Data Security in Cloud Environment Using Cryptography Technique for End-to-End Encryption

Akash Badhan, *Hitesh* Vasudev*, *Dhiraj* Kapila, *Himanshu*

School of Computer Science and Engineering, Lovely Professional University, Phagwara 144411, India

**Corresponding author: hiteshvasudev@yahoo.in*

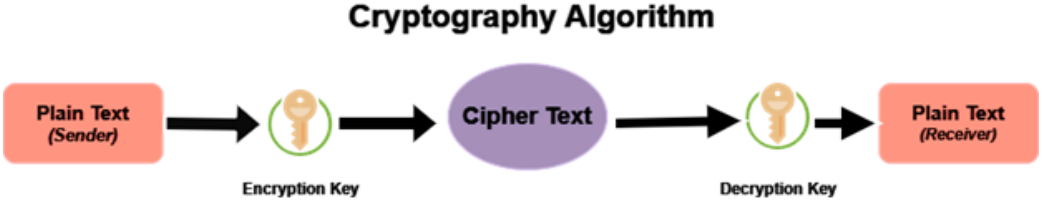
Abstract. In the modern era, data security becomes the major issue as million or trillion of data in units is being generated to cloud with every moment of time. Here the main role of cloud is to provide virtual storage for storing information or we can say it works as transmission medium for wireless data communication. So, it is very important to choose our cloud platform wisely as data is never secured while it is over cloud or in transmission medium. So, study is helping to understand the impact of data security over cloud platform, and we are reviewing the existing techniques that have been implemented by other researchers to provide encrypted communication when cloud is intermediate between sender and receiver.

Keywords: Data Security, Cloud, Cryptography, End-to-end Encryption, Network Security etc.

1. Introduction

This proposed paper shows the review study of data security techniques that could be applied to encrypt communication when it is being transferred through any cloud platform. The key aspect of data security is to provide end-to-end encryption between sender and receiver end. There are various techniques or algorithms that could be used to provide end-to-end encryption. But this study is mainly focused on cryptography techniques that could be applied to our data to maintain its confidentiality over cloud storage platforms as well. With this revolution in recent times having witnessed cloud computing as the most dynamic way to store, process and retrieve data, this striking shift in paradigms is inevitable. Cloud computing has distinct advantages including the ultimate flexibility, scalability, and the ability to be accessed by individuals to organizations. On the upside, the users have the ability to choose just how much privacy they sacrifice for convenience, and that varies from individual to individual. On the other hand, there is a security breach to your data. Cloud computing platform security poses a real challenge due to the fact that such kind of platform can be exposed to a bulk of security problems that include password theft and malicious acts. The traditional well-established security tools including firewall and access control, therefore, may not guarantee data security since data may be transmitted over the networks resides on the remote servers. Besides encryption, which has recently emerged to be a very popular means of data security in E2EE, cannot be ignored as another important strategy that can reinforce data security in the cloud. However, we have to highlight that the feature of E2EE is that the data is always encrypted from the beginning of the data's existence (starting from the moment when the data has been generated) until the data reaches its final destination- third parties are not able to look through this data at any stage of its lifecycle. In cryptography the sender sends information through any transmission medium like cloud. But information does not travel in its actual form. The information is converted to encrypted text with some key and cryptographic algorithms, and it is not in normal readable format. So, the chances of data breach are very less. In technical terms we call this encrypted text cipher text. Then cipher text is received by the receiver then it is decrypted back to its actual form of information by secret key i.e., private among authorized people only. Thus, cryptography helps to maintain confidentiality of our data. The block diagram of cryptography is shown in Figure 1, which shows that encrypted communication takes place in between sender and receiver over a network with encrypted text. [1-7]

FIG 1. Cryptography Algorithm Block Structure



as the latest technology tool for enabling E2EE, has the most important individual in cryptography. The digital signature and management of keys along with storing data in a more clever way are the tasks that can be tightened and loosened using cryptographic techniques, such as symmetric and asymmetric encryption. These approaches are designed to achieve confidentiality, integrity, and authenticity simultaneously. These procedures offer a multiple authorization deal and the same key saved for each party involved in data encryption being seen only by the right persons who have the right key, therefore, giving safety from theft of data and unauthorized access. The paper intends to examine the significance of data security in the cloud environment and machine identity verification architecture patterns that are now elevated, therefore reducing security risks. The second part will examine the majority of the cryptographic techniques and algorithms and assess their implementation in cloud by cloud securing the end-to-end encryption which is indicative of security strengths, vulnerabilities, and overall suitability for different cloud applications and cases. Also, the paper will elaborate on the difficulties and challenges surrounding the implementation of cryptographic mechanism in the cloud based on the key management, performance overhead and compliance with the respective regulatory requirements. It will investigate advancing trends and new technologies in cloud security and cryptography - including holomorphic encryption and quantum-resistant methods - and how they could influence the level of data protection in the cloud service in the future. Summing up, the purpose of this study is to explore the capabilities of cryptography to better safeguard data in the cloud, owing to a wide range of E2EE applications. Due to the grasp of the concepts and practices of cryptographic procedures, institutions can therefore cement data security in the cloud and neutralize the challenges that come with the upgrading cybercriminals.

Year	Author	Proposed Work	Research Gap
2017	Mamta et al. [6]	The study represents a review of using cryptography with genetic algorithm (GA) for data security. As per researchers they have introduced visual cryptography and used GA for encryption.	The genetic algorithm encryption now a days vulnerable to known Plaintext attacks.
2019	Jian Shen et al. [7]	The research proposed the idea of secure group data sharing in cloud computing by using the block design based key agreement. This method can be helpful even for outsourced data in cloud and provides better confidentiality level to data over cloud.	The research is carried out in much complex manner difficult to understand and flow chart for proposed study is also missing which could help people more about getting the idea of research.
2020	Anuj Kumar et al. [8]	The work was proposed securing the data over cloud for IoT models by implementing hybrid cryptography approach i.e., (RSA + DES).	RSA keys can be 1024 or 2048 bits long while DES key size is fixed to 56 bits so making them vulnerable to modern attacks such as brute force attack.
2021	Anuj Kumar [9]	This study focuses on data security by using HMAC and DNA cryptography. HMAC is good for both data integrity and authentication as well.	In HMAC technique non-repudiation is an issue due to shared key nature. Practical implementation of DNA crypto is much complex and difficult.
2021	Anuj Kumar [10]	The next study by Mr. Anuj, used DNA crypto and AES for securing data in cloud computing.	The practical implementation of DNA crypto is very challenging as require a lot of expertise.
2022	R.S. Shukla [11]	The study proposed on the topic of safeguarding secret data when it is shared over cloud or third-party platforms. Implemented DES Algorithm in MATLAB to encrypt data.	Simple cryptography algorithms are not sufficient now. It could be a hybrid approach. The size compression might also be integrated to crypto for reducing the cloud storage usage.
2023	M. Kaur et al. [12]	The proposed research shows data security over cloud using hybrid cryptographic algorithms. The researchers have implemented hybrid RSA-DES.	DES has fixed key size of 56 bits, so it limits the strength of encryption.
2024	I.Sudha et al. [13]	The study proposed a way to secure data in cloud using ECC algorithm of cryptography. The research shows that	ECC was designed for key generation so it can perform much better in hybrid approach

		ECC provides better security with small key size as compared to RSA	than individually.

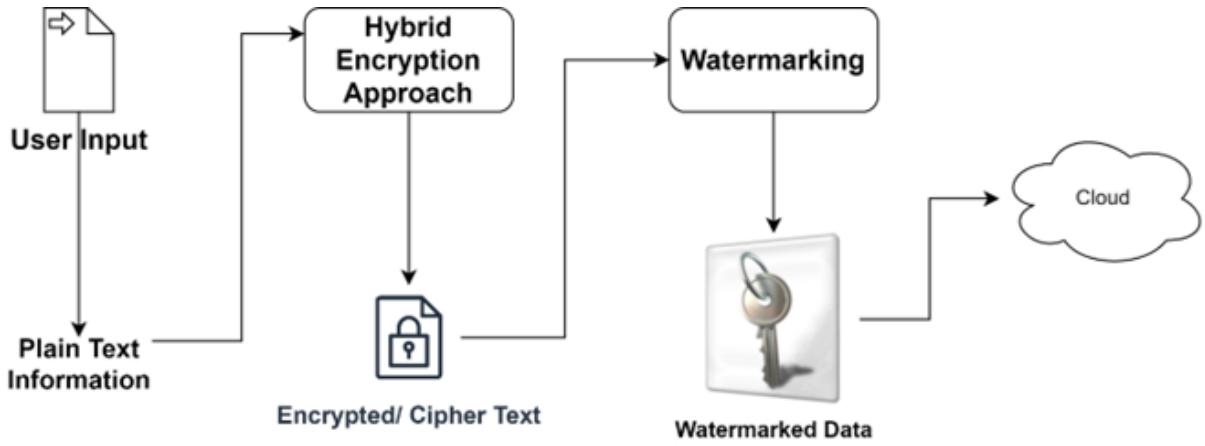
2. Related work

This proposed paper is talking about data security over cloud platforms. So far 'n' number of researchers has proposed their different approaches in order to provide secured data transmission algorithms. We have gone through a lot of literature research papers that show how confidentiality and integrity of data could be maintained over a network. D. Kuybyshev et al. [1] proposed a study on dissemination of our data on cloud which is not trustworthy. This proposed that data breaches can be prevented with cryptography, authentication, and use trustworthy cloud platforms only. Then Houda. G. et al. [2] given a study of identity based cryptography (IBC) to maintain confidentiality of data with cloud computing. The IBC involves authentication, thus only authorized users have access to data. But the limitation of this paper is that the data storage method whichever the researchers are using is efficient and secure on the assumption basis only as per their conclusion statements. Sreekumari et al. [3] further comes up with a study that encryption, authentication offers better security features. The researcher suggested that to maintain the data privacy, keyword search functionality must be performed over the cloud data and here important point is that whole keyword search functionality needs to be performed without leaking the any kind of information about private search keyword. The limitation of this study is that it lacks in describing the role of cryptography and how it could be merged into data to secure data. C. Sahin et al. [4] proposed study on security of data and privacy of outsourced data over cloud. The researchers discussed about the cryptography and data security in a theoretical manner but lacks in providing any cryptographic algorithm or technique that how it can be helpful for data security for outsourced data for any cloud storage platform.Sun Lei et al. [5] proposed research on design of the cryptography cloud-framework. The researchers in this study say that the service flow of a cryptography cloud can result in improvement of flexibility for the application of the cryptography technique in any cloud environment.
Overall, this literature review shows that researchers have implemented a lot of techniques with different approaches towards solving the issue of data security over clouds. But each approach has certain limitations. In this proposed paper we have tried to suggest that how these research gaps could be overcome to offer reliable approaches towards data security using cryptographic algorithms [8-13]

3. Proposed methodology

In this proposed study we are proposing a methodology of integration of hybrid cryptographic algorithms along with watermarking for multilayer data protection over cloud platforms. Hybrid cryptographic algorithms are more secure than single or individual cryptographic techniques. We have proposed that for multilayer data security over cloud we can also integrate watermarking encryption algorithm. The below figure 2. represents the flow of our proposed methodology.

. **FIG 2.** Our Proposed Methodology (Hybrid Cryptography + Watermarking)



The above Figure 2 clearly represents the workflow of our proposed idea which can overcome the security issue of data over cloud such as data breaches, or important information leakage risks. This proposed methodology of integration of Hybrid cryptographic approach with watermarking encryption technique would offer multilayer data security which makes this methodology more

reliable than existing ones. The workflow of this methodology is as follows, First of user input i.e., the plain text or information will be encrypted by using hybrid cryptography algorithms for e.g. RSA and DES, RSA and AES etc. Then encrypted text or cipher text will become input for the watermarking encryption. The output of watermarking encryption will be watermarked data. Watermarked data will be stored on cloud storage, and no one can read it or fetch our information out of it. Only authorized users can decrypt secret information from this. Here watermarked data is a combination of both encrypted data and watermarking encryption. Once the encrypted data is stored over cloud. It is multilayer protected as mentioned above. To decrypt this data from cloud some secret keys are required. The decryption key will only be shared with trusted and authorized users only to whom we are sending this information via cloud. The decryption process will be first receiver will be verified over cloud whether authenticated or not. If it is authenticated, then he/she will be have key to decrypt watermarked data. After decrypting watermarked data, receiver will get cipher text, then he/she again has to decrypt cipher text for two different cryptographic algorithms as hybrid cryptography approaches is applies. After passing solving so many layers of encryption, finally receiver can access the plain text out of encrypted text. For better cryptography, during the step of hybrid cryptography approach we are working with two different cryptographic algorithms together. We can use one algorithm for key generation while a second algorithm for encrypting the secret information using that secured key generated by one of the algorithms of hybrid cryptography. On the other hand, Watermarking encryption has different types of applications that it can offer to us, and it depends on us how wisely and where we are using this encryption technique. The several applications of watermarking encryption are mentioned below which enhances the features of our proposed approach of data security in cloud. The Watermarking applications are Copyright Protection, Authentication, Forensics, and Digital Right Management (DRM). Hence, our proposed model can offer multilayered data security to our cloud data from modern attacks, and it also can offer copyright protections to someone's original work and would be helpful in forensic investigations.

4. Conclusion

In conclusion to this proposed study, we have found that data security is very important but the algorithms or approach that researchers are implementing for security of data on cloud platforms is also very important. In our literature survey we have found that a lot of researchers are using single cryptographic algorithms, and this approach of security is easily breakable by modern attacks. Some of the papers have also proposed hybrid cryptography approach but lacks in key management or complexity of such algorithms are very high still offers better security than single cryptographic algorithm. Our proposed model of multilayered data security combines hybrid cryptographic approach along with watermarking encryption technique would definitely offer better results in terms of encryption of data when we are storing our secret information over some cloud storage platforms. Even if any unauthorized person gets our encrypted data, it would in non-readable form and would not be easy to decrypt it due to multilayered protection principles of our model. Overall conclusion to this work is that the introduction of hybrid cryptographic algorithms enhanced the security of data which is stored over cloud or being transferred between sender and receiver by using the third party's transmission medium. But integration of hybrid cryptography algorithms with other encryption techniques as we have proposed here watermarking encryption offers multilayered security to our secret information and is also not easily breakable even by modern attacks.

5. Future scope

In our study we have mentioned that how multilayered security can be achieved with merging the different encryption algorithms together. We have explained the workflow of our multilayered data security model as shown in Figure 1. As this is a proposed article, it can open up a new area of research for researchers in future. In future its implementation can be done by adding up more algorithms to it such as data compression which can help to reduce the cloud storage data and data compression can also helps in reducing the encryption-decryption time. [14-17]

References

1. D. Ulybyshev Et Al., "Privacy-Preserving Data Dissemination in Untrusted Cloud," 2017 IEEE 10th International Conference on Cloud Computing (CLOUD), Honolulu, HI, USA, 2017, pp. 770-773, doi: 10.1109/CLOUD.2017.111.
2. H. Guesmi and L. A. Saïdane, "Improved Data Storage Confidentiality in Cloud Computing Using Identity-Based Cryptography," 2017 25th International Conference on Systems Engineering (ICSEng), Las Vegas, NV, USA, 2017, pp. 324-330, doi: 10.1109/ICSEng.2017.32.
3. P. Sreekumari, "Privacy-Preserving Keyword Search Schemes over Encrypted Cloud Data: An Extensive Analysis," 2018 IEEE 4th International Conference on Big Data Security on Cloud (BigDataSecurity), IEEE International Conference on High Performance and Smart Computing, (HPSC) and IEEE International Conference on Intelligent Data and Security (IDS), Omaha, NE, USA, 2018, pp. 114-120, doi: 10.1109/BDS/HPSC/IDS18.2018.00035.
4. C. Sahin and A. El Abbadi, "Data Security and Privacy for Outsourced Data in the Cloud," 2018 IEEE 34th International Conference on Data Engineering (ICDE), Paris, France, 2018, pp. 1731-1734, doi: 10.1109/ICDE.2018.00225.

5. S. Lei, W. Zewu, Z. Kun, S. Ruichen and L. Shuai, "Research and design of cryptography cloud framework," 2018 IEEE 3rd International Conference on Cloud Computing and Big Data Analysis (ICCCBDA), Chengdu, China, 2018, pp. 147-154, doi: 10.1109/ICCCBDA.2018.8386503.
6. Mamta, M. D. Khare and C. S. Yadav, "Secure data transmission in cloud environment using visual cryptography and genetic algorithm: A review," 2017 International Conference on Innovations in Control, Communication and Information Systems (ICICCI), Greater Noida, India, 2017, pp. 1-4, doi: 10.1109/ICICCIS.2017.8660941.
7. J. Shen, T. Zhou, D. He, Y. Zhang, X. Sun and Y. Xiang, "Block Design-Based Key Agreement for Group Data Sharing in Cloud Computing," in IEEE Transactions on Dependable and Secure Computing, vol. 16, no. 6, pp. 996-1010, 1 Nov.-Dec. 2019, doi: 10.1109/TDSC.2017.2725953.
8. A. Kumar, V. Jain and A. Yadav, "A New Approach for Security in Cloud Data Storage for IOT Applications Using Hybrid Cryptography Technique," 2020 International Conference on Power Electronics & IoT Applications in Renewable Energy and its Control (PARC), Mathura, India, 2020, pp. 514-517, doi: 10.1109/PARC49193.2020.236666.
9. A. Kumar, "Framework for Data Security Using DNA Cryptography and HMAC Technique in Cloud Computing," 2021 Second International Conference on Electronics and Sustainable Communication Systems (ICESC), Coimbatore, India, 2021, pp. 898-903, doi: 10.1109/ICESC51422.2021.9532950.
10. A. Kumar, "Data Security and Privacy using DNA Cryptography and AES Method in Cloud Computing," 2021 Fifth International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC), Palladam, India, 2021, pp. 1529-1535, doi: 10.1109/I-SMAC52330.2021.9640708.
11. R. S. Shukla, "IoT Based Designing of Secure Data Storage System in Distributed Cloud System with Big Data using Cryptography Algorithm," 2022 11th International Conference on System Modeling & Advancement in Research Trends (SMART), Moradabad, India, 2022, pp. 264-270, doi: 10.1109/SMART55829.2022.10047177.
12. M. Kaur, A. B. Kaimal, J. K. Sandhu and R. Sahu, "Cloud Data Security using Hybrid Algorithm," 2023 3rd International Conference on Smart Data Intelligence (ICSMDI), Trichy, India, 2023, pp. 223-228, doi: 10.1109/ICSMDI57622.2023.00049.
13. I. Sudha, C. Donald, S. Navya, G. Nithya, M. Balamurugan and S. Saravanan, "A Secure Data Encryption Mechanism in Cloud Using Elliptic Curve Cryptography," 2024 International Conference on Intelligent and Innovative Technologies in Computing, Electrical and Electronics (IITCEE), Bangalore, India, 2024, pp. 1-5, doi: 10.1109/IITCEE59897.2024.10467407.
14. K. Gulati, R. S. Kumar Boddu, D. Kapila, S. L. Bangare, N. Chandnani, and G. Saravanan, "A review paper on wireless sensor network techniques in Internet of Things (IoT)," 2021, vol. 51: Elsevier Ltd, pp. 161-165, doi: 10.1016/j.matpr.2021.05.067. [Online] Available https://www.scopus.com/inward/record.uri?eid=2-s2.0-85112813731&doi=10.1016%2fj.matpr.2021.05.067&partnerID=40&md5=cdfd8aefa3368d90534d939a7354b5d8
15. M. Nagaraju and P. Chawla, "Systematic review of deep learning techniques in plant disease detection," International Journal of System Assurance Engineering and Management, Article vol. 11, no. 3, pp. 547-560, 2020, doi: 10.1007/s13198-020-00972-1.
16. G. R. Singh, M. K. Gupta, M. Mia, and V. S. Sharma, "Modeling and optimization of tool wear in MQL-assisted milling of Inconel 718 super alloy using evolutionary techniques," International Journal of Advanced Manufacturing Technology, Article vol. 97, no. 1-4, pp. 481-494, 2018, doi: 10.1007/s00170-018-1911-3.
17. S. Singh Et Al., "Nitrates in the environment: A critical review of their distribution, sensing techniques, ecological effects and remediation," Chemosphere, Review vol. 287, 2022, Art no. 131996, doi: 10.1016/j.chemosphere.2021.131996.