Library Progress International *Print version ISSN 0970 1052*
Vol.44 No.3, Jul-Dec 2024: P. 27174-27178 *Online version ISSN 2320*

Original Article *Available online at www.bpasjournals.com*

Design and Implementation of a Robust Public Key Cryptographic Framework for Secure Communication in Cloud Computing Environments

Dr Kuber Datt Gautam[1], Prof Priyanka Parmar[2], Prof Priyanka Jain[3], Prof Dhrubo Das[4],Prof Chhaya Moghe[5]

1. Assistant Professor, Department of Computer Application Medi-Caps University Indore.
2. Assistant Professor, Department of Computer Application Medi-Caps University Indore.
3. Assistant Professor, Department of Computer Science Medi-Caps University Indore.
4. Assistant Professor, Department of Computer Application Medi-Caps University Indore
5.Assistant Professor, Department of Computer Application Medi-Caps University Indore
Corresponding Author : Dr Kuber Datt Gautam, kuber.datt@gmail.com

How to cite this article: Dr Kuber Datt Gautam, Prof Priyanka Parmar, Prof Priyanka Jain, Prof Dhrubo Das,Prof Chhaya Moghe (2024) Design and Implementation of a Robust Public Key Cryptographic Framework for Secure Communication in Cloud Computing Environments. *Library Progress International,* 44(3), 27174-27178

ABSTRACT

Cloud computing offers the convenience of accessing data from anywhere through shared resources across insecure networks, raising critical concerns about confidentiality, authenticity, and data integrity. Security and privacy issues stem from factors such as data security and the lack of data confidentiality in open and shared environments. As the demand for resources grows and new technologies emerge, the need for secure data storage services in cloud environments becomes paramount. Public cloud service providers are often not fully trusted, exacerbating these concerns. This study proposes a robust security framework that combines homomorphic encryption with Elliptic Curve Cryptography (ECC) and the RSA algorithm to enhance data security in cloud computing. A comparative analysis of RSA and ECC is provided, demonstrating the strengths and weaknesses of each approach in securing cloud-based data storage.

Keywords: Cloud Computing, Homomorphic Encryption, Security, ECC, RSA.

Introduction

Cloud computing is the integrated model of several technologies such as virtualization, web services and service level agreement. The integrated model of numerous technologies, including virtualization, web services, and service level agreements, is called cloud computing. Entrepreneurs, the military, and the government employ various cloud services for network connectivity in order to provide high-quality services. Pay-as-you-go, scalable, software, platform, and infrastructure services are used to represent cloud computing. Cloud services are available to everyone.

Cloud computing is a collection of insecure shared resources and configurations that offers large amounts of storage. It is a data centre where data may be stored, accessed, and shared over the internet at any time and from any location. The cloud offers the resources necessary for cloud-based applications. Parallel, virtualized, and distributed computing are all combined in cloud computing. The cloud effectively offers the service of on-demand resource access. Via a browser that may offer services, one can access these resources and services. Different cloud models require different services because of how the cloud environment is set up. The best services for accessing any programme or hardware from the environment are provided by the cloud. Cloud technology provides on-demand services. The service providers that carry data are the cloud suppliers. Data from the cloud may be easily accessed by virtual operating systems. Data centres house cloud storage data, and each cloud has a separate data centre where all the data is kept. In a data centre, data is dispersed all around. Among the popular cloud service providers are Amazon, Hadoop, and Google Drive.

1. Related Work

In this connected paper, an algorithmic approach is provided along with procedures and mitigation strategies for

fundamental improvement.
Manish M. Potey and others. In[1] suggested using cloud-based storage to encrypt fully homomorphic encryption. In the public cloud, data is kept in an encrypted format. Results from the client's computer and any data stored in the public cloud are never kept in unencrypted. With this, confidentiality can be better achieved.
Homomorphic encryption was employed by Waters et al. in [2] by fusing threshold secret sharing and access approach. A proposed access control approach includes attribute association.

Deyan Chen et al. in[3] discussed cloud security, research on it, and its disadvantages. Applications for cloud security are created, and their importance is examined and addressed from various angles. This method implies that technology hasn't been fully embraced yet. The pros and cons of cloud security, as well as its entire architecture, are explored.
Three keys are used to carry out the security measures, according to Vishwanath S. Mahalle et al. in [4]. The reasoning for this work is that even if one key is compromised, the other two keys will prevent the user from entering the system. If one key is compromised, the other two keys will prevent the user from maintaining security by utilizing three keys. To ensure a secure transaction, security is used in this operation at the administrator end as well.
The platform for financial software as a service and the security framework in the cloud were proposed by Chang et al. in [5]. He showed how the properties of scalability, flexibility, reliability, security, accuracy, speed, and probability may be used to achieve financial services in the cloud. The author mostly came to a conclusion on cloud-based financial services and how they can be implemented using SaaS or framework.

2. Problem Domain

Problem faced in the work is security issue. Issue arises due to the open nature of cloud where there is easy to access any data. The security issue at work is a problem. The open nature of the cloud, which makes it simple to access any data, causes problems. Anyone from anywhere can access resources and use services on demand in a public cloud environment. The data is accessible in plain text format, making it simple to access.
The suggested method is employed at work to safeguard sensitive information. For authentication purposes, data protection is crucial. The data of user A should be safeguarded so that no one can access it if user A keeps his data in the cloud and user B wants to access that data for any nefarious conduct. The majority of research uses data mining techniques to encrypt the data using various encryption algorithms, but in this work we use homomorphic encryption for improved security. Various challenges in cloud can be lessened by the dynamic behaviour of boosting technology with wide level of client-server architecture.
Due to the widespread use of distributed computing, drawbacks of the centralized server are becoming more apparent with the expansion of networking. Virtual centralization, an invention for the cloud, is created. In the discipline of computer science known as the cloud, the consumer is not aware of the origin, storage location, or management of the data. The field of computer science is cloud where consumer does not know the location of data from where data comes and where it is stored, how it is managed.

3. Methodology

Homomorphic encryption involves conducting encryption in such a way that all operations are carried out on the encrypted data on a third-party server, retaining security.
Homomorphic encryption will be used to implement the solution. Partial homomorphic encryption and fully homomorphic encryption are the two types of homomorphic encryption. Operation can be carried out on already established algorithms like unpadded RSA, Elgamal, etc. thanks to partial homomorphic encryption. With fully homomorphic encryption, any data can be subjected to arbitrary addition, subtraction, and other operations; the data must be stored in encrypted form.
As part of our effort, we offer the algorithm for creating homomorphic encryption using Amazon web services. The goal is to develop processing that is robust enough to prevent data theft during transport.
Environment homomorphic technology is utilised in the cloud to protect the privacy and security of data. Yet, a problem occurs when trying to access data that has been encrypted in the cloud using homomorphic technology. This essay includes several aspects of encryption. Client pressure will be lessened if updates are not made frequently. Comparisons are made depending on how well the chosen scheme performs; this will show how much less expensive computations are.

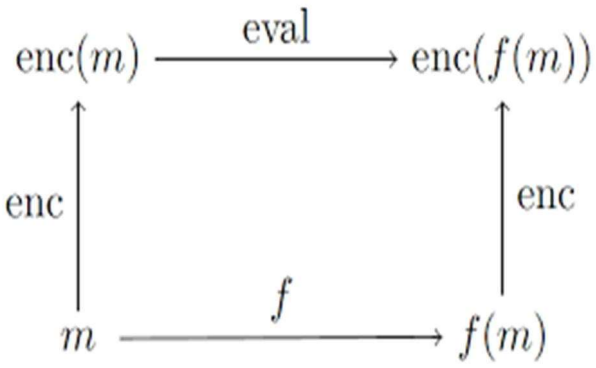

Figure 1: Conversion of message

4. System architecture

System architecture in Figure 2 of the system overview demonstrates how the entire system functions.

• Data: Data input is obtained.
• Chunks: Information is separated into chunks.
• RSA: As a public key cryptosystem that encrypts data using a public key and decrypts data using a private key, RSA is used on the chunked data.
•Following that, chunks are changed into ciphered chunks before being shuffled.
• ECC: This algorithm is used to cypher all of the shuffled chunks into text.

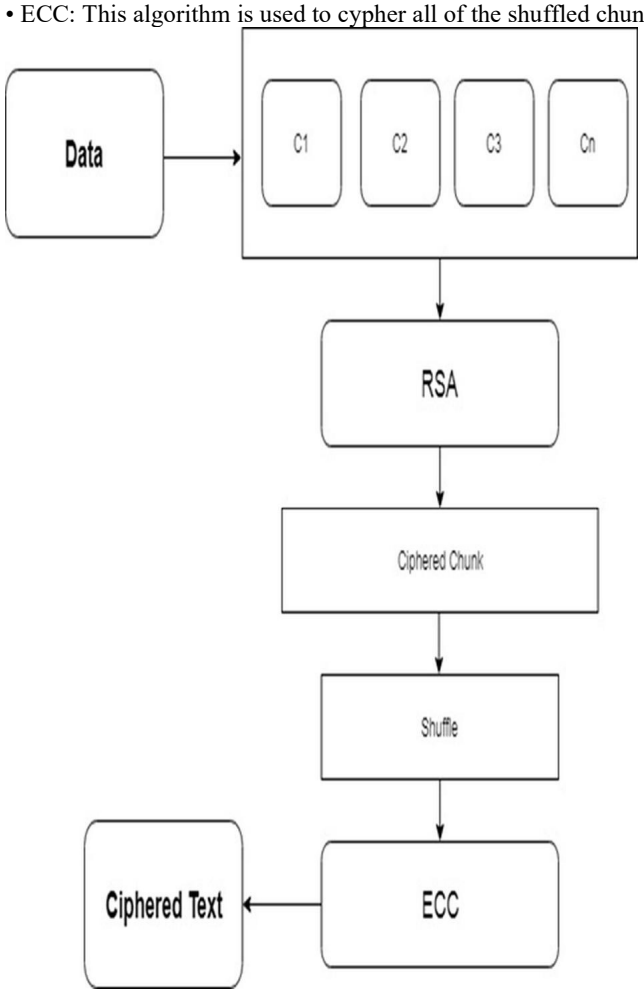

Figure 2: System Architecture

5. Result Analysis

Encryption and decryption time comparison for RSA and ECC is implemented, which calculates the performance and overall time with speed, memory and other parameters.

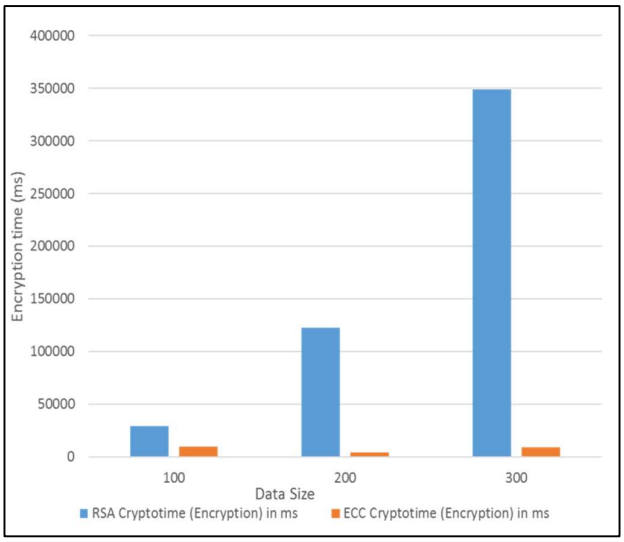

Figure 3: RSA and ECC encryption time comparison graph

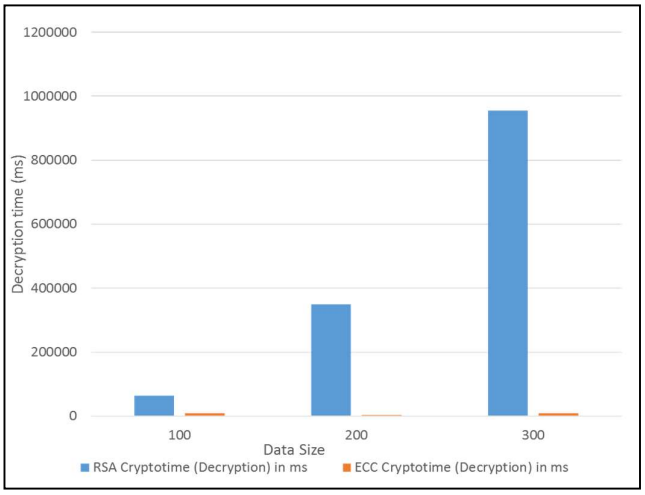

Figure 3: RSA and ECC decryption time comparison graph

6. Conclusion

Homomorphic encryption offers the certainty that the information will be concealed such that there will be no exposure. The primary tenet of the suggested plan is that third-party cloud providers shouldn't have access to any data. In order to determine which strategy should be used when, the work computes computation time and compares the parameters.

REFERENCES

1. Mr. Manish M Potey, Dr C A Dhote, Mr Deepak H Sharma, “Homomorphic Encryption for Security of Cloud Data”. 7th International Conference on Communication, Computing and Virtualization 2016.
2. Waters, “Fully Homomorphic Encryption”. Stanford University Stanford, CA, USA ©2009

3. Deyan Chen; Hong Zhao, "Data Security and Privacy Protection Issues in Cloud Computing," in Computer Science and Electronics Engineering (ICCSEE), 2012 International Conference on , vol.1, no., pp.647-651, 23-25 March 2012.
4. Vishwanath s Mahalle, Aniket K Shahade, “Enhancing the data security in Cloud by implementing hybrid (Rsa&Aes) encryption algorithm”, “Power, Automation and communication (INAP)”, 2014.
5. V. Chang, C.-S. Li, D. De Roure, G. Wills, R.J. Walters, and C. Chee, “The financial clouds review”, Cloud Computing Advancements in Design, Implementation, and Technologies, vol. 125, 2012.
6. Tebaa, M.; El Hajji, S.; El Ghazi, A., "Homomorphic encryption method applied to Cloud Computing," in Network Security and Systems (JNS2), 2012 National Days of , vol., no., pp.86-89, 20-21 April 2012.
7. Peng Xu, Chao Liu. Fully Homomorphic Encryption Algorithm Based On Integer Polynomial Ring [j]. Computer Engineering, 2012.
8. M. Brenner, J. Wiebelitz, G. Von Voigt, and M. Smith, “Secret program execution in the cloud applying homomorphic encryption”, in 5th IEEE International Conference on Digital Ecosystems and Technologies (IEEE DEST 2011). IEEE,2011,PP.114-119.
9. Lopez-Alt, E. Tromer, and V. Vaikuntanathan, “On-the-fly multiparty computation on the cloud via multikey fully homomorphic encryption”, in Proceedings of the forty-fourth annual ACM symposium on Theory of computing. ACM, 2012, pp. 1219-1234.
10. Rivest, Ronald L., Adi Shamir, and Len Adleman. "A method for obtaining digital signatures and public-key cryptosystems."Communications of the ACM 21.2 (1978): 120-126.
11. Yao. Protocols for secure computations (extended abstract). In 23rd Annual Symposium on Foundations of Computer Science (FOCS '82), pages 160-164. IEEE, 1982.
12. C. Gentry, "Fully Homomorphic Encryption Using Ideal Lattices," in Proceedings of the Forty-First Annual ACM Symposium on Theory of Computing, ACM, 2009, pp. 169-178.
13. K. Kaur, H. Singh, R. Kumar, "A Survey of Public KeyInfrastructure Based Security Mechanisms in Cloud Computing," in International Journal of Advanced Research in Computer Science and Software Engineering, vol. 5, no. 7, pp. 122-126, July 2015.
14. Goldwasser, Shafi, and Silvio Micali. "Probabilistic encryption." Journal of computer and system sciences 28.2 (1984): 270-299.
15. J. A. Garay, J. Katz, R. Kumaresan, "Adaptively Secure Broadcast, Revisited," in Advances in Cryptology - CRYPTO 2013, Springer, vol. 8042, pp. 319-336, 2013.