

Security of Data Using Cryptography in Cloud Computing: A Comprehensive Review

Shreyas PS, Shrinivasa Raddi, Thumisi Tagore Shreevan, Ullal Mohammed Adhif, Rizawan N Shaikh,
4a21cs147@gmail.com, shrinivasraddi9036@gmail.com, 4a21cs168@gmail.com,
4a21cs169@gmail.com, rizwanshaikh@aiet.org.in,
Department of Computer Science and Engineering,
Alvas Institute of Engineering and Technology, Mijar, Moodabidri, Karnataka, India

Abstract—For each and every machine user, Data has always been the most crucial Component. Since the technology has been raised over a year, The security has been reducing for these data. There is necessity for having a proper security for these data. All the day to day bank transaction, financial management, In Business, Industries, Market, Schools, Colleges, Universities etc. These all sectors run because of data. There is a threat that these data can be corrupted or leaked. Thus, security is required for these data. Hence Data security algorithms play an important role in these factors. In this paper we will see about introduction to cloud computing and security, various data security algorithm and the best algorithm, challenges and issues, merits and demerits, application and conclusion.

I. INTRODUCTION

THE Cloud computing, which originated from distributed software architecture, is now a central idea in information technology quite quickly. The extant corpus of literature has extensively explored a range of security solutions, spanning both technology innovations and security policy implementation. Recent research has taken a novel strategy in identifying and addressing emerging threats on cloud environments by introducing criminological viewpoints. Suggestions that are based on criminal theories are meant to strengthen cloud defense against these constantly changing dangers [13][15][19].

A thorough investigation determined a number of security concerns affecting cloud computing features and suggested ways to address these difficulties. A security guide that helps cloud user organizations identify and fix vulnerabilities was created as an outcome of the research [14].

The utilization of cloud services poses security concerns and challenges, mainly because of the existing cloud computing frameworks. Cybercriminals take use of flaws in these models to target computer systems' processing power to obtain unauthorized access to users' sensitive data. Building upon the "Net-work Intrusion Detection and Countermeasure

Selection system" basis, the "Autonomous Cloud Intrusion Response System" (ACIRS) has been presented as a countermeasure. When it comes to risk and challenge mitigation, ACIRS outperforms its predecessor, NICE [10][13].

Even while cloud computing is widely used in information technology, some service providers are still hesitant to completely adopt it because they believe the necessary security technologies are still in their infancy. The literature now in publication emphasizes how important it is that service providers make investments in cloud computing-related device security. An "attack tree map" (ATM) is introduced in a noteworthy research work to conduct an analysis of security risks and vulnerabilities. To improve security services including secrecy, authentication, and integrity, this research focuses on integrating cloud computing with trusted computing platforms. In conclusion, resolving these security issues is require to the expansion and broader use of cloud technology across a range of industries in leading journals to complete their grades. Furthermore, scholarly publications also carry significant weight when applying to reputable universities. Here are the tried-and-true procedures for getting the research paper published in a journal [18].

II. LITERATURE REVIEW

A. Review Stage

In this section we will see about various data security algorithms used in cloud computing. These are the latest algorithm used in cloud cryptography. First it includes symmetric algorithms like advanced encryption algorithm (AES), International data encryption algorithm (IDEA). Data encryption standard (DES), Blowfish algorithm. These are the simplest algorithm and ease to implement. Asymmetric algorithm may be considered as higher security than symmetric but very slower compared to them. Some examples are Rivest Shamir Adleman algorithm (RSA). To overcome

these issues in algorithm the latest encryption method is hybrid encryption. These are the combination of both symmetric and asymmetric algorithm. These are highly efficient, high speed, more protective. Block size, Key length, Rounds and Execution time, these are the constraints used in these algorithms [1][2][3].

B. Final Stage

Table 2.1

Symmetric Algorithm	Asymmetric Algorithm	Hybrid Algorithm
Here single key is provided for both encryption and decryption [3].	Here two separated keys are provided that is public and private key [3].	It is the combination of both symmetric and asymmetric encryption [3].
Both sender and the receiver will be having a same key. They are fast, efficient and simple to implement [3].	Encryption is done using public key and can be shared to anyone. Decryption is done using private key but only owner must have it [3].	By means of asymmetric encryption key is provided for user and receiver and using symmetric encryption, encryption and decryption is done [3].
Examples AES, DES, Blowfish [3].	Examples are RSA, DSA [3].	Examples are TSL, PGP [3].
Major advantage is large amount of data can be easily handled [3].	They are very slow compared to symmetric and their implementation is complex [3].	High maintenance is required for managing the key and they are repudiation [3].
Major disadvantage is leakage of key which leads to vulnerability of the data and they are non-repudiation meaning there won't be any proof that message was sent by sender and received by receiver [3].	They are repudiation meaning there is a proof that sender has sent or receiver has received the message [3].	They are fastest compared to all and costly comparing to symmetric and asymmetric encryption [3].

C. Figures

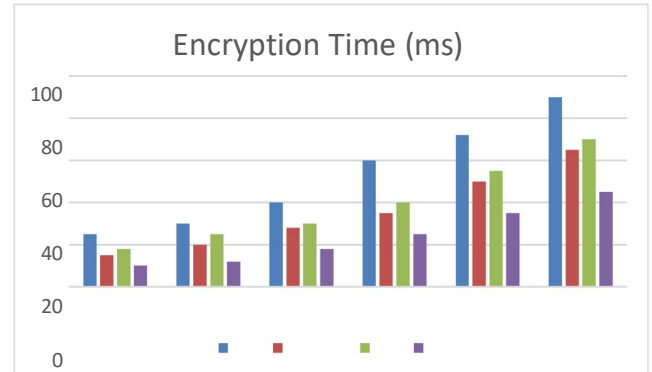


Fig 2.1

Here X axis represents Algorithm that is blue indicates RSA, red indicates Blowfish, green indicates AES and purple indicates TLS. Y axis represents encryption time in milliseconds (ms). From fig 2.1 we can conclude that encryption time taken by TLS (Hybrid) is least followed by Blowfish, AES and RSA.

Table 2.2

Key length	RSA	Blowfish	AES	TLS
100 bits	25	15	18	10
128 bits	30	20	25	12
256 bits	40	28	30	18
512 bits	60	35	40	25
1024 bits	72	50	55	35
2048 bits	90	65	70	45

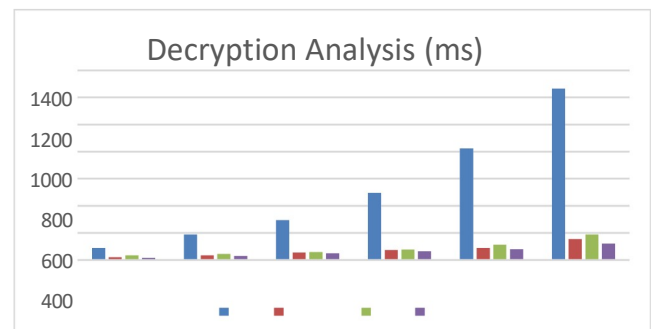


Fig 2.2

Here X axis represents Algorithm that is blue indicates RSA, red indicates Blowfish, green indicates AES and purple indicates TLS. Y axis represents decryption time in milliseconds (ms). From fig 2.1 we can conclude that decryption time taken by TLS (Hybrid) is least followed by Blowfish, AES and RSA.

Table 2.3

Key length	RSA	Blowfish	AES	TLS
100 bits	88	20	35	15
128 bits	188	35	45	30
256 bits	296	56	59	50
512 bits	496	75	78	65
1024 bits	824	88	112	80
2048 bits	1265	155	188	120

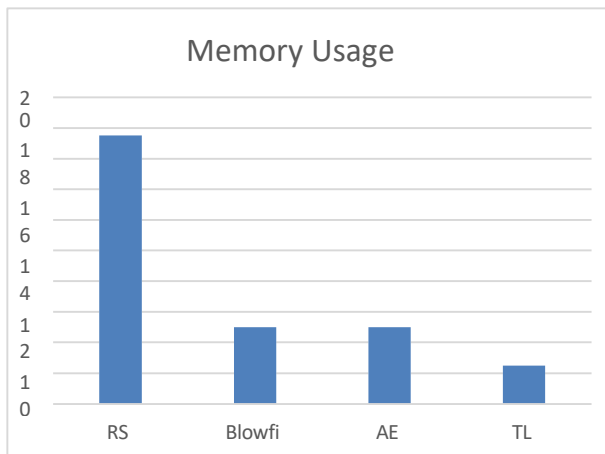


Fig 2.3

From the above analysis we can state that RSA an asymmetric algorithm takes more time for both encryption and decryption. While symmetric algorithm like AES Blowfish takes less time than RSA. TLS a hybrid algorithm takes less time for encryption and decryption. In memory usage RSA consumes more memory for execution and TLS consumes least. Hence hybrid algorithm is the best algorithm for cryptography.

III. CHALLENGES AND ISSUES

Key Management: One of the major issues of cloud computing is key management. Separate key should be provided for different users for encryption and decryption leading to unauthorized access corruption vulnerability [6][7][8].

Different Encryption Architecture: According to the Cloud Standards Customer Council, there are numerous architectural options for encryption in the cloud, including application-level, file system-based, agent-based, and storage device-level techniques. Based on how encryption keys are managed and how well they work, these methods offer unique

features. Furthermore, different algorithms are applied in different ways throughout the process. As a result, creating links and facilitating communication across these approaches is difficult [6][10][13].

Responsibility: Cloud users are next in line for responsibility for data security, after CSPs. Whoever has responsible for data encryption will have to handle and overcome all of the aforementioned problems. An increase in costs and complex coordination and communication between the cloud service provider and the cloud customer are two examples of this difficulty [4][5][6].

Data Visibility: Since the client can view the data from any location and on any type of device, monitoring traffic in a computing environment with a wide range of devices present is extremely difficult [6].

Data Control: An organization's admin has less control over the data that is being saved in the cloud server since it needs the assistance of a third-party cloud service provider to store its data in the cloud [1][5][6].

IV. MERITS AND DEMERITS

Table 4.1

Merits	Demerits
Cost Efficiency: Users only pay for what they use on a subscription basis with cloud computing, there is no longer a need for upfront infrastructure investments, which results in cost savings [9][10][11].	Data Security concerns: Suspicious actors may gain access to confidential data due to improper setups or unauthorized access to cloud servers [9][10][11][17].
Scalability: Cloud services give businesses the flexible nature to adjust to changing requirements without having to make substantial investments in hardware because they can easily scale up or down based on demand [9][10][11][19].	Data Loss: Infrastructure failures or insufficient backup procedures can cause data loss, especially if proper uptime and data backup procedures are not in place. Data Loss: Infrastructure failures or insufficient backup procedures can cause data loss, especially if proper uptime and data backup procedures are not in place [9][10][22][11].
Accessibility: cloud services are accessible from any location with an internet connection, teams can collaborate and work remotely from any location [9][10][11].	Compliance Changes: Careful management and monitoring are required when storing data in the cloud because it becomes more complicated to assure compliance with industry standards and data

	protection laws [9][10][11].
Reliability: cloud services are accessible from any location with an internet connection, teams can collaborate and work remotely from any location [9][10][11][15].	Encryption and key Management: Proper encryption storage or transit, key management procedures are important to protect data while it's in even though poor key management can allow the exchange [9][10][11][15].
Resource Optimization: cloud computing providers can dynamically allocate resources based on demand, maximizing performance and minimizing waste, it facilitates efficient resource [9][10][11].	Shared Responsibility Model: In a shared responsibility model, users are responsible for securing their data and apps, and cloud providers secure the infrastructure. Factual errors relating this model could lead in security coverage gaps [9][10][11].

V. APPLICATIONS

A comprehensive study of data security in cloud computing holds important implications for a wide range of applications across industries. The findings, recommendations, and insights presented in this research paper offer tangible benefits to organizations using cloud services. Here, we delve into the specific applications of the key elements of the comprehensive analysis - encryption techniques, access controls, compliance, and emerging technologies [25][26][27].

Encryption techniques in real world scenarios: The encryption techniques highlighted in the review are immediately applicable to real-world application scenarios. For example, organizations that handle sensitive customer information can use strong symmetric encryption algorithms to protect privacy when transmitting data. In healthcare, where privacy is paramount, the use of uniform encryption can enable secure accounting in encrypted medical records, ensuring patient confidentiality is maintained even at data analytics systems in Reviewed encryption methods, when strategically deployed, in a variety of applications and across industries, are empowering organizations to protect their data [25][26][27].

Strengthening access for improved security: Access is at the forefront of protecting data in a cloud environment, with direct applications used in assessing and detecting the severity of access Cloud users can use recommendations to have enhanced their Identity and Access Management (IAM) processes to ensure that only authorized persons or systems can access sensitive information , where stringent legal

requirements require stringent processes and an elegant access control system to protect financial data from unauthorized access and potential cyber threats [23][26][27].

Managing compliance in cloud environments: The compliance landscape is constantly changing, and cloud organizations are constantly adapting to stay in line with regulatory frameworks. The survey's assessment of GDPR, HIPAA, and ISO 27001 compliance provides useful applications for organizations across sectors. For example, multinational companies can use the assessment to ensure that their cloud operations are compliant with the GDPR's external territorial reach. Healthcare providers can use HIPAA-compliant cloud solutions, giving patients confidence in the proper storage and management of their sensitive health information [21][28][29].

VI. CONCLUSION

In conclusion, the comprehensive review of cloud cryptography provides guidance for organizations looking to strengthen their digital strategy Applications of the review's findings span a wide array of industries from finance and to manufacture beyond. By strategically implementing the recommendations from the survey, there will be improvement in organization's data security posture in cloud environments [20][22][24].

The encryption techniques described in the survey are strong security techniques that resist unauthorized access and data breaches when used Access is almost Forced existing robustness based on analytical recommendations, enables tightly monitor and manage access control, acquired to the evolving needs of their cloud operations Compliance, as a defined in survey, make sure that businesses gain the trust of stakeholders and users in addition to adhering to regulations [25][26][27].

Moreover, the integration of emerging technologies opens new frontiers for secure cloud computing. Blockchain's decentralized ledger technology can reliably guarantee data integrity during use, while zero-trust security measures provide proactive protection against evolving cyber threats.

As organizations increasingly rely on cloud computing, from this study knowledge gained are important. The real-world examples provided here highlight the observable advantages that businesses can get by addressing cloud cryptography holistically and proactively. It is direct that the research recommendation is not theoretical not only designed but processes that when implemented contribute to a resilient cloud and a secure cyber ecosystem [7][8][12].

In an ever-changing technological and cyber threat landscape, the knowledge from this study highlights the demand for continued vigilance and adaptation Proactive positioning recommended in the study ensures that organizations stay ahead of potential security challenges,

laying the foundation for a secure, compliant and resilient industrial cloud infrastructure. As the digital landscape evolves, from this analysis the knowledge learned will continue to be relevant, guiding organizations towards a future where cloud cryptography is not just a requirement but an option they are used to work [16][19][27].

ACKNOWLEDGMENT

I am grateful to all of those with whom I have had the privilege to work during this and other similar projects. My dissertation committee members have all given me a great deal of professional and personal advice and a wealth of knowledge about life in general and scientific study.

REFERENCES

- [1] "Performance evaluation of cryptographic algorithms: DES, 3DES, blowfish, twofish, and threefish" Haneen Alabdulrazzaq, Mohammed N Alenezi International Journal of Communication Networks and Information Security 14 (1), 51-61, 2022.
- [2] "Hybrid cryptography algorithms in cloud computing: A review" Sadiq Aliyu Ahmad, Ahmed Baita Garko 2019 15th International Conference on Electronics, Computer and Computation (ICECCO), 1-6, 2019.
- [3] "A Review on Cryptography based Data Security Techniques for the Cloud Computing" Kalash Gupta, Deeksha Gupta, Sanjeev Kumar Prasad, Prashant Johri 2021 International Conference on Advance Computing and Innovative Technologies in Engineering (ICACITE), 1039-1044, 2021.
- [4] "Cryptography using blowfish algorithm" Sugandha Sharma, Krishna Nand Patel, Aashish Siddhath Jha 2021 3rd International Conference on Advances in Computing, Communication Control and Networking (ICAC3N), 1375-1377, 2021.
- [5] YAN, Zheng; DENG, Robert H.; and VARADHARAJAN, Vijay. Cryptography and data security in cloud computing. (2017). Information Sciences. 387, 53-55.
- [6] "Issues and Challenges of Classical Cryptography in Cloud Computing" Amrutanshu Panigrahi, Ajit Kumar Nayak and Rourab Paul Department of CSE, I.T.E.R., S'O'A University, Bhubaneswar, India July 2021. [CrossRef]
- [7] Qiu, S., Wang, B., Li, M., Liu, J., Shi, Y., Toward practical privacy-preserving frequent itemset mining on encrypted cloud data. IEEE Trans. Cloud Comput., 8, 1, 312-323, 2020.
- [8] Qiu, S., Wang, B., Li, M., Liu, J., Shi, Y., Toward practical privacy-preserving frequent itemset mining on encrypted cloud data. IEEE Trans. Cloud Comput., 8, 1, 312-323, 2020. Liao, Y., Zhang, G., Chen, H., Cost-Ef.
- [9] Nizamuddin, N.; Hasan, H.; Salah, K.; Iqbal, R. Blockchain-Based Framework for Protecting Author Royalty of Digital Assets. Arab. J. Sci. Eng. 2019, 44, 3849-3866. [CrossRef]
- [10] Dai, M.; Zhang, S.; Wang, H.; Jin, S. A Low Storage Room Requirement Framework for Distributed Ledger in Blockchain. IEEE Access 2018, 6, 22970-22975. [CrossRef]
- [11] Bharany, S.; Sharma, S.; Frnda, J.; Shuaib, M.; Khalid, M.I.; Hussain, S.; Iqbal, J.; Ullah, S.S. Wildfire Monitoring Based on Energy Efficient Clustering Approach for FANETS. Drones 2022, 6, 193.
- [12] Bharany, S.; Kaur, K.; Badotra, S.; Rani, S.; Kavita; Wozniak, M.; Shafi, J.; Ijaz, M.F. Efficient Middleware for the Portability of PaaS Services Consuming Applications among Heterogeneous Clouds. Sensors 2022, 22, 5013. [CrossRef]
- [13] Y. -C. Chen, T. -H. Hung, S. -H. Hsieh and C. -W. Shiu, "A New Reversible Data Hiding in Encrypted Image Based on Multi-Secret Sharing and Lightweight Cryptographic Algorithms," in IEEE Transactions on Information Forensics and Security, vol.14, no. 12, pp. 3332-3343, Dec. 2019, doi: 10.1109/TIFS.2019.2914557.
- [14] S. Bojjagani, V. N. Sastry, C. M. Chen, S. Kumari, M. K. Khan, "Systematic survey of mobile payments, protocols, and security infrastructure," Journal of Ambient Intelligence and Humanized Computing, 2021, doi: 10.1007/s12652-021-03316-4.
- [15] G. Viswanath, P. V. Krishna, "Hybrid encryption framework for securing big data storage in multi-cloud environment," Evolution Intelligent, vol. 14, pp. 691-698, 2021, doi: 10.1007/s12065-020-00404-w.
- [16] K. R. Sajay, S. S. Babu, and Y. Vijayalakshmi, "Enhancing the security of cloud data using hybrid encryption algorithm," J Ambient Intell Human Comput, Jul. 2019, doi: 10.1007/s12652-019-01403-1.
- [17] M. Hamdi, J. Miri, and B. Moalla, "Hybrid encryption algorithm (HEA) based on chaotic system," Soft Comput, vol. 25, no. 3, pp. 1847-1858, Feb. 2021, doi: 10.1007/s00500-020-05258-z.
- [18] F. Yao and J. Su, "Hybrid Encryption Scheme for Hospital Financial Data Based on Noekeon Algorithm," Sec. and Commun. Netw., vol. 2021, Jan. 2021, doi: 10.1155/2021/7578752.
- [19] O. P. Akomolafe and M. O. Abodunrin, "A Hybrid Cryptographic Model for Data Storage in Mobile Cloud Computing," International Journal of Computer Network and Information Security(IJCNIS), vol. 9, no. 6, pp. 53-60, Jun. 2017, doi: 10.5815/ijcnis.2017.06.06.
- [20] I. Chillotti, N. Gama, M. Georgieva, and M. Izabachène, "TFHE: Fast fully homomorphic encryption over the torus," J. Cryptol., vol. 33, no. 1, pp. 3491, Jan. 2020. [CrossRef]
- [21] X. Liu, S. Zhao, A. Liu, N. Xiong, and A. V. Vasilakos, "Knowledge-aware proactive nodes selection approach for energy management in Internet of Things," Future Gener. Comput. Syst., vol. 92, pp. 11421156, Mar. 2019. [CrossRef]
- [22] H. M. Pandey, "Secure medical data transmission using a fusion of bit mask oriented genetic algorithm, encryption and steganography," Future Gener. Comput. Syst., vol. 111, pp. 213-225, Oct. 2020.
- [23] A. Subashini and P. Kanaka Raju, "Hybrid AES model with elliptic curve and ID based key generation for IoT in telemedicine," Measurement: Sensors, vol. 28, Aug. 2023, Art. no. 100824. [CrossRef]
- [24] H. Kadry, A. Farouk, E. A. Zanyat, and O. Reyad, "Intrusion detection model using optimized quantum neural network and elliptical curve cryptography for data security," Alexandria Eng. J., vol. 71, pp. 491-500, May 2023.
- [25] S. Baccouri, H. Farhat, T. Azzabi, and R. Attia, "Lightweight authentication for IoT devices based on elliptic curve ElGamal using ephemeral encoding parameters," in Proc. IEEE Int. Conf. Adv. Syst. Emergent Technol. (IC_ASET), Apr. 2023, pp. 1-7.
- [26] K. Javeed, A. El-Moursy, and D. Gregg, "EC-crypto: Highly efficient area-delay optimized elliptic curve cryptography processor," IEEE Access, vol. 11, pp. 56649-56662, 2023.
- [27] Moura, J., & Hutchison, D. (2020). Fog computing systems: State of the art, research issues and future trends, with a focus on resilience. Journal of Network and Computer Applications, 102784.
- [28] Liu, T., Wang, Y., Li, Y., Tong, X., Qi, L., & Jiang, N. (2020). Privacy Protection Based on Stream Cipher for Spatiotemporal Data in IoT. IEEE Internet of Things Journal, 7(9), 7928-7940.
- [29] Podimatas, P.; Limnitis, K. Evaluating the Performance of Lightweight Ciphers in Constrained Environments—The Case of Saturnin. Signals 2022, 3, 86-94. [CrossRef]