split up the key and store them into diff places to enhance the security of the data. The authors also built an application to securely store their data to the cloud [14].

Al-Hyari et al. (2022) proposed the most efficient and secure way to store digital color images(CASDC) using a special key which makes it difficult for hackers. The authors compared the proposed algorithm with other standard algorithms which is Data Encryption Standard (DES), Tripple-DES (3DES), Advanced Encryption Standard (AES), and Blow Fish (BF), and the author showed the efficiency of that algorithm. The proposed technique bring-down the encryption and decryption time where time complexity is O(N). The authors also showed the practical result that it will take hundreds of years or nearly impossible to break the security of CASDC through hacking [15].

Alemami et al. (2023) analyzed various types of encryption algorithms such as Advanced Encryption Algorithm (AES),data encryption standard (DES), Blowfish, Rivest-Shamir-Adleman (RSA) encryption, and international data encryption algorithm (IDEA). The authors also compared all the algorithms based on the analyzed result. According to the authors' result, RSA and IDEA algorithms are less effective in terms of encipherment and less secure than other algorithm and also AES is more effective for vast amount of data. The authors also encouraged to use of hybrid algorithms to get more security [16].

Yadav and Tiwari, (2023) proposed broadcast encryption than an ARIBBE cryptosystem mechanism based on a public key framework using a type-I bi-linear map. According to the authors, with the proposed encryption system the provider can provide multimedia data to the specific user. Any revoked users won't be able to get those data. the Author also detailed the anonymity of the broadcast encryption feature which will hide the users and also the proposed encryption will help the users from IND-ID-CPA attacks [17].

Yadav & Tiwari, (2023) proposed a scheme using cryptographic broadcast encryption with a personalized message system to securely share the user data in another paper. The authors used Shamir's secret sharing scheme to increase the security of the data and the secret value only shared with the shareholders and also the scheme is Asymmetric pairings whereas others are symmetric pairings. Fixed decryption key also bring down the channel requirement which helps to improve the performance. The author mentioned about the limitation which is reducing the size of public parameter and building traitor tracing sytem for the proposed scheme [18].

Yadav & Tiwari, (2023) again proposed a secure data sharing technique with shorter ciphertext in public key setting using asymmetric (Type-III) pairings which is more effective and efficient than all other pairings in terms of security. the author also compared the standard broadcast encryption system with multichannel broadcast encryption system where is standard broadcast encryption is not efficient but multichannel broadcast encryption allow to securely share data from diff users to diff set of legitimate users. the proposed method require less storage, better performance and also minimum cost compare to existed methods [19].

Sabitha & Rajasree (2021) analyzed on-demand access control for flexible data sharing between random users. The authors proposed a hierarchical attribute-based access control scheme to fulfill the limitation of Attribute-Based Encryption(ABE) and also securely share data in the cloud storage. The proposed method provides multilevel and tunable access control over the flexible and sharing data. According to the authors, it's lower the communication cost and also enhanced the performance. The proposed methods give more control to the data owner over their data and also provide control over the individual or group of users. The author mentioned about the limitation of Attribute-Based Encryption (ABE) [20]. Hidayat & Mahardiko, (2020) proposed Advanced Encryption System (AES) encryption algorithm to enhanced the security of the user's data during data sharing from the hackers. The authors compared the past studies with the recent studies where past studies were more focused on data storage but recent studies focused on the security during data sharing. The author mentioned that future research can done by a systematic literature review (SLR) to get better suggestions about AES cloud computing. [21].

Anguraj (2022) used Trusted Execution Environments (TEEs) and relevent cryptographic methods to securely store and process data. The authors proposed a framework which is intregrted by Advanced encryption system (AES) and intel Software Guard Extensions (SGX). So, whenever the data pass through SGX, it will be in an encrypted format and also AES cryptographic technique provides end to end encryption. The authors proposed framework will prevent the hackers to capture the users data. Data from real users and simulated IOT devices used to determine the performance of the proposed framework. The authors mentioned that from the proposed framework they couldn't get the notable performance except improvement of data security. [22].

Kamil et al, 2021 used cryptographic protocols to share data between system components and validation system and also used System Usability Scale (SUS) to validate the real user data to prevent fraud during blockchain based e-voting. According to authors if the SUS score is 90 then the vote will be accepted. The technique will help to conduct election during pendamic situation specialy covid-19 and Multichain method used to store vast amount of e-voting data. Current information and Past information are stored to generate new blocks which will continue to avoid duplication or conflict. [23].

The another authors proposed a new hybrid data protection and confidentiality technique that utilizes the ECC and Blowfish algorithms to address the limitations of traditional symmetric and asymmetric encryption methods, thereby ensuring high levels of data transfer and storage security in the cloud computing environment [27].

6. Objective Of The Study

- To find out the innovative techniques of data sharing using cryptography by systematic literature review.

7. Methodology

Mahendra and Prabha (2022) observed the data but not measured it. On the other hand, (Alemami et al.,2023) measured data to show efficiency and effectiveness. Mahendra and Prabha (2022) described diff encryption algorithms which are qualitative but (Alemami et al.,2023) analyzed with numbers that are quantitative. Mahendra and Prabha (2022) deal with subjective data whereas (Alemami et al.,2023) deal with statistical data [25,26]. Hossen et al., 2023 also use systematic literature review for their research purposes because they also use quantitative data as their research purposes [24].

7.1. Paper selection

We search papers using systematic search. We search papers on various websites. The figure below represented our search method.

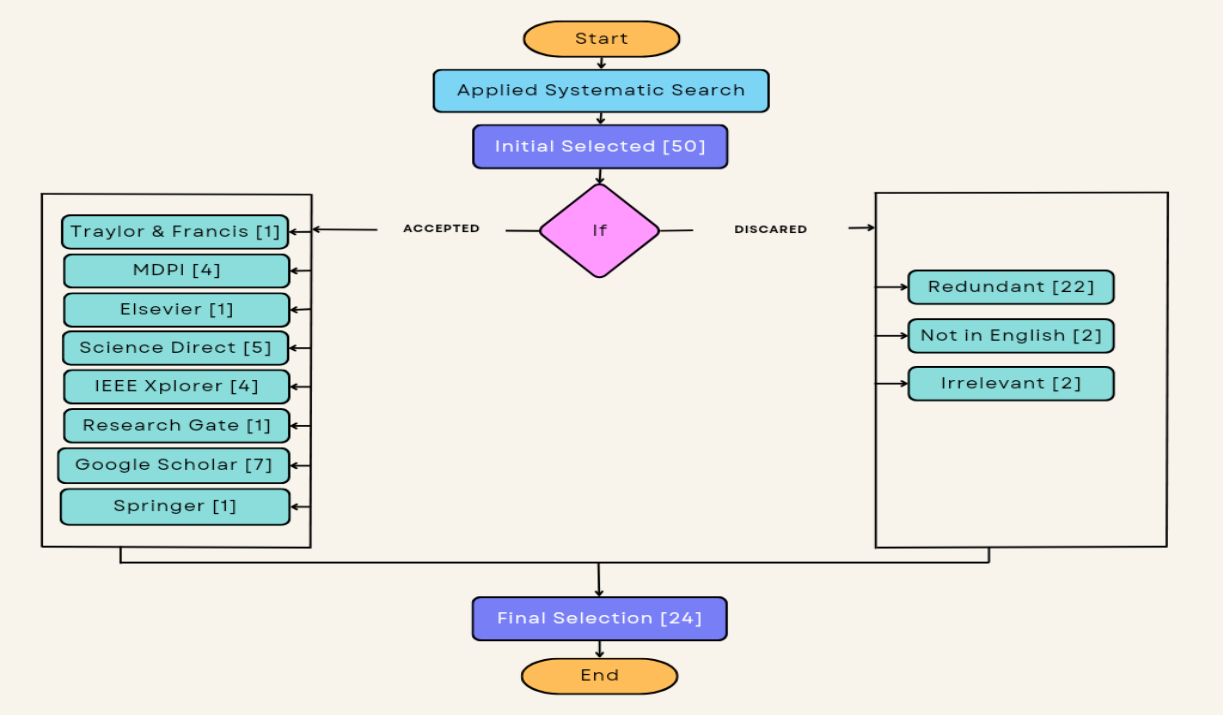

Figure.1 Use Prisma guidelines for paper selection.

8. Result

Extracted Information	Citation
Voting Classifier combining LR and KNN where accuracy is 99.61%	Singh et al., 2022 [1]
Suggested CL-HSC scheme and a re-encryption protocol	Luo & Ma, 2019 [2]
Hybrid encryption, LSB steganography, and	Adee & Mouratidis, 2022 [3]

identity-based encryption	
Presents a Fabric blockchain-based scheme for multi-authority attribute access control, enhancing traditional data sharing with secure storage, distributed access control, and transparency	Xie et al., 2023[4]
Examines RSA and ElGamal algorithms for enhancing information security and implements the SHA-256 hash function for data integrity	Adeniyi et al, 2022[5]
Result indicates that two types of algorithms were discovered based on key arrangement: symmetric and asymmetric cryptography. Currently, commonly used symmetric algorithms in IoT security are block ciphers and stream ciphers	Rana et al., 2022[6]
Used LSB matching technique in steganography and employs Boolean functions commonly used in cryptography	Song et al., 2011[7]
Suggested a method that involves utilizing DNA cryptography alongside a secure socket layer (SSL) to establish a highly secure channel for exchanging information during communication and data transmission	Upadhyaya, S. (2015) [8]
Serve as an effective remedy for cryptography concerns within cloud environments	Rahmani et al., 2013[9]
Worked on the implementation of quantum communication featuring RLP quantum-resistant cryptography within the realm of industrial manufacturing	Senapati et al., 2023 [10]
Used secure shell protocol (SSH).	Kumar, 2015 [11]
Secure shell protocol(SSH) is used	Mahendra, 2022 [12]
Proposed algorithm which is blowfish algorithm	Gupta et al., 2023 [13]
Proposed two approaches in this paper, one of them was securely sharing one user's data to other users without compromising privacy and another approach was any user can allow specific accounts to share their data without providing any credintials for certain times	Vats et al., 2022 [14]
Used RSA algorihtm	Al-Hyari et al., 2022 [15]
Proposes algorithm with other standard algorithms which is Data Encryption Standard (DES), Tripple-DES (3DES), Advanced Encryption Standard (AES), and Blow Fish (BF) and the author showed the effeciency of that algorithm.	Alemami et al., 2023[16]
Proposed encryption system the provider can provide their multimedia data with the specific user	Yadav and Tiwari, (2023) [17]
Proposed boardcast encryption then a ARIBBE cryptosystem mechanism based on a public key framework using type-I bi-linear map	Yadav, & Tiwari, (2023) [18]
Proposed a scheme using cryptographic broadcast encryption with personalised message system to securely share the user data	Yadav, & Tiwari, (2023) [19]
Again proposed a secure data sharing technique with shorter ciphertext in public key setting using asymmetric (Type-III) pairings which is more effective and efficient than all other pairings in terms of security	Sabitha & Rajasree, (2021) [20]
Proposed a hierarchical attribute-based access control scheme to fulfill the limitation of Attribute-Based Encryption(ABE) and also securely share data in the cloud storage	Hidayat & Mahardiko,2020 [21]

Advanced Encryption System (AES) encryption algorithm to enhanced the security of the users data during data sharing from the hackers.	Anguraj, (2022) [22]
Proposed a framework which is intregrted by Advanced encryption system (AES) and intel Software Guard Extensions (SGX). So, whenever the data pass through SGX, it will be in an encrypted format and also AES cryptographic technique provides end to end encryption.	Kamil et al., 2021 [23]
Proposed a new hybrid data protection and confidentiality technique that utilizes the ECC and Blowfish algorithms	Buvana, 2021 [25]

9. Conclusion

The study is actually analyzed in this study and highlights the significance of cryptography in ensuring secure data sharing and access over various platforms, including federated cloud services, cloud storage, IoT networks, and online social platforms. These papers propose different approaches to enhance security and efficiency through the integration of machine learning, steganography, blockchain technology, lightweight cryptography, DNA cryptography, threshold cryptography, and encryption algorithms like RSA and Blowfish. While each paper addresses specific limitations and challenges in data sharing, they collectively contribute to the development of robust encryption techniques and protocols. Further research is needed to optimize key management, address scalability issues, and explore the integration of different cryptographic methods to ensure maximum security and privacy in data-sharing systems.

References

[1] Singh, A. K., & Saxena, D. (2022). A cryptography and machine learning based authentication for secure data-sharing in federated cloud services environment. *Journal of Applied Security Research*, *17*(3), 385-412.
[2] Luo, W., & Ma, W. (2019). Secure and efficient data sharing scheme based on certificates hybrid encryption for cloud storage. *Electronics*, *8*(5), 590.
[3] Adee, R., & Mouratidis, H. (2022). A dynamic four-step data security model for data in cloud computing based on cryptography and steganography. *Sensors*, *22*(3), 1109.
[4] Xie, B., Zhou, Y. P., Yi, X. Y., & Wang, C. Y. (2023). An Improved Multi-Authority Attribute Access Control Scheme Base on Blockchain and Elliptic Curve for Efficient and Secure Data Sharing. *Electronics*, *12*(7), 1691.
[5] Adeniyi, E. A., Falola, P. B., Maashi, M. S., Aljebreen, M., & Bharany, S. (2022). Secure sensitive data sharing using RSA and ElGamal cryptographic algorithms with hash functions. *Information*, *13*(10), 442.
[6] Rana, M., Mamun, Q., & Islam, R. (2022). Lightweight cryptography in IoT networks: A survey. *Future Generation Computer Systems*, *129*, 77-89.
[7] Song, S., Zhang, J., Liao, X., Du, J., & Wen, Q. (2011). A novel secure communication protocol combining steganography and cryptography. *Procedia Engineering*, *15*, 2767-2772.
[8] Upadhyaya, S. (2015). Secure communication using DNA cryptography with secure socket layer (SSL) protocol in wireless sensor networks. *Procedia Computer Science*, *70*, 808-813.
[9] Rahmani, H., Sundararajan, E., Ali, Z. M., & Zin, A. M. (2013). Encryption as a Service (EaaS) as a Solution for Cryptography in Cloud. *Procedia Technology*, *11*, 1202-1210.
[10] Senapati, B., & Rawal, B. S. (2023). Quantum Communication with RLP Quantum Resistant Cryptography In Industrial Manufacturing. *Cyber Security and Applications*, 100019.
[11] Kumar, S. N. (2015). Cryptography during data sharing and accessing over cloud. *International Transaction of Electrical and Computer Engineers System*, *3*(1), 12-18.
[12] Mahendra, M., & Prabha, P. S. (2022, April). Classification of security levels to enhance the data sharing transmissions using blowfish algorithm in comparison with data encryption standard. In *2022 International Conference on Sustainable Computing and Data Communication Systems (ICSCDS)* (pp. 1154-1160). IEEE.
[13] Gupta, K. M., Reddy, K. S., Vineeth, L., Kumar, R. L., & Suryanarayana, G. (2023, February). Peer to Peer Credentials Sharing using RSA and Session Token Techniques. In *2023 7th International Conference on Computing Methodologies and Communication (ICCMC)* (pp. 1101-1105). IEEE.
[14] Vats, A., Jimmy, P., Mishra, A., & Aju, D. (2022, October). LockNKey: Improvised Cloud Storage System using Threshold Cryptography Approach. In *2022 2nd International Conference on Emerging Smart Technologies and Applications (eSmarTA)* (pp. 1-6). IEEE.

[15] Al-Hyari, A., Al-Taharwa, I., Al-Ahmad, B., & Alqadi, Z. (2022). CASDC: A Cryptographically Secure Data System Based on Two Private Key Images. IEEE Access, 10, 126304-126314. doi: 10.1109/ACCESS.2022.3226319.

[16] Alemami, Y., Al-Ghonmein, A. M., Al-Moghrabi, K. G., & Mohamed, M. A. (2023). Cloud data security and various cryptographic algorithms. *International Journal of Electrical and Computer Engineering*, *13*(2), 1867.

[17] Yadav, S., & Tiwari, N. (2023). Privacy preserving data sharing method for social media platforms. *PloS one*, *18*(1), e0280182.

[18] Yadav, S., & Tiwari, N. (2023). Secure and efficient online data sharing scheme using broadcast encryption with personalised message system.

[19] Yadav, S., & Tiwari, N. (2022). An Efficient and Secure Data Sharing Method Using Asymmetric Pairing with Shorter Ciphertext to Enable Rapid Learning in Healthcare. *Computational Intelligence and Neuroscience*, *2022*.

[20] Sabitha, S., & Rajasree, M. S. (2021). Multi-level on-demand access control for flexible data sharing in cloud. *Cluster Computing*, *24*(2), 1455-1478.

[21] Hidayat, T., & Mahardiko, R. (2020). A Systematic literature review method on aes algorithm for data sharing encryption on cloud computing. *International Journal of Artificial Intelligence Research*, *4*(1), 49-57.

[22] Anguraj, D. K. (2022). Advanced Encryption Standard based Secure IoT Data Transfer Model for Cloud Analytics Applications. *Journal of Information Technology and Digital World*, *4*(2), 114-124.

[23] Kamil, M., Bist, A. S., Rahardja, U., Santoso, N. P. L., & Iqbal, M. (2021). COVID-19: Implementation e-voting blockchain concept. *International Journal of Artificial Intelligence Research*, *5*(1), 25-34.

[24] Hossen, M. I., Fahad, N., Sarkar, M. R., & Rabbi, M. R. (2023). Artificial Intelligence in Agriculture: A Systematic Literature Review. *Turkish Journal of Computer and Mathematics Education (TURCOMAT)*, *14*(1), 137-146.

[25] Mahendra, M., & Prabha, P. S. (2022, April). Classification of security levels to enhance the data sharing transmissions using blowfish algorithm in comparison with data encryption standard. In *2022 International Conference on Sustainable Computing and Data Communication Systems (ICSCDS)* (pp. 1154-1160). IEEE.

[26] Alemami, Y., Al-Ghonmein, A. M., Al-Moghrabi, K. G., & Mohamed, M. A. (2023). Cloud data security and various cryptographic algorithms. *International Journal of Electrical and Computer Engineering*, *13*(2), 1867.

[27] Buvana, M. (2021). Optimize Cryptography Algorithm for Efficient Data Security on Cloud Computing. *Turkish Journal of Computer and Mathematics Education (TURCOMAT)*, *12*(1S), 459-464.

[28] Gunduz, M. Z., & Das, R. (2020). Cyber-security on smart grid: Threats and potential solutions. *Computer networks*, *169*, 107094.

[29] Saxena, N., Choi, B. J., & Lu, R. (2015). Authentication and authorization scheme for various user roles and devices in smart grid. *IEEE transactions on Information forensics and security*, *11*(5), 907-921.

[30] Misbha, A., Baswal, K., Simha, M. N., Abujam, R., & CM, S. (2017). GUPTDOC AN ENTERPRISE PORTAL FOR CRYPTING WITH AES. *Int. Res. J. Eng. Technol*, *4*, 1309-1311.

[31] Emmanuel, A. A., Okeyinka, A. E., Adebiyi, M. O., & Asani, E. O. (2021). A note on time and space complexity of rSA and ElGamal cryptographic algorithms. *International Journal of Advanced Computer Science and Applications*, *12*(7).

[32] Chandra, S., Paira, S., Alam, S. S., & Sanyal, G. (2014, November). A comparative survey of symmetric and asymmetric key cryptography. In *2014 international conference on electronics, communication and computational engineering (ICECCE)* (pp. 83-93). IEEE.

[33] Sejfuli-Ramadani, N. (2017). The Role and the Impact of Digital Certificate and Digital Signature in Improving Security During Data Transmittion. *European Journal of Sustainable Development Research*, *2*(1), 116-120.

.