Accomplishment of New Protocol for Stupendous Security in Cloud Environment

S Balaji, S Saravanakumar

Abstract: ***Cloud is that the rising and thirst area of analysis and advantageous in all the fields. However security is the main disquiet for not espouse cloud for each application. Mainly of the security crisis are connected by authentication with data protection by the respect to cloud security alliance (CSA). The projected New (Biometric encoding and Biometric authentication) protocol can conquer every safety crisis in cloud adjacent. In NEW protocol biometric encryption has been provided for the cloud consumer's valuable information and identity verification has been utilized in a unique way to scale back the problems associated with authentication and authorization. In NEW protocol Identity verification in cloud environment has been joint by pattern security in coincidence with four entirely dissimilar and influential encryption algorithms for accumulated safety. This protocol improves biometric template protection by the combination of RSA and AES encryption algorithms in proper locations and 3DES, Blowfish has been utilized in information security and solution safety supervision. By implementing such technique can vanish out the un trustiness of adopting cloud, specifically public and hybrid clouds. Since all the users information are hold on in off premise. Adopting this protocol has given nice results when examining with existing work and all the vulnerable places has been considered for improved security.***

Keywords: Cloud, Biometric Encryption, Cryptography, Authentication Protocol, Protocol, Identity Verification.

I. INTRODUCTION

Cloud computing has been the future of computing with plenty of advantages. Even though it has some lag in security so it has not been adopted by every industry. Has stated in NIST cloud reference architecture it has four deployment models (public, private, community and hybrid) and three service models (SAAS, PAAS, IAAS).

The public and hybrid clouds are the major models where the cloud consumers are afraid of storing their personal data. Since all the data have been stored and used in off premises without the knowledge of consumer. At the same time SAAS and IAAS are the services which are more vulnerable because cloud consumers data has been stored, used and manipulated. In SAAS the users data have been given as input for manipulation and high end processing. In IAAS cloud is considered to be the remote desk top in which all our computations and storage is going to be happened in cloud itself which creates more risk of adopting cloud.

Has stated in notorious nine the article published by cloud security alliance (CSA) in 2013, Nine major problems affects the trust of using cloud in which most of the problems are happening by lack of authentication. From the nine issues such as data breaches ,data loss, account (or) service hijacking ,insecure interfaces and API ,denial of service, malicious insider ,abuse of cloud services, insufficient due diligence ,shared technology vulnerabilities five major issues such as data breaches , account (or) service hijacking ,insecure interfaces and API ,denial of service, malicious insider ,shared technology vulnerabilities have been drastically vanished by proper authentication and identity management . Biometric authentication is one of the best authentication mechanisms in which no need to possess anything and no need to remember anything but gives greater security.

Biometric authentication is also a problem when the biometric templates have not been stated and used securely. As stated in an innovative proposal for secure cloud authentication using encrypted biometric authentication scheme gives how to protect biometric templates using different types of encryption schemes. If the template is secured then no one can compromise the biometric authentication module so it will increase the security of cloud environment. In this paper along with biometric authentication, biometric encryption has been used in the presence of cloud auditor. And the data protection keys have been safe guarded by using biometric template. Such innovative method will change the vision about cloud environment and increase the number of consumers for using cloud environment.

II. RELATED WORKS

The reasons for the lack of trust against cloud are transparent access of data with remote locations and unauthorized usage of data. In order to overcome such problems lots and lots of literature surveys have been reviewed from that many more encryption methodologies have been adopted to protect data stored in cloud and accessed in cloud.

Specifically in public and hybrid cloud the valuable data has been processed in off premise.

Revised Manuscript Received on November 30, 2019.
* Correspondence Author

S Balaji*, Research Scholar, Department of Computer Science & Engineering, BIHER- Bharath Institute of Higher Education and Research, Chennai, India.

S Saravanakumar, Research Supervisor, BIHER- Bharath Institute of Higher Education and Research, Chennai, India.

For authentication and authorization already we have user names and passwords RFID cards barcode readers, phone and email messages and one time passwords, even biometrics is also there for authentication without possessing anything and remembering anything.

But template security is the major issue in biometrics. In existing work cloud data have been protected by means of many types of encryption algorithms but key safety is the major concern since it has been passed in an untrusted network.

Template protection can be carried out by adopting strong encryption algorithms but biometric template privacy is lost. In order to have both security and privacy in template protection the biometric template has to be converted into data and it has to be encrypted while storage and transmission but template matching has to be done only on plain templates. Different encryption algorithms have been used to protect data in the cloud as well as protecting the authentication process but those encryption methodologies have to be used in proper locations and vulnerable parts.

In this NEW protocol RSA encryption has been used in the template during transit since it is a public key encryption so key protection is very high. Blow fish encryption have been adopted in cloud data encryption and storage since it has enormous data blowfish computing speed is very high when comparing with other encryption methods.AES,3DES is used in template encryption during storage , Key encryption for data key retrieval respectively . Such encryption algorithms are already available one but proper placement will give extensive security in template protection as well as cloud data security.

Table.1 Comparison of different biometrics

Biometric	Efficiency	Price	Easy To Use	Uniqueness	False Acceptance Rate	False Rejection Rate
Finger Print	High	Medium	High	High	Low	Low
Iris	High	High	Average	High	Low	Low
Facial Recognition	Medium-Low	Medium	Average	Medium	Medium	Medium
Voice Recognition	Medium	Medium	High	Medium-Low	High	High
Signature Recognition	Low	Medium	High	Low	High	Medium
Hand Geometry	Medium-Low	Low	High	High	Medium	Low

III. RESEARCH METHODOLOGY

The proposed work has been separated into four different parts i) Template protection by public key encryption ii) Template protection by private key encryption iii) key safety by encrypting with template data as key iv) Encrypting consumers data with protected key. Our proposed methodology is suitable for both single and multi-cloud since it is a door step to access cloud and secured data storage in cloud. Cloud auditor plays a vital role in comparing the biometric template and release of key and accessing of key.

In the template protection using public key level biometric template have been encrypted by RSA algorithm, In template protection by private key level the biometric template is going to be encrypted by AES algorithm, In the third level only when the authentication succeeds then the key is going to be released for data encryption and decryption. In the fourth level the consumer's data is going to be protected by means of released key after authentication.

Table.2 List of Notations

NOTATION	DESCRIPTION
CAS	Cloud Authentication Server
CC	Cloud Consumer
CSP	Cloud Service Provider
DP_{KEY}	Data Protection Key
PU_{KEY}	Public Key
PR_{KEY}	Private Key
CADB	Cloud Authentication Db
CA	Cloud Auditor
KD	Data Key
RSA	Rivest,Shammir,Adleman
AES	Advanced Encryption Standard
3DES	Triple Data Encryption Standard

Table.3 Algorithms used in New Protocol

NEW PROTOCOL		
S.NO	ALGORITHM	USES
1	RSA	Template protection by public key encryption
2	AES	Template protection by private key encryption
3	3DES	Key safety by encrypting with template data as key
4	Blowfish	Encrypting consumers data with protected key

As shown in table 3 the proposed NEW protocol we have used biometric finger print for authentication but it can be extended to any type of biometrics. The first two parts of proposed work that is i) Template protection by public key encryption ii) Template protection by private key encryption have been broadly classified into two levels based upon their usage i) Enrolment ii) Authentication. In the enrolment level the cloud consumer has to give their finger print from that features are extracted and converted into template data. This template data is encrypted by public key encryption (RSA) with the key provided by cloud authentication server. Then encrypted key is forwarded to cloud authentication server where is decrypted and again encrypted by private key encryption (AES) and then stored in a cloud database.

In the authentication level the same steps like enrolment have to be carried out until the finger print template data reaches authentication server as shown in Fig.1. Then the equaling template data has been retrieved from cloud data base and comparison will be taken place in decrypted mode with the presence of cloud auditor. If comparison is succeeded consumer is authenticated to access the cloud otherwise rejected. The Authentication process using key encryption and decryption process shown in Fig.2

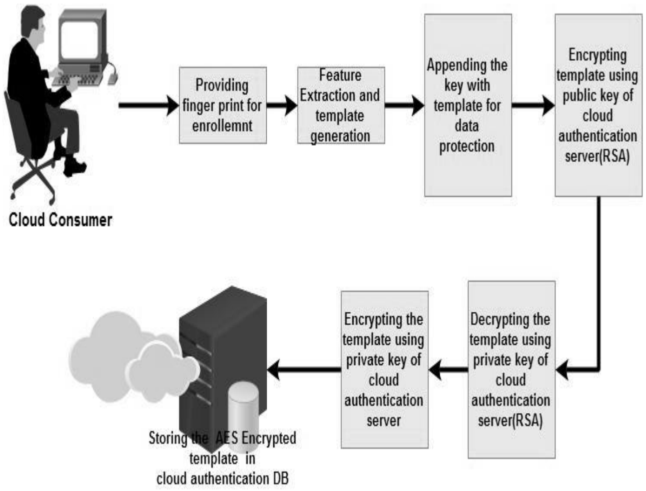
Cloud Consumer
Providing finger print for enrollemnt
Feature Extraction and template generation
Appending the key with template for data protection
Encrypting template using public key of cloud authentication server(RSA)
Decrypting the template using private key of cloud authentication server(RSA)
Encrypting the template using private key of cloud authentication server
Storing the AES Encrypted template in cloud authentication DB

Fig.1 Enrollment

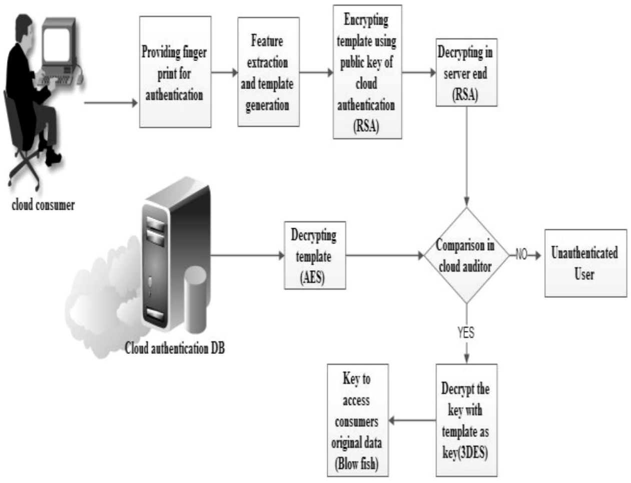
cloud consumer
Providing finger print for authentication
Feature extraction and template generation
Encrypting template using public key of cloud authentication (RSA)
Decrypting in server end (RSA)
Cloud authentication DB
Decrypting template (AES)
Comparison in cloud auditor
NO
Unauthenticated User
YES
Key to access consumers original data (Blow fish)
Decrypt the key with template as key(3DES)

Fig.2 Authentication

The key(Kd) which is used to encrypt the cloud consumers data will be encrypted by finger print template as key(Kk). Fig.3 After the authentication is completed the key (Kd) which has been decrypted (3DES) by finger print template as key(Kk). Then cloud consumers valuable data will be encrypted by blowfish algorithm with the key Kd.

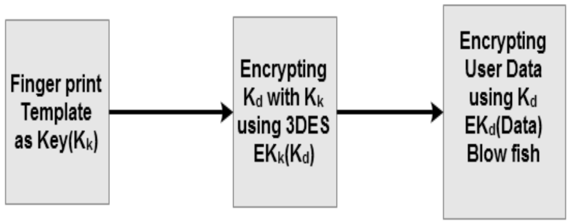
Finger print Template as Key(K_k)
Encrypting K_d with K_k using 3DES $EK_k(K_d)$
Encrypting User Data using K_d EK_d(Data) Blow fish

Fig.3 Data Protection

IV. PROTOCOL DESIGN DESCRIPTION

Different phases of proposed New Protocol

The proposed method have been divided into three basic levels

i. Enrollment Phase
ii. Authentication Phase
iii. Data Protection Phase

I. Enrollment Phase

Step 1: Cloud consumer has to provide the necessary details and finger print to CAS server.

Step 2: Finger print features are extracted using minutiae extraction algorithm and template is generated.

Step 3: CC details and finger print template and the key (DP KEY) for data protection is appended.

Step 4: Requesting for the public key (PU KEY) from CAS Server.

Step 5: Encrypting the template using PU key of CAS server using RSA algorithm and forwarding it CAS Server

Step 6: Decrypting the received template in CAS server using private key (PR key) using RSA algorithm.

Step 7: Encrypt the template using AES algorithm before storing it in cloud authentication Database (CADB).

II. Authentication Phase

Step 1: Cloud consumer has to provide username password along with finger print.

Step 2: Username and password is verified against the database.

Step 3: Finger print features are extracted using minutiae extraction algorithm and template is generated.

Step 4: Requesting for the public key (PU KEY) from CAS Server.

Step 5: Encrypting the template using PU key of CAS server using RSA algorithm and forwarding it CAS Server

Step 6: Decrypting the received template in CAS server using private key (PR key) using RSA algorithm.

Step 7: Collect the already registered AES encrypted template form CADB and decrypt it.

Step 8: Separate the template and the DP key.

Step 9: Now do the comparison using matching algorithm by cloud auditor.

Step 10: Result of the comparison is yes the release the key otherwise unauthenticated user.

III. Data Protection Phase

Step 1: If the result of authentication is yes then decrypt the Key (Kd) using 3DES algorithm.

Step 2: This Kd is used to encrypt and decrypt the user data using blow fish algorithm.

V. RESULTS AND DISCUSSION

Fig.4 Test Data

For cloud hosting layer shift (www.layershift.com) free cloud storage have been used with 15 days validity. In this implementation we have succeeded with the all parameters like template protection, user privacy, security, trust between client and server, cloud data protection , cloud authentication etc. The test data what we have used is obtained from http://www.csee.wvu.edu/ which has thousand different finger prints.

The sample test data has been shown in figure 4.

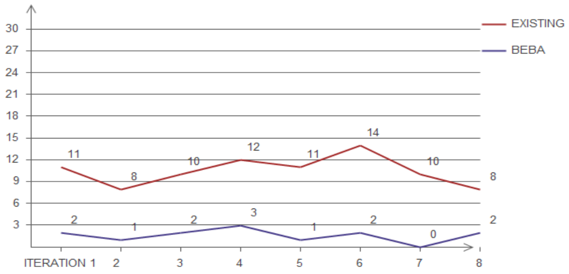

Fig.5 FRR(False Rejection Rate)

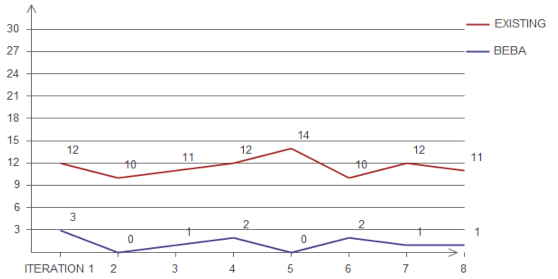

Fig.6 FAR(False Acceptance rate)

The Fig.5 and Fig.6 shows the result analysis has two portions one is false acceptance rate which gives falsely accepting invalid user. And another one is false rejection rate which gives falsely rejecting valid user. In both the results we have tested 30 different fingerprints in eight different iterations in which we got improved results when comparing with the existing work. This result indicates the proposed work improves the security along with reduces false acceptance rate and false rejection rate.

The NEW protocol have been tested against 100 text documents stored in cloud storage and validated against the security parameters like authentication ,confidentiality ,integrity, Data protection. Since all the parameter validations provide 100% result so it increases the confidence about cloud environment.

VI. SECURITY INVESTIGATION OF PROPOSED PROTOCOL

This security investigation explains about the proposed protocol mitigation of possible threats.

(a)BRUTE FORCE ATTACK

Simply using usernames and passwords is very much vulnerable to brute force attack and it is hard to remember the passwords and usernames also. Instead of that biometrics have been used it cannot be guessed and not subject to brute force attack.

(b)TEMPLATE SECURITY

Biometric templates can be hacked from the template database and it can be reused. But in our NEW protocol the biometric template has been protected by two different encryption algorithms.

(c) DENIAL OF SERVICE ATTACK

Since biometrics have been used then client cannot engage DOS attack, and public key encryption is used from server end then server cannot participate DOS attack.

(d)MAN IN THE MIDDLE ATTACK

Such attack is related to attacks in network path . By using NEW methodology no data has been transferred via the insecure network without encryption.

(E) VULNERABILITY IN DIFFERENT PARTS OF THE CLOUD AUTHENTICATION SYSTEM

NEW protocol overcome the risks of vulnerable parts of the cloud environment by means of four different and strong encryption algorithms in different locations in order to protect biometric template and secure authentication mechanism.

(F) CLOUD DATA PROTECTION

The personal data stored in cloud is protected by means of biometric encryption that is encryption key used to protect the data will be only released when the authentication has been successfully completed.

(G) INCREASES CLOUD CONFIDENCE

Since cloud is the place where all the valuable information are getting processed but it is susceptible to heavy risk then adoption of cloud is a problem in order to bring the confidence among cloud the NEW protocol have been designed and implemented.

VII. CONCLUSION

The above said NEW protocol uses four different types of encryption algorithms each has some unique features based upon the place where it has been used. By implementing NEW protocol the trust of cloud usage will be increased drastically. Though the authentication is very much secure enough it reduces identity theft, un authorized access, Denial of service etc. And Data breaches and data protection is maintained by Encryption with double protected key usage. And also Security, Privacy of data will be protected.

In future the same work can be carried out with different biometrics, since we used finger print with different encryption algorithms and more number of cloud servers. The levels of key encryption can also be increased if we need greater security. Not only it will be used in cloud environment but it can be used in the situations where we need greater security and increased use of authentication. To increase the overall security and template protection one time passwords can be used.

REFERENCES

1. Lee, S., Ong, I., Lim, H. T., & Lee, H. J. (2010). Two factor authentication for cloud computing. Journal of information and communication convergence engineering, 8(4), 427-432.
2. Jain, A. K., Ross, A., & Prabhakar, S. (2004). An introduction to biometric recognition. Circuits and Systems for Video Technology, IEEE Transactions on, 14(1), 4-20.
3. Ratha, N. K., Connell, J. H., & Bolle, R. M. (2001). Enhancing security and privacy in biometrics-based authentication systems. IBM systems Journal,40(3), 614-634.
4. Sudhan, S. K. H. H., & Kumar, S. S. (2015). An Innovative Proposal for Secure Cloud Authentication using Encrypted Biometric Authentication Scheme. Indian Journal of Science and Technology, 8(35).
5. Rivest, R. L., Shamir, A., & Adleman, L. (1978). A method for obtaining digital signatures and public-key cryptosystems. Communications of the ACM,21(2), 120-126.
6. Balaji S, S. Saravanakumar., "Performance Evaluation of Security and Privacy Challenges in Cloud Computing Services"-JARDCS ISSN 1943-023X issue 12-2017.