International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Impact Factor (2012): 3.358

Securing Data in Cloud Using Homomorphic Encryption

Honey Patel[1], Jasmin Jha[2]

[1]M.E. Information Technology, L.J. Institute of Engineering & Technology, Ahmedabad, India

[2] Assistant Professor, L.J. Institute of Engineering & Technology, Ahmedabad, India

Abstract*: Security and privacy in cloud computing is one of the most challenging ongoing research areas because data owner stores their sensitive data to remote servers and users also access required data from remote cloud servers which is not controlled and managed by data owners. Since cloud computing is rest on internet, various security issues like privacy, data integrity, confidentiality, authentication and trust encounter. In this paper, we will comprehensively survey the various existing hybrid security techniques of cloud computing. We will compare these combinations of security techniques with their key features.*

Keywords: cloud computing, security, Homomorphic Encryption, Elgamal Algorithm, OTP(One Time Password), Amazon AWS S3

1. Introduction

Cloud computing simply means internet computing. Cloud is a computing model that refers to both the applications derived as services over the Internet, the hardware and system software in the datacenters that provide those services. Cloud Computing is a kind of computing technique where IT services are provided by massive low-cost computing units connected by IP networks [1]. This concept also explains the applications that are broaden to be accessible through the Internet. Cloud applications use large datacenters and effective servers that host web applications and services. According to NIST, "Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources that can be rapidly provisioned and released with minimal management effort or service provider interaction [2]".

2. Service Models of Cloud Computing

A. Cloud computing service models [5]

- Cloud Software as a Service (SaaS): Application and Information clouds, Use provider's applications over a network, cloud provider examples Zoho, Salesforce.com, Google Apps.
- Cloud Platform as a Service (PaaS): Development clouds, Deploy customer-created applications to a cloud, cloud provider examples Windows Azure, Google App Engine, Aptana Cloud.
- Cloud Infrastructure as a Service (IaaS): Infrastructure clouds, Rent processing, storage, network capacity, and other fundamental computing resources, Dropbox, Amazon Web Services, Mozy, Akamai.

B. Cloud computing deployment models[5]

- Private cloud: Enterprise owned or leased
- Community cloud: Shared infrastructure for specific community
- Public cloud: Sold to the public, mega-scale infrastructure
- Hybrid cloud: Composition of two or more clouds

C. Cloud computing sub-services models

- IaaS: DataBase-as-a-Service (DBaaS): DBaaS allows the access and use ofa database management system as a service.
- PaaS: Storage-as-a-Service (STaaS): STaaS involves the delivery of data storage as a service, including database-like services, often billed on a utility computing basis, e.g., per gigabyte per month.
- SaaS: Communications-as-a-Service (CaaS): CaaS is the delivery of an enterprise communications solution,such as Voice over IP, instant messaging, and video conferencing applications as a service.
- SaaS: SECurity-as-a-Service (SECaaS): SECaaS is the security of business networks and mobile networks through the Internet for events, database, application, transaction, and system incidents.
- SaaS: Monitoring-as-a-Service (MaaS): MaaS refers to the delivery of second-tier infrastructure components, such as log management and asset tracking, as a service.
- PaaS: Desktop-as-a-Service (DTaaS): DTaaS is the decoupling of a user's physical machine from the desktop and software he or she uses to work.
- IaaS: Compute Capacity-as-a-Service (CCaaS) CCaaS is the provision of "raw" computing resource, typically used in the execution of mathematically complex models from either a single "supercomputer" resource or a large number of distributed computing resources where the task performs well.

D. Cloud computing providers

Amazon Web Services (AWS) -include Amazon S3, Amazon EC2, Amazon Simple-DB, Amazon SQS, Amazon FPS, and others. Salesforce.com - Delivers businesses over the internet using the software as a service model. Google Apps-Software-as-a-service for business email, information sharing and security. And others providers such as Microsoft Azure

Services Platform, Proof-point, Sun Open Cloud Platform, Workday and etc

3. Related Work

A single technique can`t provide security in depth in Cloud, it really requires a strong authentication, confidentiality in transit and data integrity. Various approaches have been discussed below which provide different tier of authenticity in order to ensure security.

Sulochana and Parimelazhagan [7] have described a puzzle based authentication scheme in Cloud computing in which user first registers and solves the puzzle, puzzle solving pattern and time is stored and validated by local server and if user get authenticated, start accessing the Cloud services. Although this scheme ensures 2 tier authentications but static in nature, if attacker once identified the stored pattern, he could easily break the security.

Yogita et al. [8] have described that not a single technique is enough to provide security in Cloud, she has used Diffie Hellman with digital signature for providing 2 tier authentication. But digital signature uses so many parameter that`s why it is heavy enough and also requires a proper key management.

Arasu et al. [9] have given a approach of Hash Message Authentication Code (HMAC) in which key, message and hash function is concatenated together for ensuring authentication. This approach describes only single tier authentication which is weak in case of Cloud computing.

Neha and Ganesan [10] have used Diffie Hellman Key Exchange mechanism for connection establishment and Elliptic curve cryptography for data encryption. In this paper authors used a traditional one tier authentication which is vulnerable to security attacks.

Govind et al. [11] have provided security using digital certificate authentication method. Here author uses RSA Algorithm for encryption/decryption which is followed by the process of digital certification. This method ensures only single tier authentication using Digital certification which raised a problem of key management.

Maninder and Sarbjeet [12] have provided an advance multi tier authentication scheme for enhancing security in financial transactions, in which in first tier, user has to simply pass the traditional login authentication and in second tier a fake screen will appear before user from local server, which is filled by the user by predefined stored pattern, if it is correct then only server will allow access to the resources. Problem with this approach is that it is static in nature, once user identifies or observes the pattern of fake screen from behind, he can easily break this authentication.

Parsi and Sudha [13] have proposed method that use RSA algorithm for authentication and data transfer securely. This method involves a phase of key generation, encryption and decryption.

Timm et al. [14] from Fermi Private Cloud have used a method of X.509 digital certificate for authentication purpose, which is used by many open source Cloud services provider like Eucalyptus and Nimbus. Digital certificate requires both public key and private key for authentication, hence key management is serious issue which needs to be tackled. Apart from this problem, digital certificate requires many others parameters as a purpose of authentication which really makes it heavy enough. Various hybrid approaches of security in Cloud which have been discussed above summarized in a table 3.1. Which covers the proposed method with given year, authentication tier and flaws.

4. Problem Statement

In the existing authentication system, single authentication is not enough for the cloud security. Suppose if you are using only one authentication credential like user id and password only and if the hacker is able to get this information (i.e. user id and password), he will surely get access to the stored data at cloud. So we need such an authentication system in which even if the hacker is able to get one credential, still he should not be able to access the user data and that is where multi-authentication plays role.

5. Proposed Solution

The proposed scheme is divided into two tiers. First tier authentication uses the encryption decryption mechanism as followed in normal authentication schemes. The second tier authentication requires the user to input another password from his/her personal device like Email which will be generated from cloud server and sent over to the user's personal device. When the login screen appears in the user interface of computer and user enters the required cloud id and password, a One-Time Password (OTP) must be generated from the server and sent to the cloud user's registered personal device. Then user must enter that password in the personal device and send to the cloud server. User may send this device through Email of specific cloud server. Then both the standard user password entered in computer's login interface as well as the password entered in user's personal device's interface is authenticated at the cloud server end. If any of the authentications fails, the cloud access will be denied

Elgamal Algorithm[12]:

1. Get the File f to be stored on cloud.
2. Call elgmal_encryption( )
3. a. Generate Keys.
4. b. If (flength< p)then
5. E(f) ← encrypt the file Elgmal(f)
6. else
7. fpart[x] ←create_file_partion( )
8. E(fpart[x] ←encrypt each fpart[x]
9. Concate each part to single fileE(f) ← E(fpart[0])+E(fpart[1])+…….+E(fpart[n])
10. 3. Upload E (f)to cloud.

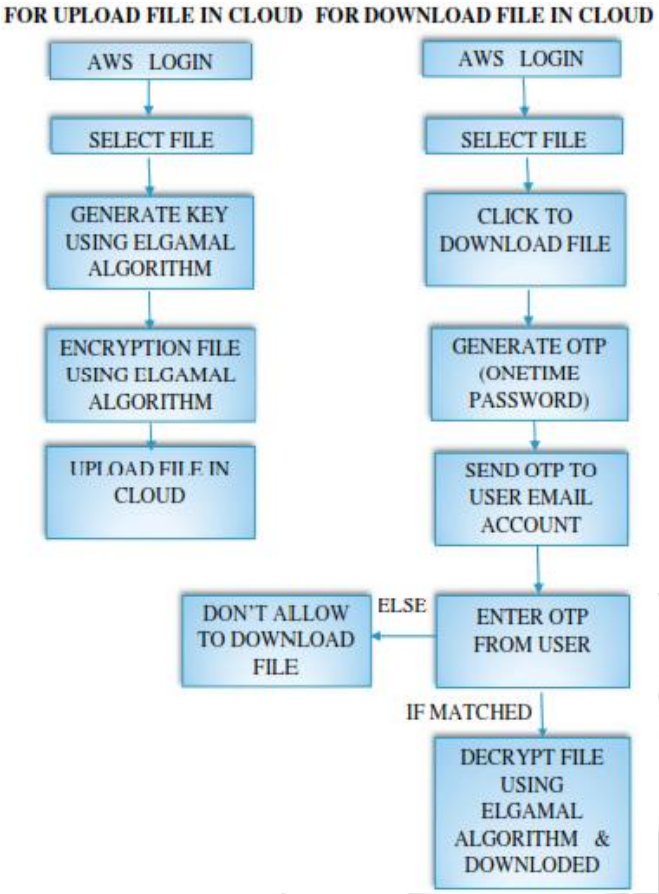

Figure: Proposed Model

6. Results

Figure 2 shows the comparison of encryption time in seconds among Elgamal and RSA. The X-axis represents the File size and Y-axis represents the encryption time in seconds.

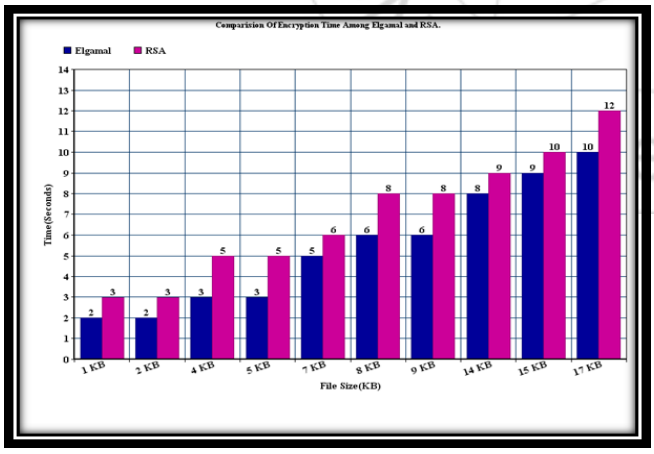

Figure 2: Comparision Of Encryption Time among Elgamal and RSA

Figure3 shows the comparison of decryption time in seconds among Elgamal and RSA. The X-axis represents the File size and Y-axis represents the encryption time in seconds.

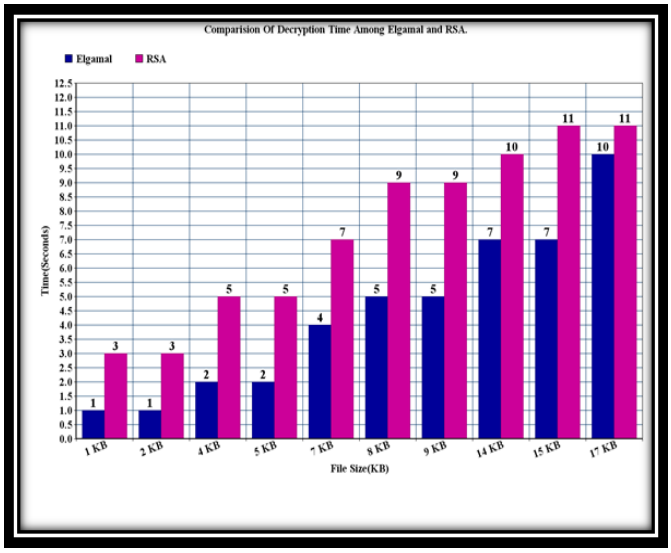

Figure 3: Comparision of Decryption Time among Elgamal and RSA

It is concluded from Figure 2 and Figure 3 that Elgamal showed better over RSA in encryption and decryption process.

7. Conclusion

We used public key cryptography for encrypting and decrypting one time password and data is encrypted/decrypted using elgamal algorithm. In the proposed system encrypted one time password is directly send to user through the network. In the proposed system third party such as GSM mobile number or email is required. The proposed system is designed to improve security, efficiency. Proposed system is highly secure and is dependent on the key size. The key pairs are generated with the help of public key cryptography algorithm.

8. Future Work

Future developments include a user friendly GUI and extending the encrypted OTP algorithm so that system become more secure

References

[1] Ling Qian, Zhiguo Luo, Yujian Du and Leitao Guo, "Cloud Computing: An Overview", Springer-Verlag Berlin Heidelberg CloudCom, LNCS 5931, pp. 626-631, 2009

[2] Peter Mell and Timothy Grance, "The NIST Definition of Cloud Computing", National Institute of Standards and Technology Special Publication 800-145, 2011.

[3] Tharam Dillon, Chen Wu and Elizabeth Chang, "Cloud Computing: Issues and Challenges", 24th IEEE International Conference on Advanced Information Networking and Applications, pp. 27-33, 2010.

[4] S. Ramgovind, MM. Eloff and E. Smith, "The Management of Security in Cloud Computing," IEEE Information Security for South Africa (ISSA), pp. 1-7, 2010.

[5] Sherif el-etriby, Eman M. Mohamed and Hatem S. Abdelkader, "Modern Encryption Techniques for Cloud Computing Randomness andPerformance Testing," 3rd International Conference on Communications and Information Technology (ICCIT), pp. 800-805, 2012.
[6] Satish Kumar and Anita Ganpati, "Multi-Authentication for Cloud Security: A Framework," International Journal of Computer Science & Engineering Technology (IJCSET),Vol. 5, Issue 4, pp. 295-303, Apr. 2014.
[7] V. Sulochana and R. Parimelazhagan, "A Puzzle Based Authentication Scheme for Cloud Computing," International Journal of Computer Trends and Technology (IJCTT), Vol. 6, Issue 4, pp. 210-213, Dec. 2013.
[8] Prashant Rewagad and Yogita Pawar, "Use of Digital Signature with Diffie Hellman Key Exchange and AES Encryption Algorithm to Enhance Data Security in Cloud Computing," IEEE International Conference on Communication Systems and Network Technologies (CSNT), pp. 437-439, 2013.
[9] Sarbjeet Singh and Maninder Singh, "Design and Implementation of Multi-tier Authentication Scheme in Cloud," International Journal of Computer Science Issues (IJCSI), Vol. 9, Issue 5, pp. 181-187, Sep. 2012.
[10] H.A. Dinesha and V.K. Agrawal, "Multi-level Authentication Technique for Accessing Cloud Services," IEEE International Conference on Computing, Communication and Applications (ICCCA), pp. 1-4, 2012.
[11]]Neha Tirthani and R. Ganeshan, "Data Security in Cloud Architecture Based on Diffie Hellman and Elliptical Curve Cryptography," International Association for Cryptologic Research (IACR), ePrint archive, 2014.
[12] Eman M. Mohamed, Hatem S. Abdelkader and Sherif el-etriby, "Enhanced Data Security Model for Cloud Computing," IEEE 8th International Conference on Informatics and Systems (INFOS2012), pp. CC12-CC17 , 2012.
[13] Uma Somani, Kanika Lakhani and Manish Mundra, "Implementing Digital Signature with RSA Encryption Algorithm to Enhance the Data Security of Cloud in Cloud Computing", IEEE 1st International Conference on Parallel, Distributed and Grid Computing (PDGC2010), pp. 211-216, 2010.