International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 09 Issue: 04 | Apr 2022 www.irjet.net p-ISSN: 2395-0072

SECURITY IN COULD DATA STORAGE USING SOFT COMPUTING TECHNIQUES AND ELGAMAL CRYPTOSTEM

Basima Mukhtar[1], Ankur Gupta[2]

[1]Pg Scholar, Department of computer science& Engineering, School of Engineering, RIMT University
[2]Assistant Professor, Department of computer science& Engineering, School of Engineering, RIMT University

---

Abstract - *A wide variety of data security solutions are available, with encryption being the most popular. Encryption by itself isn't sufficient to protect the private information of a huge number of people. In addition, the encryption and decryption steps for each query take longer to complete. Second, focusing only on the user's needs is a poor strategy since, once uploaded to the Cloud, user data is no longer within the user's control. In light of this fact, we must take into account the security of Cloud servers' critical information. Obfuscation, one of the most important methods, is used to accomplish this. An solution that incorporates both Elgamal and Encryption is proposed in this study to reduce the burden on Cloud servers while still protecting user information. RSA and Elgamal's encryption and decryption times for files ranging from 1KB to 1000KB. As a result, RSA encryption takes less time than Elgamal encryption, while decryption takes longer. When it comes to decryption, Elgamal outperforms the competition.*

Key Words: security, Data storage, Elgamal, soft computing…

1. INTRODUCTION

As the demand of internet is increasing, the service provided such as Software, Platform, Database services, Storage services etc. through internet also gradually increases. Here the important terms cloud computing comes into existence which provides huge amount of different services to its users via network. As it provides 'Pay as you Go' fundamental user can get maximum benefits by using this service for cheaper cost.

Data and programmes are maintained on central distant servers through the internet in Cloud Computing.

Businesses and individuals may now view their personal files from any computer with an internet connection thanks to new technology that eliminates the need for software to be installed.

It is possible to achieve substantially more computer efficiency via the use of the cloud by consolidating storage, memory, bandwidth, and computation.

Cloud storage has many benefits, but it also has a number of security concerns. Cloud storage customers are most concerned about maintaining the privacy of their data. Client data is, in fact, handled outside of the governance of the customers themselves.

Maintaining compliance while also enforcing security policies may be difficult enough when working in conjunction with external third parties and their many subcontractors, known and unknown.

By presenting a technique that encrypts client data before it is sent to the cloud storage and decrypts it with the same secret key after it has been received, we hope to improve data confidentiality in cloud storage systems. A secret key is used to do these tasks on the client side. Cloud storage data is secure, as the user's private key never leaves their computer.

1.1 Could Computing Models

Cloud is a Web based figuring innovation, where shared assets, for example, programming, stage, stockpiling and data are given to clients on request. Distributed computing is a figuring stage for sharing assets that incorporate frameworks, programming, applications, and business processes. Distributed computing is a virtual pool of processing assets. It gives processing assets in the pool for clients through web. Distributed computing as an arising processing worldview intends to share stockpiling, calculation and administrations straightforwardly among enormous clients.

Current Distributed computing frameworks presents genuine restriction in securing clients' information classification. Since clients' delicate information is introduced in decoded structures to remote machines possessed and worked by outsider specialist co-ops, the dangers of unapproved divulgence of the clients' touchy information by specialist co-ops might be very high. approach is introduced to shielding the secrecy of clients' information from specialist organizations, and guarantees specialist organizations can't gather clients' classified information while the information is handled and put away in Distributed computing frameworks. Distributed computing frameworks give different web based information stockpiling and administrations. Because of its many significant advantages, including cost viability and high versatility and adaptability, Distributed computing is

acquiring huge energy as of late as another worldview of circulated figuring for different applications, particularly for business applications alongside the fast development of the Web. With the ascent of the time of "Distributed computing", worries about "Web Security" keep on expanding.

2 SECURITY CHALLENGES IN CLOUD COMPUTING ENVIRONMENT

Every cloud computing based service has different sorts of security challenges. An intruder can utilize the vulnerabilities of network infrastructure to attack the services on features of cloud like on demand self-service, multitenancy, broad network access etc. This could make a considerable measure of vulnerabilities in the service delivered [3]. An overview conducted by [4] demonstrates that security is a major concern toward the clients staying far from the cloud. In this subsection, we analyze different sorts of security that back their heads prevalently in the applications deployed on the cloud.

With the services provided over the cloud Computing Environment, network infrastructures have caused several security issues and challenges. The attacks Distributed Denial of Services (DDOS) are realized by malicious software. Theyprevent the server from providing services to its users by sending un-accessible request to the client. DDOS attack is performed on other machines when a system on the cloud is hacked and used as base. To obtain the main information about the user, attacker can analyze all packets passing through the system. But to find out the open port that can be attacked, scanning is done. Attackers use SQL injections to attack the cloud based database [5].

3. PROPOSED WORK

A cyclic group of ECC discrete points over a finite field is constructed. A wide variety of public cryptographic systems may be implemented in a comparable fashion utilising the ECC. Although it provides the same amount of security as other public cryptography based systems, Elliptic Curve Cryptography has not attained the same level of popularity as the ELGamal and RSA schemes. The discrete logarithm of an elliptic curve serves as the foundation for the ECC [9, 10]. As contrast to the RSA and DSA algorithms, the Elliptical Curve Discrete Log Problem (ECDLP) makes it more difficult to break an ECC since factorization and discrete log problems may be solved in subexponential time. Meaning that in order-competitive systems like DSA and RSA less parameters may be employed. This benefit considerably reduces the amount of energy needed to process.

Cloud storage and access to outsourced data may be secured using elliptic curve cryptography encryption. The cloud storage server may be divided into two sections: a private data portion and a shared data section, according to the suggested concept. There are two sections: one for personal information that is available exclusively to the user and one for information that must be shared with other trusted users. The data storage mechanism will encrypt all of the information in both sections (DSModel).

A. Authentication

Cloud security is predicated on authentication and non-repudiation between the client and the cloud. Authentication Model handles this issue.

The user must be authenticated in order to utilise the cloud service. Authentication is accomplished via the use of a unique username and password combination. Authentication model (AuModel) computes A = hash (password) and encrypts A with the client's secret key and the cloud service provider private key to have C and transmit it to the cloud service provider to verify the user's identity. Afterwards, the user will be able to take use of cloud computing.

Figure 1 depicts the Authentication Model's

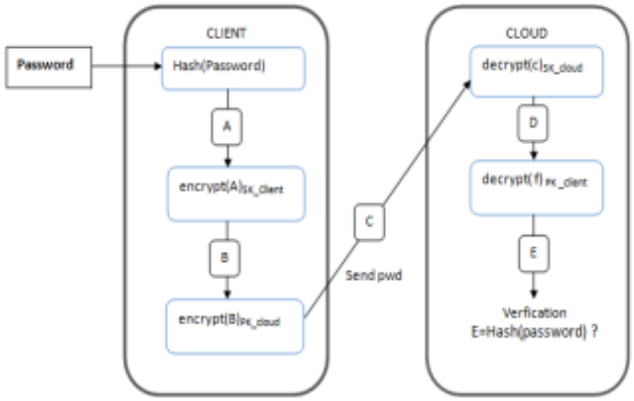


Figure 1: Authentication Model

B. Encryption or decryption

Confidentiality, integrity, and availability are all important aspects of data storage in a cloud-based virtual infrastructure (DS-Model).

Secrecy key cryptography underpins this approach; hence, private data is encrypted using ECC's private key, while public key cryptography is used to encrypt data on shared storage. Users who wish to transmit messages using elliptic curve cryptography must first get the key pair consisting of an elliptic curve equation's base point of primes order G, as well as an integer secret key x, in order to do so. Encryption is required to store data in a cloud since it cannot be stored in plaintext. Users' private keys are combined with the cloud provider's public key to create a cryptographic model that protects their data.

Requests for data from the cloud are always sent encrypted by the server when they come from a user. It will be

decrypted using a cryptographic model, and the original file will be accessible to the client.

C. DATA STORAGE

The data I received by cloud will be decrypted using client's public key then cloud's secret key to have the file K. Data storage model decrypts the data encrypted G to have the original file named DATA then computes hash (DATA) and compares it to the signature K to verify if the original file is not modified during its transmission

D. RSA Algorithm

The RSA algorithm (Rivest-Shamir-Adleman) is the basis of a cryptosystem -- a suite of cryptographic algorithms that are used for specific security services or purposes -- which enables public key encryption and is widely used to secure sensitive data, particularly when it is being sent over an insecure network such as the internet.

RSA derives its security from the difficulty of factoring large integers that are the product of two large prime numbers. Multiplying these two numbers is easy, but determining the original prime numbers from the total -- or *factoring* -- is considered infeasible due to the time it would take using even today's supercomputers.

.Following are the steps involved in ElGamalen cryption algorithm:

Key Generation

The key generation process works as follows:

a. Assume a large prime number **p**.

b. Choose a primitive element **g** modulo p.

c. Choose a private key **a** randomly from {1,...,p-1}.

d. Compute public key **y** as follows :a.y=gamodp

Encryption

The encryption algorithmis as follows:

The plaintext is expressed as a set of numbers modulo p.Data owner encrypt s a message M, CP be the cip her text;CP comprises of two values ciphertext1 (y1) and ciphertext2(y2).

e. Generate a random number k less than p

f. Compute two values y1 and y2 , wherey1=gk mod p

y2=M x or y k

g. Transmit the cip her text CP consisting two values y1 and y2.

Decryption

Upon receiving the cip her text CT (y1 and y2), the receiver computes original message M as:

M=(y1amodp)**x or** y2.

4. RESULTS AND DISCUSSIONS

The whole field of technical research has been revolutionised by cryptography. It hides the text behind a series of hidden keys. It's a straightforward mathematical formula. Plain text may be turned into cypher text by using cryptosystems. Humans cannot decipher cypher text. It's also not easy to figure out how data is encrypted without any previous information. . The cloud storage is one of the prominent services offered in cloud computing. Data stored over cloud in the plain text format is a security threat. This paper proposes a method for cloud storage that allows user to store and access the data securely. It also guarantees that no one can access the data neither the cloud storage provider except the authenticated user. This method provides security and privacy for data stored in public servers

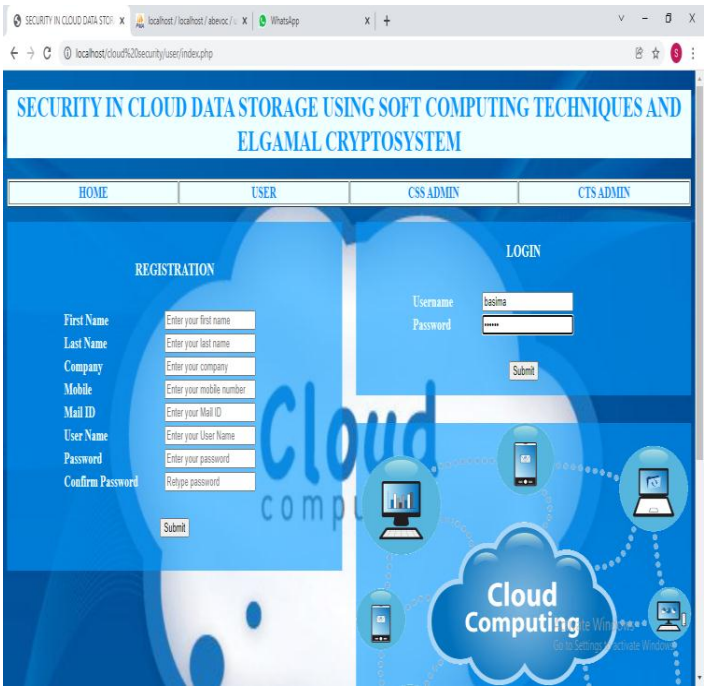


Figure 2 : User Login page

Data owner has to find the signature using his/her own private key a. then he upload the data as pair of data and signature

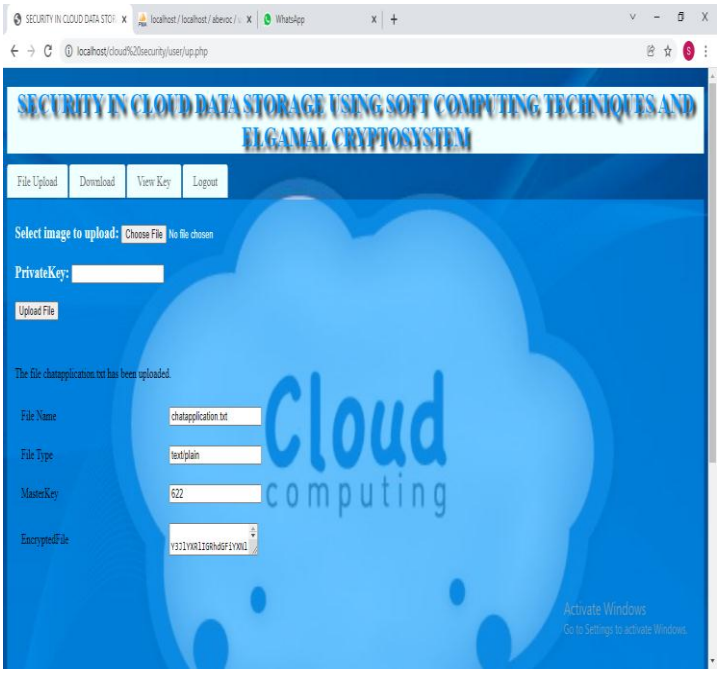


Figure 3: Private Keys

The authorized user verifies the signature with his / her public key. In cloud storage system, the cloud user should perform this task. This allows the authorized users as they have public key.

Table1: Comparative Analysis of Encryption Time

File Size(KB)	Existing system RSA(ms)	Proposed system Elgamal (ms)
1	1100	265
2	288	15
10	720	86
100	1353	1320
500	4223	33310
1000	8266	326790

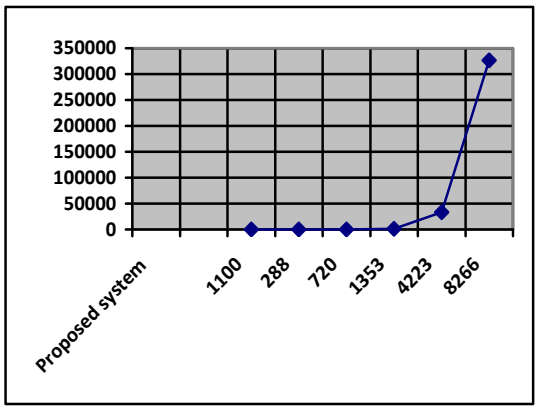
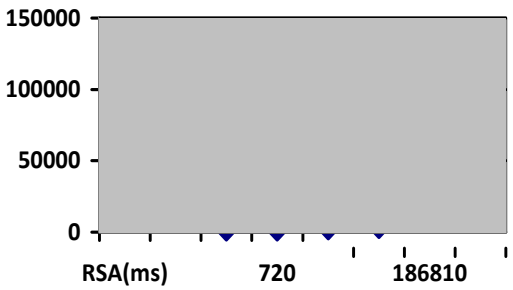


Table2:Comparative Analysis of Decryption Time

FileSize(KB)	Existing system RSA(ms)	Proposed system ElGamal(ms)
1	740	310
2	720	230
10	3010	1008
100	26570	13420
500	186810	81210
1000	218150	130307



Elgamal algorithm is also public key cryptographic algorithm. The private key will be hidden. So if the private key is not known, as we know, it is not possible to reveal the message. So encryption and decryption of message will provide more security for the data.

4. CONCLUSIONS

The primary goal is to securely store and retrieve data in a cloud that is not under the authority of the data's original owner. elliptic curve cryptography is used for cloud storage and access to data files in order to protect them. There are advantages to use the ECC algorithm for encryption, such as speeding up encryption and decryption. In our opinion, this approach of storing data is both fast and safe.

Only members of the group have access to the data kept in the shared data area under this system. Group data sharing in the shared data component of cloud computing models will be addressed in future study.

Before sending data on Cloud encryption, it provides security to the data which is on transition in the network by which user ensures the confidentiality of his data. We have proposed a secure storage sever which keep track of user keys as well hash of the document uploaded on the server. For the Cloud providers, efficient obfuscation technique is proposed by which the secret information of Client like password, contact details etc. are not tempered by third party

REFERENCES

1. R. Soni, S. Ambalkar, and P. Bansal, "Security and privacy in cloud computing," in *Proceedings of the 2016 Symposium on Colossal Data Analysis and Networking (CDAN)*, pp. 1–6, Indore, India, March 2016.View at: Google Scholar

2. E. Veldman and R. A. Verzijlbergh, "Distribution grid impacts of smart electric vehicle charging from different perspectives," *IEEE Transactions on Smart Grid*, vol. 6, no. 1, pp. 333–342, 2015.View at: Publisher Site | Google Scholar

3. A. El-Yahyaoui and M. Dafir, "Data privacy in cloud computing," in *Proceedings of the 2018 4th International Conference on Computer and Technology Applications (ICCTA)*, pp. 25–28, Istanbul, Turkey, May 2019.View at: Google Scholar

4. S. Maharjan, Q. Zhu, Y. Zhang, S. Gjessing, and T. Basar, "Dependable demand response management in the smart grid: a stackelberg game approach," *IEEE Transactions on Smart Grid*, vol. 4, no. 1, pp. 120–132, 2013.View at: Publisher Site | Google Scholar

5. A. Panigrahi and M. R. Patra, "Network intrusion detection model based on fuzzy-rough classifiers," *Handbook of Neural Computation*, Elsevier, Amsterdam, Netherlands, 2017.View at: Publisher Site | Google Scholar

6. P. Wang, J. Ma, and L. Song, "Balanced interest distribution in smart grid: a Nash bargaining demand side management scheme," in *Proceedings of the 2016 IEEE Global Communications Conference (GLOBECOM)*, Washington, DC, USA, December 2016.View at: Publisher Site | Google Scholar

7. P. D. Diamantoulakis, K. N. Pappi, P.-Y. Kong, and G. K. Karagiannidis, "Game theoretic approach to demand side management in smart grid with user dependent acceptance prices," in *Proceedings of the 2016 IEEE 84th Vehicular Technology Conference (VTC-Fall)*, Montreal, Canada, September 2016.View at: Publisher Site | Google Scholar

8. T. Devi and R. Ganesan, "Environmental benefits of enhanced Hecc-elgamal cryptosystem for security in cloud data storage using soft computing techniques," *International Journal of Electronics and Telecommunications*, vol. 10, no. 5, pp. 115–124, 2019.View at: Publisher Site | Google Scholar

9. M. M. Mowla, I. Ahmad, D. Habibi, and Q. Viet Phung, "A green communication model for 5G systems," *IEEE Transactions on Green Communications and Networking*, vol. 1, no. 3, pp. 264–280, 2017.View at: Publisher Site | Google Scholar

10. M. H. Alsharif, R. Nordin, N. F. Abdullah, and A. H. Kelechi, "How to make key 5G wireless technologies environmental friendly: a review," *Transactions on Emerging Telecommunications Technologies*, vol. 29, no. 1, Article ID e3254, 2017.View at: Publisher Site | Google Scholar

11. K. Wang and L. He M. Gao, "Probabilistic model checking and scheduling implementation of energy router system in energy internet for green cities," *IEEE Transactions on Industrial Informatics*, vol. 14, no. 4, pp. 1501–1510, 2018.View at: Publisher Site | Google Scholar

12. P. Liu, S. R. Chaudhry, T. Huang, X. Wang, and M. Collier, "Multi-factorial energy aware resource management in edge networks," *IEEE Transactions on Green Communications and Networking*, vol. 3, no. 1, pp. 45–56, 2018.View at: Publisher Site | Google Scholar

13. M. Imran Tariq, "Agent based information security framework for hybrid cloud computing," *KSII Transactions on Internet and Information Systems*, vol. 13, no. 1, 2019.View at: Publisher Site | Google Scholar

14. E. M. Mohamed, H. S. Abdelkader, and S. El-Etriby, "Data security model for cloud computing," *Journal of Communication and Computer*, vol. 10, no. 8, pp. 1047–1062, 2013.View at: Google Scholar

15. E. Cayirci, A. Garaga, A. S. de Oliveira, and Y. Roudier, "A risk assessment model for selecting cloud service providers," *Journal of Cloud Computing: Advances, Systems and Applications*, vol. 5, no. 1, 2016.

16. Dr. Arockiam L., Monikandan S.. "Efficient Cloud Storage Confidentiality to Ensure Data Security" In Proceedings of the International Conference on Computer Communication and Informatics (ICCCI 2014), IEEE Jan. 03 – 05, 2014, Coimbatore,.

17. Atiq R., Hussain M." Ensuring The Data Integrity in Cloud Data Storage " Proceedings of IEEE CCIS 2011.

18. Arvind N., Vitaly S., "Obfuscated databases and group privacy" Proceedings of the 12th ACM conference on Computer and communications security, Pages 102 – 111. 2005