International Journal of Recent Technology and Engineering (IJRTE)
ISSN: 2277-3878 (Online), Volume-8 Issue-4, November 2019

Enhance the Security of Data Storage and Retrieval in Cloud Computing Through Authentication Based Encryption

J. Sai Geetha

Abstract: ***The digital computing infrastructure is rapidly moving towards cloud based architecture. The protection of data is becoming a difficult task in the current scenario as more and more confidential and sensitive data is stored in cloud environment and transmitted between cloud users. In a cloud computing environment, the entire data reside over a set of networked resources of remote servers and locations. These data has been accessed by unauthorized cloud users through virtual machines. To provide additional level of cloud data security, Biometric based authentication with encryption using public key cryptography is proposed in this paper. The proposed model Authentication Based Encryption (ABE) helps to enhance the security of data as well as the authentication of cloud user. The sensitive data is initially encrypted and then stored secretly with biometric finger print image. The resultant image is transmitted through the in-secured channel. However to avoid unauthorized access, the image is decomposed and stored in cloud separately as encrypted message and finger print. Before beginning the decryption process, the finger print of the cloud user is being compared with the stored image for authentication. If the match is found, the encrypted data is decrypted by the authenticated cloud user. Otherwise access to the data is denied to ensure security. Thus, the proposed framework provides an additional level of protection to public key algorithm with authentication.***

Key words: ***cloud computing, Communication and storage security, biometric based Image Encryption and Decryption, Public key cryptography and authentication.***

1. INTRODUCTION

A. Cloud Computing

Cloud computing is a pool of configurable computer resources and services that can be provisioned with minimal management effort through Internet [1]. It refers to the features and services of total computing which could be done by cloud users through internet, where the ownership of hardware and soft resources are of third parties. In general practice, the distributed nature of the resources is considered to be the 'cloud' which is an essential property in cloud computing environment.

Many of the people are moving to the cloud to use an on-demand nature of applications, documents and services.There are three types of services available in cloud such as SaaS (Software as a Service), PaaS (Platform as a Service) and IaaS (Infrastructure as a Service) with the evolution of cloud
computing as in Fig.1.1. The consumer must have the capability to provide or use the applications running on a cloud infrastructure. It comes under the software as a service. The applications are accessible from various client devices through a web browser or a program interface. The consumer also has the facility to deploy their own application created using different programming languages, libraries, tools supported through the cloud service provider. The Platform as a service does not manage or control the cloud infrastructure like network, servers, operating systems or storage, but has control over the deployed applications and also the settings of the configuration and the application-hosting environment. The online services and APIs underlying network infrastructure such as physical computing resources, location, data partitioning, scaling, security and backup are comes under the Infrastructure as a service. The technical arrangement, control and management of the Cloud Service Provider (CSP) network are transparent to the cloud user. The cloud user is allowed to use all the service from the provider such as SaaS, PaaS or IaaS without knowing about the internal arrangement of the CSP's network.

B. Deployment Models of Cloud Computing

The popularity of cloud computing is purely depends on the development of various types of deployment models. There are four models such as private cloud, public cloud, community cloud and hybrid cloud.

The infrastructure of private cloud is used by stand-alone organization with greater level of control and security. Only the authorized users has the permission to access the information within the cloud .It is also called as internal cloud. The public cloud is the shared cost model and also accessed by all the users. The level of security is purely depending on Cloud Service Provider and cloud users. Hence, it is suitable for less sensitive data.

Another type of cloud computing is the community cloud which can be shared manually with various organizations that belongs to the particular community that is multi-tenant approach. The security of this model is managed and controlled by the third party vendors. The hybrid cloud is an integrated model of all the above three models that is private, public and community models.

Manuscript published on November 30, 2019.
* Correspondence Author
Dr.J.Sai Geetha*, Dept of Information Technology, Bishop Heber College, Tiruchirappalli, Tamil Nadu, India,

It is more suitable for the organizations which can protect their sensitive data in private cloud and communicate with the clients through the public cloud.

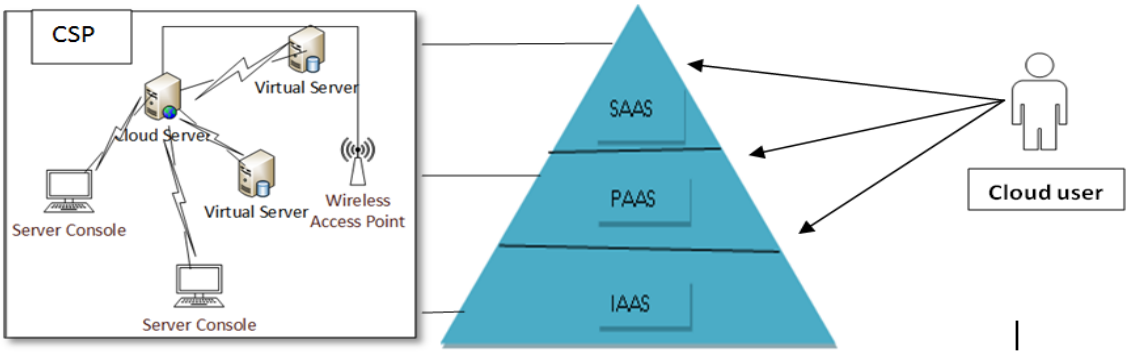

Fig.1.1 Model of Cloud services

C. Authentication in Cloud

In hybrid and public cloud architecture, the authentication service is the platform to access the secured cloud data. It provides the permission to the users to access the centralized resource[2]. The transparent and interactive methods are used for cloud authentication services. It includes password, biometric methods, hardware devices, context based authentication such as network and location. All these authentication system are brittle in nature and vulnerable through brute force attack and also needs some additional tools and services.

II. RELATED WORK

The business people are using the technology of cloud computing to improve their performance by covering the customers in world wide. However, it is necessary to use this cloud services only by the authorized customers, who can verify through the authentication mechanisms. The researchers introduced more number of authentication methods to solve the security challenges of cloud environment. Dinesha et. Al. presented the multilevel authentication technique which generates the password in different levels to access the cloud resources. It can be used to improve the security and authentication of cloud services [3].

Shen et. Al. proposed a lightweight certificate-less and cloud aided authentication protocol for wireless body area network. This protocol helps to check the real identity of the user except for the network manager in the registration phase [4].

Santosh et.Al, initiated a method for data security in cloud using RSA. They analyzed the algorithm using three parameters viz., time complexity, space complexity and throughput. The algorithm RSA provides the data security by allowing only the concerned owner of the data to access the same [5].

Sasi et.Al. proposed a biometric algorithm using both finger-print and iris. The minutia matching algorithm is used to compare the image by the percentage level. It also provides access control for secured sharing and authentication [6].

Sunanda et.al introduced multi-prime RSA algorithm to emphasis that the data availability is an important aspect in cloud storage service. Only the authenticated user, that is, only the user who knows the decryption key is allowed to access the confidential data [7].

Sarat et.Al presented a new technology with the combination of biometric and symmetric key cryptography for the purpose of data security in cloud environment. Biometric involved in two stages such as enrolment and identification process. The secret key is hided into the biometric image file [8].

A. Security Challenges in Cloud

In cloud based environment, there are several security issues because of virtualization. The end to end security is a critical task in cloud computing scenario. The entire data is residing into a set of network resources. These data may be enabled and accessed through virtual machine from anywhere beyond the control of intended users [9]. The authentication and confidentiality are the two main issues in cloud security. Hence it is necessary to resolve security and privacy challenges in cloud environment.

III. PROPOSED METHODOLOGY

In the existing system, the security enhancement (core feature) can be done through the Asymmetric algorithms such as RSA [10]. In the same way, proper authentication is achieved through the biometric mechanisms such as finger print, iris, etc.[13]. These two key features are combined together to arrive at the proposed algorithm. The data confidentiality and communication security is achieved only through the public key cryptography. The data is encrypted by using one of the public key algorithms, namely, RSA. The encrypted data can be stored into the public cloud. It satisfies only two of the security principles such as confidentiality and Integrity of the data. It is necessary to include one more important security parameter, namely, authentication which can be implemented through the biometric based authentication by using the finger print of the user in the proposed methodology. Each time user sends a request for the data with finger print to the cloud service provider, the authentication of the user needs to be confirmed by the CSP towards delivery of the data.

Algorithm : Data Storage	**Algorithm: Data Retrieval**
Input : Plain data (D) Output: Cipher Data hide with finger print Image(IDC) Step1: Read plain Data(D) Step2: Generate Key using RSA algorithm Encryption key(ek) and Decryption Key(dk) Step3: Encrypt the plain data (D) using 'ek' (i) Divide the Data into 'n' blocks DB_i Where i=1,2,3…n (ii) After encryption, the result is blocks of cipher data DC_i Where i=1,2,3…n Step4: Read the finger print image (SImg) of the cloud user Step5: Hide DC_i within the finger print image Step6: The result IDC sends to the cloud Storage. //**Final Steps by CSP** // Separate finger print image (SImg) and blocks of cipher data(DC) // Store into authentication table	Input :Cipher Data hide with finger print Image(IDC) Output: Plain data (D) **// Initial steps by CSP** // Read fingerprint image (RImg) // check Authentication using Authentication table // Produce IDC and send to the cloud user Step1:Read IDC Step2:Separate finger print image and cipher Data(DC_i where i=1,2,3 … n) Step3:Decrypt the cipher data (DC) using 'dk' (i) After decryption, the result is blocks of DB_i Where i=1,2,3…n (ii) DB_1,DB_2…DB_n are combined together to form the plain data (D) Step4: Receive and print the plain data(D).

Fig.3.1 Pseudo code of ABE Algorithm

A. Authentication Based Encryption (*ABE*)

The proposed method (***ABE***) consists of two stages, viz., data storage and retrieval. The data storage phase helps to store the data in a secured manner and also satisfies the security principles such as confidentiality and integrity.

It includes additional level of security for the purpose of authentication. The pseudo code of the algorithm is illustrated in Fig. 3.1.

B. Data Storage

The cloud user tries to store the plain data(D) in the encrypted form(DC) using the public key (or) encryption key (ek) of RSA algorithm. RSA algorithm is more suitable for providing security in data communication as well as data storage. It is not possible to access the plain data by the intruders without knowing the private key. At times, the encrypted data have been accessed by the unauthorized cloud users. To overcome this crisis, the biometric based
authentication such as finger print is used to protect the illegal access of confidential data. The encrypted data has been hided with finger print (SImg) of the owner of original data and then send to the cloud storage [11]. The plain data and finger print image are divided into the equal size of blocks [12]. The plain data is to be fitted into the alternative position of the image block to produce embedded image (IDC) and then send to the cloud storage.

The IDC have been separated into fingerprint image (SImg) and encrypted data(DC) by the Cloud Service Provider (CSP). Finally these data has been stored into the authentication table. This table consists of two fields, out of which one of the field maintains the finger print image(SImg) received from the owner of the plain data, known as 'Image field' and another field points the location of cipher data(DC) known as 'Data field'. Before storage, if the finger print image is already exists in the table, then the cipher data (DC) is appended in the data field of the authentication table. Otherwise, both the fields of authentication table are updated. This table helps to check the authentication of cloud users using the finger print.

C. Data Retrieval

Before the process of data retrieval, the cloud user sends their own finger print image(RImg) to CSP. This image(RImg) will be compared with the image(SImg) in the authentication table. If the match is found, then the corresponding cipher data(DC) is retrieved. The finger print (SImg) is embedded with the cipher data(DC) and produce IDC. Finally, IDC is forwarded to the cloud user. Otherwise, the CSP sends an error message to the cloud user. This process is called as "authentication checking". The cloud users receive their own data which is in the form of IDC such as encrypted data (DC) stored secretly with the finger print (SImg). Before decryption, the user confirms their finger print with SImg. Finally, the encrypted data (DC) is decrypted using private key or decryption key (dk). Hence, the cloud user is satisfied with the security as well as the ownership of the data. The detailed framework of secured and authentication based data storage and retrieval is given in Fig.3.2.

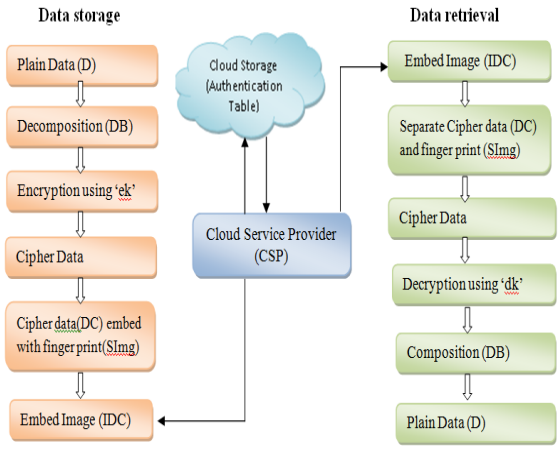

Fig.3.2. Frame work of Data storage and retrieval in Cloud

IV. RESULTS AND DISCUSSION

The more important key parameters in cryptography are speed and security. These parameters are analysed using various size of files. The algorithm ABE has been implemented and tested in JAVA. The data storage and retrieval time are analyzed and tabulated in Table 4.1.

Table. 4.1. Comparison of data storage and retrieval between RSA and ABE

File Size (KB)	RSA		ABE	
	Data Storage Time (ms)	Data Retrieval Time (ms)	Data Storage Time (ms)	Data Retrieval Time (ms)
10	23705	23910	25594	25648
20	31924	31925	33239	34561
30	40233	40756	42239	43658
40	55864	55948	57335	57669
50	62541	62754	64432	64564

In Table 4.1, the data retrieval time is slightly greater than data storage time because of the size of encryption and decryption key. At times, it may be vice-versa. The storage and retrieval time of RSA is less than ABE. The proposed method (ABE) is consists of two segments, first one being encryption and another one is embedding the cipher data(DC) into finger print image (SImg). Hence, it takes more time than RSA.

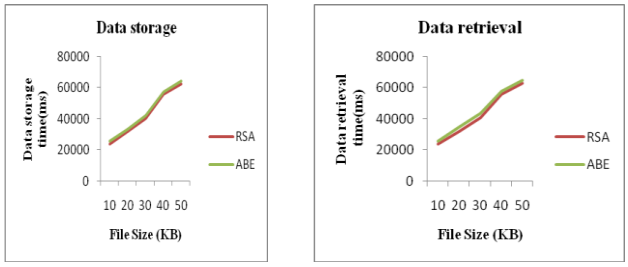

Fig.4.1 . Comparison of Data storage and retrieval time

In Fig.4.1., there is no major time variation between normal storage and authenticated storage. Whenever the file size increases, the data storage and retrieval time are also increased. There is major time variation between normal RSA and ABE algorithm.

From the above analysis, two formulas are derived towards time parameter. The formula for authenticated storage and retrieval are represented in eq. 4.1. and eq.4.2 respectively.

Data Storage time$_{new}$ (DST) = DST$_{old}$ +IST+EAF -eq.4.1

where DST$_{old}$ --- Actual time for storage
IST --- Separation time for finger print image and cipher data(DC)
EAF --- Searching time of authentication table (check new or existing user)

Data Retrieval time$_{new}$ (DRT) = DRT$_{old}$ +IET+EAF - eq.4.2

where DST$_{old}$ --- Actual time for retrieval
IET --- Embedding time for finger print image and cipher data(DC)
EAF --- Searching time of authentication table (check the authentication)

V. CONCLUSION

Cloud computing is one among the frequently used emerging technology. The service of the cloud has given more benefit to the users particularly for big business entities. The secured storage of data is more imperative to realize the advantages of cloud. In public cloud, anyone can store and retrieve the data. There is no access control and security in the cloud environment.The proposed algorithm provides assured access control through biometric authentication and addresses the security concern via public key cryptography. The finger print of data's owner is maintained in authentication table by the CSP. It is evidenced from the result of speed analysis such as data storage and retrieval time affirms the better performance of the proposed method. Any change in the file size, influences the performance of the cloud storage service. The data accessing is not possible without sending proper finger print image. It facilitates the enhancement of data protection in public cloud. In future, the cost of data storage and retrieval needs to be analyzed. In addition, the execution speed of the public key cryptography algorithm needs to be increased towards better productivity.

REFERENCES

1. Rajkumar Buyya, James Broberg and Andrzej Goscinski, "Cloud Computing Principles and Paradigms", John Wiley and Sons, Inc, 2011.
2. Bisong, A. and Rahman, S.S.M. (2011) "An Overview of the Security Concerns in Enterprise Cloud Computing. International Journal of Network Security & Its Applications, Vol. 3, Issue 1, Pg. 30-45, 2011
3. Dinesha, H. A., & Agrawal, V. K. "Multi-level authentication technique for accessing cloud services" In 2012 International Conference on Computing, Communication and Applications (pp. 1-4). IEEE, Feb 2012
4. Shen, J., Gui, Z., Ji, S., Shen, J., Tan, H., & Tang, Y, Cloud-aided lightweight certificate less authentication protocol with anonymity for wireless body area networks. Journal of Network and Computer Applications, 106, 117-123, 2018.
5. Santosh Kumar Singh, Dr. P.K. Manjhi, Dr. R.K. Tiwari, Data Security using RSA Algorithm in Cloud Computing, International Journal of Advanced Research in Computer and Communication Engineering,Vol. 5, Issue 8, Aug 2016

6. E. Sasi, R. Saranyapriyadharshini, Secured Biometric Authentication in Cloud Sharing System, International Journal of Computer Science and Mobile Computing, Vol. 4, Issue. 3, pg.572 – 577, Mar 2015.
7. Sunanda Nalajala, Pratyusha Ch, Meghana A, Phani Meghana B, Data Security Using Multi Prime RSA in Cloud, International Journal of Recent Technology and Engineering (IJRTE), ISSN: 2277-3878, Volume-7, Issue-6S, Mar 2019
8. K Sarat Chand and Dr. B Kezia Rani, Biometric Authentication using SaaS in Cloud Computing, International Research Journal of Engineering and Technology (IRJET), Volume: 05, Issue 02 , Feb 2018.
9. Monjur Ahmed and Mohammad Ashraf Hossain, Cloud Computing and Security Issues in the Cloud, International Journal of Network Security & Its Applications (IJNSA), Vol.6, No.1, Jan 2014
10. Kalpana, Parsi and Sudha Singaraju "Data security in cloud computing using RSA algorithm" IJRCCT vol 1, issue. 4 pp: 143-146, 2012.
11. D.I.George Amalarethinam, J.SaiGeetha, K.Mani, "MRImgEncA-Analysis and Enhancement of speed and security in Public key Cryptography for image file", International Journal of Applied Engineering Research (IJAER), Vol. 10, Issue 82, 2015
12. D.I.George Amalarethinam, J.Sai Geetha, K.Mani, "Analysis and Enhancement of speed in Public key Cryptography using Message Encoding Algorithm", Indian Journal of Science and Technology (IJST), Vol.8, Issue 16, pp.69809-69815, 2015.
13. A. Amali Mary Bastina, N. Rama, Biometric Identification and Authentication Providence using Fingerprint for Cloud Data Access, International Journal of Electrical and Computer Engineering (IJECE), Vol. 7, No. 1, pp. 408~416 , Feb 2017.

AUTHOR PROFILE

Dr. J. Sai Geetha is an Assistant Professor of Computer Science at Bishop Heber College, Tiruchirappalli, Tamilnadu, India. She has more than twenty years of teaching experience in educational institutions of higher learning. The thesis submitted by the author towards Doctoral degree is first of its kind at that time. The author has published her research works in many international journals and presented papers in conferences. In addition, the author has also published chapters and books in Indian and German publications Her current research interests include Network Security in Cloud Computing, Internet of Things and Bigdata.