Role of Biometric Cryptography in Cloud Computing

Praveen Tiwari
Assistant Professor
Dept. Of Computer Science
H.N.B Garhwal Central University
Srinagar Garhwal,

Ashis Saklani
Assistant Professor
Dept. Of Computer Science
H.N.B Garhwal Central University
Srinagar Garhwal

ABSTRACT

Cloud Computing presents a distinct way to share distributed resources and services with the help of internet. Cloud computing includes sharing of distributed resources via internet- an open network, therefore security becomes an essential issue. A secure data transmission and key management is needed in cloud computing, to overcome such problems. Securing information is the key issue in the field of network security. Cryptography is one of the most effective way to enhance information security. Biometric cryptography is a technique which uses biometric features to encrypt the data and overcome the defects of traditional cryptography. In this paper, a biometric based encryption and decryption scheme, in which a master key is generated using whole/partial hash portion of combined sender and receiver finger print. From this master key many random keys are generated using pseudo random generator which is used as a secret key for both encryption and decryption. The pseudo random number generator may have different algorithm to generate one dimensional number from a piece of image matrix of biometry. This one dimensional number is considered as master key and remains valid for one session unless renewed. This master key and sequence number (seed value, other parameter) is sent by the sender after watermarking it in sender's fingerprint along with encrypted message. Proposed system has an advantage that no need to search public key database and security is maintained. The computational requirement and network security features are duly addressed in this paper to make a normal cloud computing platform to trusted cloud computing platform and assured a secure data transmission.

Keywords:-Cloud computing, Security, Biometric Cryptography.

1. Introduction

Cloud computing platform is a set of Scalable large-scale data server clusters, it provide computing and storage services to customers. The cloud storage is a relatively basic and widely applied service which can provide users with stable, massive data storage space.[1]

Cloud computing is fast becoming a popular option for renting of computing and storage infrastructure services (called Infrastructure as a Service or IaaS); for remote platform building and customization for business processes (called Platform as a Service or PaaS); and for renting of business applications as a whole (called Software as a Service or SaaS). The cloud infrastructure has been further sub-divided into, Public cloud - where the infrastructure resides totally outside of the tenant / enterprises? firewall; Hybrid cloud - where the infrastructure and business processes reside partly within the enterprise and partly consumed from third party; and Private cloud - where IT services are mounted on top of large-scale conglomerated and virtualized infrastructure within enterprise firewall and consumed in "per transaction" basis.[3].

There is a growing body of work dealing with various cloud computing security issues. Authors have mostly discussed about singular aspects of cloud security such as vulnerabilities in platform layer (virtualization, network, or common software stacks); vulnerabilities with co-located user data and multi- tenancy; access control; identity management and so on.

We observe that data, platform, user access and physical security issues; although accentuated in cloud computing; are generally applicable in other enterprise computing scenario as well. For example, hypervisor related threats such as cross channel attacks will be present in any virtualized environment not specific to cloud. Two of the great virtues of cloud computing are service abstraction and location transparency. However, from security point of view these two points in conjunction with third-party control of data can create challenging security implications [3].

In the system architecture, there is a central entity to index or manage the distributed data storage entities. It is effective to simplify the design and maintenance of the system by a central managed architecture, but the central entity may become a bottleneck if the visiting to it is very frequent. Although systems in practice have used some technique as backup recovery to avoid the probably disaster from the central bottle neck, the flaw come from the architecture has not resolved essentially [1]. On Other side, Security and privacy are two prime barriers to adoption of the cloud computing [2]. Cloud computing, which is considered to be the next big trend of information age by many people, offers great benefits including: low up front IT investments, pay-for-use model allows for reduced operating expenses, reduced complexity, etc. However organizations or companies have to upload their data or programs to the cloud, obviously security and privacy will be two significant barriers to Adoption [2]. Electronic Communication in today's world involves around a millions of computers networked together. While this network increase the possibility of resource sharing to make life easier and communication cost effective but some unscrupulous breaches can easily break the communication paradise we live in. There it is essential to verify, identify the threats and vulnerabilities to make secure and communication and computation network works towards its security goal. By applying some methods the unscrupulous will soon catch up, but the challenge remains alive in future to come. Inclusion of biometric data in communication is very successful today, to thwart the various attacks and hacking basically for its enormity. Examples of biometric information are facial features, fingerprints, iris, retina, voice, signature stroke, ear shape etc. Further strengthen the communication security. Biometric data is the biological characteristics which is unique for every human being. On the basis of these properties we can easily recognize or identify a human being. Biometric

techniques for security include recognition of faces, finger print, iris, retina, ear shape etc. Cryptography is a technique by which we can send the data one place to another place securely over the insecure channel. Information in the computer can be easily secured by using many of the cryptographic and biometric algorithms as well.

2. ABOUT CLOUD COMPUTING SECURITY

2.1 Security Concerned Cloud Computing

A. Current Security model of the cloud computing

In order to archive security in cloud computing system, some technologies have been used to build the security mechanism for cloud computing. The cloud computing security can be provided as security services. Security messages and secured messages can be transported. Even the mechanism for the cloud computing security has many merits now, but there are still some disadvantages. For example, there is short of the mechanism on the hardware to support the trusted computing in cloud computing system. The creation and protection of certificates are not secure enough for cloud computing environments. The performance is reduced apparently when the cryptographic computing are processed. There are also lack of some mechanisms to register and classify the participants carefully, such as the tracing and monitoring for them [4].

B. The challenge for the security in cloud computing

In cloud computing environment, many users participate in the CLOUD and they join or leave CLOUD dynamically. Other resources in the cloud computing environments are the same too. Users, resources, and the CLOUD should establish the trustful relationship among themselves. And they will be able to deal with the changing dynamically. The CLOUD includes distributed users and resource from distributed local systems or organizes, which have different security policies. According to this reason, how to build a suitable relationship among them is a challenge. In fact, the requirements for the security in cloud computing environment have some aspects, including confidentiality, multiple security policy, dynamic of the services, the trust among the entities, dynamically building trust domains [4].

2.2 The main security problem of cloud computing

1) Attacks:- The network attack is still the biggest challenge of network security. As more and more packages, customers, and enterprises migrate their data into the cloud computing, cloud computing will appear more and more network attacks and fraud. According to a Survey, Security experts said that cloud computing will be the focus of hackers within five years.

2) Data Security:- "Data of Cloud" is stored in different physical locations, in the absence of

Corresponding technical and regulatory constraints, data security is difficult to get protection.

3) Safety standards:- There were not the security model and standards for cloud computing architecture, the confidentiality, integrity and availability of data in the cloud service will be borne by the ultimate consumers of cloud computing, not by the cloud service providers, the rapid development of cloud computing is Promoted by several major IT giants, although they are taking the money in the IT field, after all cloud computing is a new thing, and structural standard between the different cloud computing service provider is not perfect.

4) Private information not Safer:-

Cloud users store data in the cloud, but they can't ensure if their private information is sold out by cloud service providers or not. How to select the Trusted Cloud Computing service provider? For example, in March of 2009, the famous Google has admitted that it leaked private customer information accidentally.

3. Previous Work in Terms of Cryptography

Though work has been done in the field of network security using biometric data and cryptography but consider ring both the concepts together and applying it to a possible application is new and innovative. In fact, with the short introduction of biometry in cryptography as has been dealt by a number of authors the discipline of biometric cryptography is born in this paper. In every sample different data are produced. Cryptography relies on stable and unique key to encrypt and decrypt messages. For implementing the biometrics into cryptography there are two approaches of key release and key generation. Key release algorithms described in the literature ([11], [12], [13], [14]) require that (1) Cryptographic keys are stored in users database (2) If matching is found with cryptographic key, access to database is available, (3) User authentication and key generation are two different processes. Storing keys in database is traditionally insecure as it could be easily hacked. Key generation algorithms avoid some of the problems due to the key release algorithms by , (1) Binding the secret key to the biometric information and (2) Not requiring to access the biometric template. Key generation literature is abound with the works of ([10], [13], [14], [15]) among others, in which key generation is more complicated than key release. Considerable research work has been done in this field ([19], [16], [17], [18])they proposed many algorithms but that were not secure. The algorithms have many defects and fail to achieve many cryptographic properties. Which are mentioned below:(a) No sender authentication (b) No integrity check of watermark data (c) Biometric resources are vulnerable on open channel (d) B's non repudiation could not be achieved (e) Incorrect image to A is not detected In this paper we propose three better secured algorithm which will eliminate all the above mentioned problems of network security and achieve robustness.

4. Model and Problem Work

Now a day cloud computing make everything flexible and easier but there is another aspect that is what about security? Is cloud computing in current scenario is providing confidentiality, integrity and being regulated by compliance like Data Protection Act. Through cloud computing the resource are centralized, so the exposure factor proportionally increase which results in risk. So it is necessary to put a countermeasure to mitigate the potential risk. According to the survey, some company says that due to cloud computing it

become easier for bad guys to focus their effort and breach hundred of thousand of record [1]. There is no security rating system in place for cloud computing, so business users can't rely on third party security mechanism. Risk factor with cloud computing are high because level of security provided by cloud provider are not same.

1. General Framework

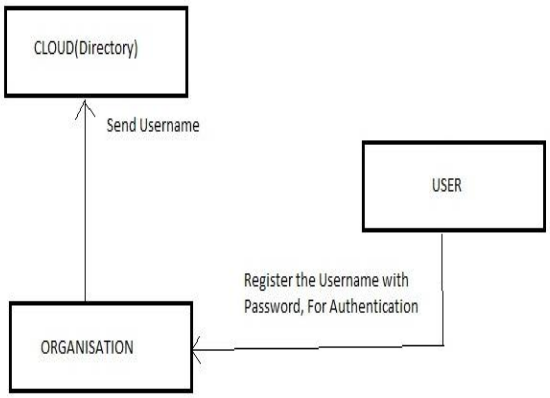


Figure 1

After classification of data, three entity is considered, first one is cloud provider itself, second is organization whose data resides at cloud and last one is employee or anonymous user who request for access of cloud data.

Now the above figure gives overview of Registration phase, in which if a user (either employee or anonymous) want to access the data then user have to register itself (if he is already registered need not require further registration), after registering itself then the transaction will become secure and the process become authenticated.

In this Process the user registered itself for accessing data, organization will provide username and password for authentication. At the same time organization sends the username to cloud provider.

5. A SECRET KEY GENERATION USING BIOMETRIC CHARACTERISTICS

The key generation process will be same for all the algorithms, which we propose. A secret key is generated because it is needed for secure transmission of finger print image. Let q be a globally known parameter. During the key generation process initially, sender A will calculate the hash on its finger print image and hash value is assigned to a variable X A and Y A can be calculated according to the given formula

Y A = X A mod q

Similarly, receiver B calculates the hash on its finger print image and assigns this value to the X B and calculates Y B in similar fashion

Y B = X B mod q

Now, sender and receiver exchange the value of YA and Y B to one another and calculate secret key K accordingly-

K = Y B XA mod q

K = Y A X B mod q

Now, this generated secret key will be used for secure transmission of finger print image over insecure channel in all the algorithms presented in this research paper.

A. Dialogue for key generation

SECRET KEY EXCHANGE USING DIFFIEHELLMAN

- A Calculates : H(FP_A) or X_A = H(FP_A) or $Y_A = X_A$ mod q
- B Calculates : H(FP_B) or X_B = H(FP_B) or $Y_B = X_B$ mod q
- A To B : $Img_{WM}(FP_A, Y_A)$
- B To A : $Img_{WM}(FP_B, Y_B)$

KEY GENERATION

- A Calculates : K = $Y_A X_B$ Mod q
- B Calculates : K = $Y_A X_B$ Mod q

5.1 DESCRIPTION OF IST PROPOSED ALGORITHM-

Let sender A and receiver B both have a common secret key (they have generated secret key using similar technique of Diffie Hellman method). In this proposed algorithm, we will exchange finger print image of A and B by encrypting with secret key. The algorithm leaves no room for false image transmission by third party. After exchange of images, sender A will decrypt the finger print image of receiver B and then will merge finger print of A with finger print of B. After that he will calculate hash on combined image using hash algorithms which is negotiated between sender and receiver. A 128 bit key is generated out of this key generation process. This generated key will be used to generate a random sequence of keys using the pseudo random generator. A random key according to the length of the message is obtained after randomizing all the keys in the key space generated. These random keys are used to encrypt the message of arbitrary length. Sender will watermark the 128 bit key and a random sequence (seed value + other parameter) in the sender finger print image. Sender sends watermark image and encrypted message to the receiver. Similarly, receiver B generates a 128 bit key by applying a hash on combined image of finger print of sender A and receiver B. Now, receiver will be de watermark the received watermark image from the sender and get 128 bit key + a random sequence + FPA (finger print of A). Receiver pick 128 bit key and compare it with the generated 128 bit key. If it is same, then he can be assured that the key has not been altered in the way and authenticate the user also. After that he will pick random sequence and apply on the 128 bit key and generate a random sequence of keys, by which he will decrypt the message that was encrypted earlier by sender.

A. Dialogue for 1st Algorithm

SENDER SIDE

B To A: $E_K(FPB)$

A : H($D_K(E_K(FPB))$+ FPA) : Say k 1

A : Set seed value and other parameters

A : *K I* = Random(*K I* IISVIIOP)

A : Get random key according to message length.

A To B : *Ek I* (M) II Img*WM* (*FPA*, SVIIOPII *K I*)

RECEIVER SIDE

A To B: *E K* (*FPA*)

B: H(*D K* (*E K* (*FPA*))+ *FPB*) : Say k *2*

B: Img *DWM* (Img *WM* (*FPA* , SVIIOPII *K I*)

B: Check if *K I* = *K 2* Then integrity and authentication is confirmed if the check is true.

B : *K I* = Random(*K 2*IISVIIOP)

B: D*K I* (E*K I* (M))

5.2 DESCRIPTION OF 2ND PROPOSED ALGORITHM

Sender A encrypts the message by using secret key and sends this message to receiver. Receiver also encrypts finger print by using secret key and sends to sender. Now, the sender decrypts the finger print of B and merges it with its own finger print, calculate hash on partial portion of merged image which generate a 128 bit key. After taking hash on partial portion, Random keys are generated by this master key using random sequence (seed value + other parameter). A pseudo random generator usually extends to the solution space of hash values or it may even consider the pattern space of finger print to randomize the pattern itself. Now, we use these random keys to encrypt the message of arbitrary length. Calculated hash on master key and random sequence (seed value + other parameter) provides the requisite information of this algorithm. After calculating all these values, sender watermarks(master key + random sequence) and hash of (master key + random sequence). Sender A sends watermarked image and encrypted message to receiver B. At receiver side, after dewater marking receiver, finds 128 bit key, random sequence, image of finger print of A and hash of (128bit key and random sequence). Receiver apply hash on dewater marked random sequence and master key and compare it with the received hash value for checking the integrity of the message. The sender authentication gets executed when receiver compare dewater marked sender image by previous image. After this receiver use pseudo random generator to generate keys and message is obtained after decryption.

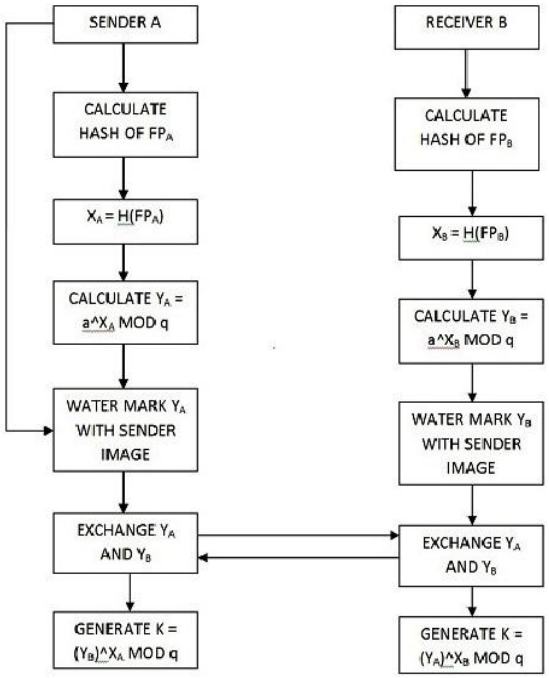
A. Dialogue for 2nd Algorithm

SENDER SIDE

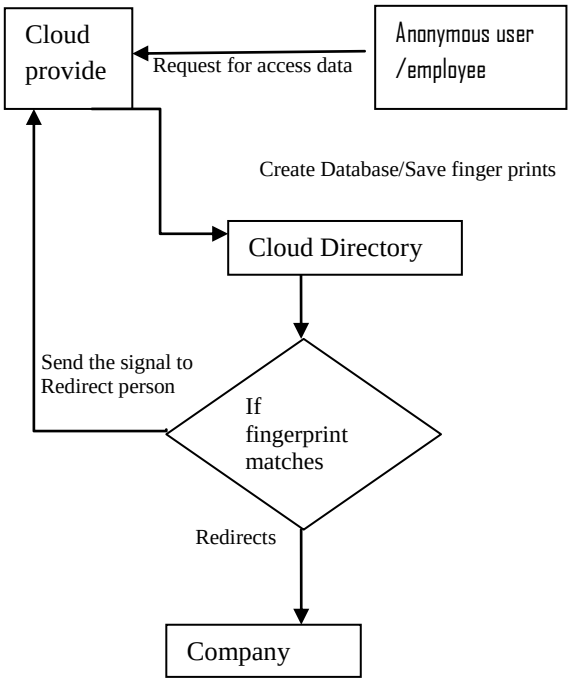
- B To A : *E K* (*FPB*) II Request
- A : H(Img *P AR T I AL* (*D K* (*E K* (*FPB*))+ *FPA*) : Say k *I*
- A : Set seed value and other parameters
- A : k *I* = Random(k *I* II SV II OP)
- A To B : *E K*1(M) II Img *WM* (*FPA*,
- SV II OP II k *I* II H(*K I* +SV+OP))

RECEIVER SIDE

- B To A : *E K* (*FPB*)
- B : Compare *FPB*,R E C E I V E D = DK (*E K* (*FPA*))C O M P U T E D
- B : Compare H(*K I* +SV+OP)R E C E I V E D = H(*K I* +SV+OP)C O M P U T E D
- B : *K I* = Random(*K I* II SV II OP)
- B : D *K I* (E *K I* (M))



Overview of key generation



Overview of Cloud implementing Biometric Cryptography

6. Conclusion

The biometric key formed from the sender's and the receiver's fingerprints has many advantages over current authentication methods because it can neither be forgotten nor shared and is convenient for users to generate. The technique provides a new way to authenticate in different approaches. It provides availability of data by overcoming many existing problem like denial of services, data leakage. As additional it also provides more flexibility and capability to meet the new demand of today's complex and diverse network.

7. References

[1] Ke Xu et al : 2009, A cloud computing platform based on P2P,

[2] Wang Han-zhang et al : 2010, An improved trusted cloud computing platform model based on DAA and Privacy CA scheme,

[3] Shubhashis Sengupta etal :2011 Cloud Computing Security - Trends and Research Directions,

[4] Zhidong Shen et al:2010 The Security of Cloud Computing System enabled by Trusted Computing Technology,

[5] Wang Jun-jie et al: 2011 Security Issues and Countermeasures in Cloud Computing,

[6] John harauz et al: 2010 Data security in the world of cloud computing,

[7] Sameera Abdulrahman et al: 2009 Cloud computing security management,

[8] Xuan Zhang et al : 2010 Inforamtion security risk management framework for cloud computing environments,

[9] Mehnet Yeldiz et al: 2010 A layered security approach for cloud computing infrastructure,

[10] Clancy, T.C., Kiyavash, N., Lin, D.J.:2003 Secure smartcard-based fingerprint authentication. In: Proceedings ACM SIGMM 2003 Multimedia, Biometrics Methods and Workshop, pp. 45-52

[11] Soutar, C., Roberge, D., Stojanov, S.A., Gilroy, R., Vijaya Kumar, B.V.K.:1998 Biometric encryption using image processing. In: Proceedings of the SPIE - Optical Security and Counterfeit Deterrence Techniques II, vol. 3314, pp. 178-188

[12] Roginsky, A.:2004 A New Method for Generating RSA Keys. In: International Business Machines Consulting Group

[13] Davida, G.I., Frankel, Y., Matt, B.J.:1998 On enabling secure appli- cations through offline biometric identification. In: Proceedings of the IEEE Privacy and Security, pp. 148-157

[14] Davida, G.I., Matt, B.J., Peralta, R.:1999 On the relation of error correction and cryptography to an offline biometric based identification scheme. In: Proceedings Workshop Coding and Cryptography, pp. 129-138

[15] Monrose, F., Reiter, M.K., Li, Q., Wetzel, S.: 2001 Cryptographic Key Generation from Voice. In: Proceedings IEEE Symposium on Security and Privacy

[16] Costanzo , C.R.: Active Biometric Cryptography: 2007 Key Generation Using Feature and Parametric Aggregation. In: Second International Conference on Internet Monitoring and Protection, ICIMP 2007, July 1-5, p. 28

[17] Poh, G.S., Martin, K.M.: A Framework for Design and Analysis of Asymmetric Fingerprint Protocols. In:2007 Third International Symposium on Information Assurance and Security, IAS 2007, August 29-31, pp. 457-461

[18] Schenier, B.:1996 Applied Cryptography Protocol, Algorithms, and Source Code in C, 2nd edn., p. 184. Wiley Computer Publishing/John Wiley and Sons, Chichester

[19] Dutta, Sandeep, Kar, Avijit, Mahanti, N.C., Chatterji, B.N :2008 Network Security Using Biometric and Cryptography. In:J.Blanc-Talon et al. (Eds.): ACIVS 2008, LNCS 5259, pp. 38-44, 2008. Copyright Springer-Verlag Berlin Heidelberg