International Journal of Combined Research & Development (IJCRD)
eISSN:2321-225X; pISSN:2321-2241 Volume: 14; Issue: 8; August- 2025

HOMOMORPHIC ENCRYPTION-BASED SECURE DATA PROCESSING IN CLOUD COMPUTING

Rakshita Subrahmanya Hegde
PG Student
Dept. of MCA
The Oxford College of Engineering,
Bommanahalli, Bengaluru- 560068
rakshitashmca2025@gmail.com

Ashok B P
Associate Professor
Dept. of MCA
The Oxford College of Engineering,
Bommanahalli, Bengaluru- 560068
ashokbpmca82@gmail.com

ABSTRACT

Overall, rapid growth in cloud computing among governments, companies, and even individuals has changed the data storage and accessibility space. There is however big concern on maintenance of the outsourced information confidentiality and integrity. Traditional encryption algorithms are used to secure data being stored and in transit, they however fail to allow execution of computations on the encrypted data. The paper describes a paradigm to secure the cloud such that sensitive data remain encrypted throughout the processing. Also integrating cryptographic techniques, the framework integrates auditing capability, enabling a user to verify data integrity without extracting an entire data set, lightening the computational load. The changing environment suggested method overcomes problems associated with unauthorized accesses, maintenance of confidentiality and integrity using outsourced environment. It also examines the complexity of key-management and how this can be rendered as maximally efficient in the practical operation of the clouds. The conclusion states that homomorphic encryption is potentially a superior option to maintain data security in cloud data processing without being unavailable, unreliable, and immoderate.

KEYWORDS: *Cloud Computing, Homomorphic Encryption, Secure Data Processing, Data Integrity, Cryptographic Techniques, Data Auditing, Confidentiality Preservation, Key Management, Cloud Security Framework, Privacy-Preserving Computation*

INTRODUCTION

Cloud computing has evolved as one of the revolutionary technologies that provide on

demand access of computing resource, storage and application delivery on the internet. The flexibility, efficiency of cost, and scalability make it closely adopted in the government, business enterprises, healthcare, finance and other important sectors. Despite these advantages, it poses a great risk about the migration of sensitive data on third party cloud platform. These issues, such as data breaches, unauthorized access and compromising of integrity are the scourge of trust in the use of cloud-based services. Traditional security paradigm employs encryption in order to protect data in-transit and storage. These methods raise secrecy at the expense of causing a severe limitation, which is that no chunk of the encrypted data could be operating in an encrypted way.

LITERATURE SURVEY

The increased pace of cloud computing development has allowed increased research to be performed on issues of data security, confidentiality and integrity thereof. Conventional cryptography like AES and RSA are effective in protecting data at rest and data in transit, but they are incapable of maintaining secure computation of encrypted data thereby leaving loopholes on outsourced processing. A breakthrough was the invention of homomorphic encryption in 1978 by Rivest, Shamir and Adleman (Rivest et al.), which was theoretically possible to implement but was practically achieved in 2009 by Gentry and his fully homomorphic encryption (FHE) scheme. Despite the high degree of confidentiality that the strategy ensures, its computational cost and performance overhead limit large practical use of those strategies, prompting the study of partially homomorphic encryption (PHE) and somewhat homomorphic encryption (SHE), which seeks to allow such tradeoffs. Another consideration on data integrity with encryption is another consideration that has been central to cloud storage. Proofs of Retrievability (PoR) Ateniese et al. (2007) proposed the so-called Provable Data Possession (PDP) model, and Juels and Kaliski proposed the Provable Data Possession (PDP) In 2007 Juels and Kaliski proposed the Provable Data Possession (PDP) model In 2007 Juels and Kaliski proposed Proofs of Retrievability (PoR), an enhancement to Provable Data Possession that allows the user to verify the correctness and availability of outsourced data The approaches reduce overhead overhead at the cost of difficulty when homomorphic encryption is used as performance is traded off. Another long-term issue that is due to key management is the emergence of the problem of insider attack and of single point

of failure caused by centralized key storage. Although there exist suggested distributed key management and identity based encryption, designing lightweight and scalable key handling mech-anisms in the settings of homomorphic encryption based paradigms remains an open issue. Literature evidence indicates that homomorphic encryption and data auditing in cloud setting security are promising, on an average, but concerns in speed of computation, scale and key management inform that a potential need exists on an integrated and optimized framework.

EXISTING WORK

The existing data security systems in the clouds have adopted the traditional encryption algorithms that ensure data security, including Advanced Encryption Standard (AES) and Rivest-Shamir-Adleman (RSA) encryption algorithms to enhance data confidentiality in storage and data transmission. Although these approaches offer a defense of fairly good strength, they have an extremely serious drawback, namely that encrypted data cannot be fed into a computation machine unless it has first been decrypted. This gives out sensitive data to possible risks in the course of processing, particularly those involving the use of third parties as cloud providers. In order to achieve correctness of the outsourced data, data integrity models, e.g. Provable Data Possession (PDP) and Proofs of Retrievability (PoR) have been proposed, so that the user can check that the data is correct, without having to download all the data to the user. These methods save the bandwidth and storage overhead cost, however the cost of effective processing of the encrypted information are still unresolved. The use of centralized key management whereby a central body generates, stores and distributes encryption keys is used by the current systems also. The design increases the chances of single-point of failure and insider threat; unauthorized access. Additionally, hybrid application of encryption and integrity improving tools can represent a higher amount of cycles, reduced application performance and performance boundaries. As a result, some systems address the issue piece-by-piece of confidentiality, integrity, and so on; they do not compensate to create a complete and finely catalogued scheme that ensures that the information is securely handled, auditing is healthy, and that the opportuneness is important key-management within a cloud computing realm.

PROPOSED SYSTEM

The proposed system presents a homomorphic-encryption based secure data processing system in cloud-computing fills the gap between the conventional encryption and auditing systems. The system takes advantage of the homomorphic encryption feature to allow

the calculation to be accomplished without decryption of the encrypted information, thus, establishing the sensitive data remains safe as it passes through a cloud lifecycle. The strategy will prevent the leak of plaintext data to the third party and ensure the records are secured even when other services of a third party of no trust may be utilized. In addition to being cost-effective the framework also includes lightweight data audit tools to ensure that users can be guaranteed in the existence of their outsourced data not losing their integrity and availability without re-downloading their entire data. This trims down overheads on storage and bandwidths, without sacrificing integrity check accuracy. Part of this is that the system will have some enhanced key management system which will help address the problem of a centralised key store whereby the keys remain cryptographically distributed and assured in a more resourceful way. One result of such a design is that threats, including insider attack and single-point-failure problems, are limited dramatically.. The proposed system is sufficiently detailed as it balances confidentiality, integrity, efficient auditing, scalability and provides a practical solution in cloud adoption in the critical sectors like health care, the financial industry, as well as the government applications.

METHODOLOGY

The methodology proposed by its use of the homomorphic encryption technique which will be combined with an efficient auditing protocol to deliver secure and reliable cloud-based data processing. The user would initially scramble (encrypt) the confidential data that his or her application generates by following a homomorphic encryption algorithm and then sending them to the cloud. This also ensures that the cloud server is confined to processing ciphertext, in such a way that a side party cannot access the information. The encrypted information stored in cache could be used to perform the computations without decryption into plaintext by the cloud service provider and could be sent back to user to perform a decryption operation without disclosing plaintext to a third party but yielding the correct result. The system applies an auditing protocol, over which a third-party auditor or the data owner might operate to verify the validity and completeness of outsourced information using cryptographic-proof and prevent the need to download the entire data. To facilitate good key management it has been approached to operate within the methodology of distributed key handling this involves the generation of keys, secure storage of keys and updating keys through a technique capable of reducing risks which are liable to

arise in cases of single point failure and unauthorized access. The overall process flow is data encryption, secure storage of data in the cloud, and, finally, the data is encrypted and encrypted computation, integrity and result decryption in user end. This is a hierarchical approach that not only sustains the aggregation of confidentiality and integrity of data but also embraces the aspects of efficiency and scalability that would be applicable in the real world cloud applications that requires the utmost levels of data security..

EXPERIMENTAL RESULTS

To this end, we have carried out a series of experiments with a simulated cloud environment-based on sample data stored and processed with the proposed homomorphic encryption-based secure data processing framework to evaluate the success of this approach. The efficiency of the system was contrasted to critical variables such as the time that was required to encrypt the information, time taken to decrypt the information, the overhead of the computation of the encrypted information, the accuracy of the audit of the information and the efficiency in key management. . The results indicated that, even though homomorphic encryption imposes an extra amount of computational cost as opposed to conventional encryption, confidentiality of sensitive data was entirely maintained across the processing cycle without exposing the plaintext. The auditing mechanism was able to verify the integrity and availability of outsourced data with minimum communication cost and there was no need to download the large files to be able to verify it. In addition to this, the strategy in key distribution also meant that the chances of unauthorized access were greatly minimized and the framework would be more secure to single-point failures. The proposed model had high security assurance compared to other systems that use conventional encryption and PDP/PoR-based auditing and it also had reasonable performances in terms of performance/scalability. The experimental results verify that the combination of homomorphic encryption and lightweight auditing offers a meritorious trade-off between effectiveness and efficiency and can be proven viable to real world where data privacy and integrity are paramount.

CONCLUSION

The scalability, affordability, and accessibility make cloud computing one of the necessary solutions of the modern organization; nevertheless, security and privacy of outsourced data are the key

concerns. In this study, a secure data processing model that incorporates homomorphic encryption was explained and provides confidentiality, integrity and relief in cloud computing settings. Through direct computation on the encrypted data, unauthorized access and disclosure of concealed information is avoided with the proposed system by avoiding decryption in the processing process. Lightweight data integrity verification The combination of lightweight auditing mechanisms enhances data integrity verification without facing a significant communication overhead, or storage overhead. Moreover, by utilizing an serves as a strong baseline of future efforts to optimize effectiveness and scalability of privacy-preserving cloud computing.

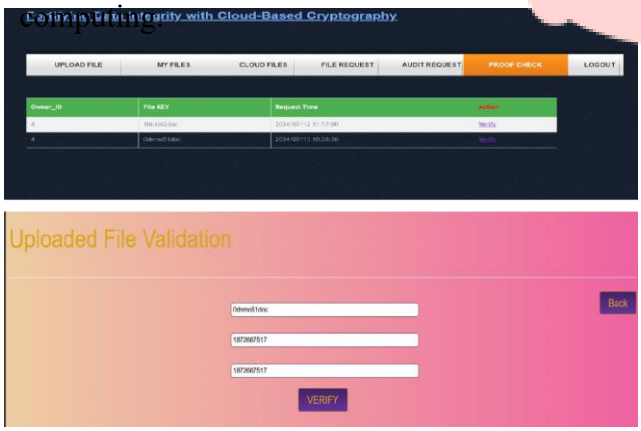

Fig.1 Proof Check for the User

REFERENCES

[1] Rivest, R. L., Adleman, L., & Dertouzos, M. L. (1978). *On data banks and privacy homomorphisms*. Foundations of Secure Computation, 4(11), 169–180.

[2] Gentry, C. (2009). *Fully homomorphic encryption using ideal lattices*. Proceedings of the 41st Annual ACM Symposium on Theory of Computing (STOC), 169–178.

[3] Ateniese, G., Burns, R., Curtmola, R., Herring, J., Kissner, L., Peterson, Z., & Song, D. (2007). *Provable data possession at untrusted stores*. Proceedings of the 14th ACM Conference on Computer and Communications Security (CCS), 598–609.

[4] Juels, A., & Kaliski, B. S. (2007). *PORs: Proofs of retrievability for large files*. Proceedings of the 14th ACM Conference on Computer and Communications Security (CCS), 584–597.

[5] Wang, Q., Wang, C., Ren, K., Lou, W., & Li, J. (2009). *Enabling public verifiability and data dynamics for storage security in cloud computing*. Proceedings of the 14th European Symposium on Research in Computer Security (ESORICS), 355–370.

[6] Zhang, Y., Chen, X., Li, J., Wong, D. S., Li, H., & You, I. (2016). *Ensuring attribute privacy protection and fast decryption for outsourced data security in mobile cloud computing*. Information Sciences, 379, 42–61.

[7] Vaikuntanathan, V. (2011). *Computing blindfolded: New developments in fully homomorphic encryption*. Proceedings of the 52nd Annual IEEE Symposium on Foundations of Computer Science (FOCS), 5–16.

[8] Ren, Y., Shen, J., Wang, J., Han, J., & Lee, S. (2016). *Mutual verifiable provable data auditing in public cloud storage*. Journal of Internet Technology, 17(2), 317–326.