DEVELOPING THE ENCRYPTION, API, ARCHITECTURE AND SECURITY OF BIOMETRIC TECHNOLOGY

Ms. Y. Jyosthna[1]
3rd Year Student,
Department of Computer Science,
SV U CM & CS, Tirupati.

Prof. G. Anjan Babu[2],
Professor,
Department of Computer Science,
SV U CM & CS,, Tirupati.

Abstract: In this paper we introduce a new projected protocol, BEBA (Biometric encoding and Biometric authentication) to over come all the security problems in cloud surroundings. Most of the safety problems are associated with authentication and information protection with respect to cloud security alliance (CSA). In BEBA protocol, biometric encryption has been provided for cloud consumer's valuable information and identity verification has been utilized in a unique way. Identity verification has been combined with template protection in conjunction with four completely different and powerful (RC4, RSA, AES and 3DES) encryption algorithms for accumulated safety. Blowfish has been used in data protection and key safety management. Adopting this protocol has given nice results when examining with existing work and all vulnerable places has been considered for improved security.

Keywords: *M-commerce, Cloud, Biometric Encryption, Cryptography, Authentication Protocol, Identity Verification.*

INTRODUCTION

M-commerce using Cloud computing is the future of computing with plenty of advantages. It has not been adopted by every industry because of its security concerns. Cloud reference architecture has four deployment models (public, private, community and hybrid) and three service models (SAAS, PAAS, IAAS)as stated in NIST [1, 2]. Among these, public and hybrid clouds are the major models where the cloud consumers are afraid of storing their personal data, as all the data are stored and used in off premises without the knowledge of consumer. Service models like SAAS and IAAS are more vulnerable to threats because data can be stored, used and manipulated. In SAAS the user's data is given as input for manipulation and high end processing. IAAS cloud is just like a remote desk top which stores all our data and computations. Hence it is at greater risk for threats. It has been stated in notorious nine articles (published by cloud security alliance (CSA) in 2013) that nine major

Problems affect the trust of cloud usage among which lack of authentication is the major cause [3]. Nine major problems mentioned in the article are; 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. Among these, only 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 as it doesn't require customer to possess or remember anything (eg, PIN number) yet it gives greater security [4]. However, Biometric authentication is not effective when the biometric templates are not stated and used securely. Different ways to protect biometric templates using different types of encryption schemes has been stated in an innovative proposal for secure cloud authentication using encrypted biometric authentication scheme [5, 6].Once the template is secure then there is no compromise in biometric authentication module and hence the security of cloud environment is increased [7–9].In this paper along with biometric authentication, biometric encryption has also been used in the presence of cloud auditor. Also 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.

PROPOSED SYSTEM

The proposed work has four different modules

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.

proposed methodology is suitable for both single and multi-cloud environment since it is a door step to access cloud and secured data storage. Cloud auditor plays a vital role in comparing the biometric template and release of key and accessing of key. For the template protection using public key level, biometric template was encrypted by RSA algorithm and for the template protection by private key level the biometric template was encrypted by AES algorithm [16, 17].

When authentication succeeds at the third level, the key is released for data encryption and decryption. At the fourth level, the consumer's data is protected by a released key after authentication [17, 20].We have also used biometric finger print for authentication in this protocol. But BEBA protocol can be extended to any type of biometrics.

The first two modules of proposed work that is; Template protection by public key encryption and 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 mobile cloud consumer was made to give their finger print for identification.

The given fingerprint features were extracted and converted into template data using Minutiae feature extraction algorithm. This template data is encrypted by public key encryption (RSA) [29] with the key provided by cloud authentication server. Then encrypted key was forwarded to cloud authentication server where it was decrypted and re-encrypted by private key encryption (AES) and was then stored in a cloud data base. In the authentication level, same steps were carried out until the finger print template data reaches authentication server.

Then the equaling template data was retrieved from cloud data base and comparison of fingerprints was done in decrypted mode with the presence of cloud auditor. The given fingerprint was compared with the fingerprint template, and when it succeeds, consumer was authenticated to access the cloud environment. The Authentication process using key encryption and decryption process has been shown in Fig. 2 and Fig. 3The key (Kd) which is used to encrypt the cloud consumers data is encrypted by his finger print template as

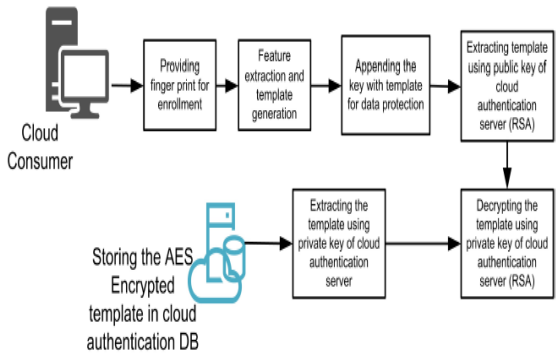

Fig. 1: Enrollment.

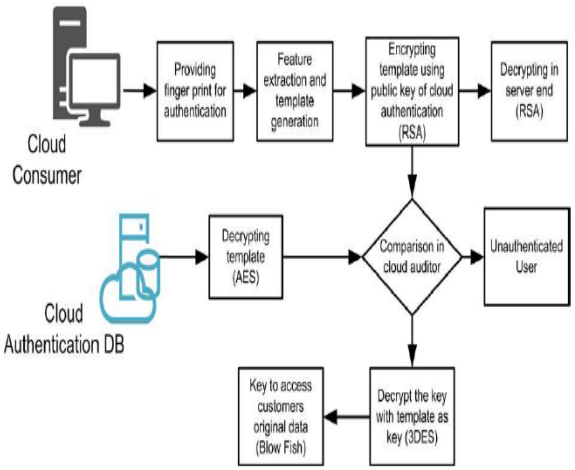

Fig. 2: Authentication.

k ey(Kk). After the authentication is completed the key(Kd) is decrypted (3DES) by finger print template askey(Kk). Then cloud consumers valuable data will beencrypted by blowfish algorithm with the key Kd [29].

PROTOCOL DESIGN DESCRIPTION

The proposed BEBA Protocol method have been divided into three phases are

1. Enrollment Phase

2. Authentication Phase

3. Data Protection Phase

4.1 Enrollment Phase

Consumer (user) sends the Product and customer details to the Service provider through the WAP gateway. The overall phase steps is explained below.

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(DPKEY) for data protection is appended.

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

Step 5: Encrypting the template using PUKEY) 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).

Authentication Phase Service provider verifies the Product & consumer details and sends to the Biometric server through the WAP gateway.

The overall steps are explained below:

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

2: Username and password is verified against the database.

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

4: Requesting for the public key (PUKEY) from CAS Server.

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

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

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

8: Separate the template and the DPKEY

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

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

DATA PROTECTION PHASE

Biometric server sends the Comparison result details to the Service provider. Analyzing the matching score service provider decides access or denies the process ofcustomer.1: If the result of authentication is yes then decrypt the Key (Kd) using 3DES algorithm.

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

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 BEBA 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 BEBA methodology no data has been transferred via the insecure network without encryption.

(E) Vulnerability in Different Parts of the M-Commerce Cloud Authentication System: BEBA 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 toprotect 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 BEBA protocol have been designed and implemented.

RESULT ANALYSIS

The proposed BEBA protocol was implemented in Intel Pentium duo core processor with 4 GB RAM and 160 GB hard disk was used for all the experiments done as shown in Fig. 5. Windows XP operating system was used in these experiments. Visual studio 2008 and MY SQL were used as front end designing and for back end data storage respectively. Two parameter have been used for determination of accuracy of the system which includes FMR and FNMR. Free cloud storage with 10 days validity was used for cloud hosting layer shift (www.layershift.com). We were successful in implementing all the parameter like user privacy, template protection, security trust between client and server, cloud data protection, cloud authentication etc. in this experiment. The development language Java has been used. For RSA, AES, 3DES, and Blowfish We used opensource software codes from internet. For test data we usedBiometrics ideal test website with the URL ofhttp://biometrics.idealtest.org.The accuracy of the system is determined based onthe two parameters i.e. False Match Rate (FMR) andFalse Non Match Rate (FNMR). The false match isoccurring when an unregistered finger is falsely matched.For cloud hosting layer shift (www.layershift.com) freecloud storage have been used with 15 days validity. In this implementation we have succeeded with the allparameters like template protection, user privacy, security,trust between client and server, cloud data protection,cloud authentication etc. The

test data what we have usedis obtained from http://www.csee.wvu.edu/ which has thousand different finger prints.

CONCLUSION

The proposed BEBA protocol uses four different types ofencryption algorithms each has some unique featuresbased upon the place where it has been used. Byimplementing BEBA protocol the trust of cloud usagewill be increased drastically. The experimental resultsrevealed that the RC4 algorithm using BEBA protocol is faster and more effective in execution time and security concern as compared with other algorithms. The secrecyis analyzed and compared among DES, 3DES, AES, RC4algorithms in the mobile environment. Even there is no much variation in execution time in mobile with different mobile processor speed and RAM size. It is showing onlydifference while increasing/decreasing the mobileprocessor speed and RAM size. From these experimentresults, it is inferred that the execution time is notcompletely dependent on the processor speed and RAMof the mobile. So the advantage of this architecture is thatit can be implemented in any mobile environmentirrespective of the processor speed and RAM size.

Our proposed model also puts the light on certainvulnerability and wireless link threats in commercetransactions, such as payment security risks that needcertain improved security solutions. Though theauthentication is very much secure enough it reducesidentity theft, un authorized access, Denial of service etc.Data breaches and data protection is maintained by encryption with double protected key usage and alsosecurity, privacy of data will be protected.In future the same work can be carried out withdifferent biometrics, since we used finger print withdifferent encryption algorithms and more number ofcloud servers. The levels of key encryption can also beincreased if we need greater security. Not only it will be used in cloud environment but it can be used in thesituations where we need greater security and increaseduse of authentication. To increase the overall security andtemplate protection one time passwords can be used.

REFERENCES

[1] Lee, S., Ong, I., Lim, H.T. and Lee, H.J., Two factorauthentication for cloud computing, Journal of Informationand Communication Convergence Engineering, 8(4), 427–432, 2010.

[2] NIST SP 500–292, Cloud Computing ReferenceArchitecture: An Overview National Institute of Standardsand Technology, 3–4, 2011

[3] Jain, A.K., Ross, A. and Prabhakar, S., An introduction tobiometric recognition, IEEE Transactions on Circuits andSystems for Video Technology, 14(1), 4–20, 2004.

[4] Ratha, N.K., Connell, J.H. and Bolle, R.M., EnhancingSecurity and Privacy in Biometrics-based AuthenticationSystems, IBM Systems Journal, 40(3), 614–634, 2001.

[5] Sudhan, S.K.H.H. and Kumar, S.S., An Innovative Proposalfor Secure Cloud Authentication using Encrypted BiometricAuthentication Scheme, Indian Journal of Science andTechnology, 8(35), 2015

[6] Rivest, R.L., Shamir, A. and Adleman, L., A methodfor Obtaining Digital Signatures and Public-keyCryptosystems, Communications of the ACM, 21(2),120–126, 1978.

[7] Gorman, L.O., Comparing Passwords, Tokens, andBiometrics for User Authentication, Proceedings of theIEEE, 91(12), 2021–2040, 2003.

[8] Upmanyu, M., Namboodiri, A.M., Srinathan, K. andJawahar, C.V., Blind Authentication: A Secure Crypto Biometric Verification Protocol, IEEE Transactions onInformation Forensics and Security, 5(2), 255–268, 2010..

[9] Kavinhariharasudhan S. and Ramamoorthy, S., DoubleEncryption Based Secure Biometric AuthenticationSystem, International Journal of Engineering Trends andTechnology, 3(1), 64–70, 2012.

[10] Kadam, Y., Security Issues in Cloud Computing ATransparent View, International Journal of ComputerScience Emerging Technology, 2(5), 316–322, 2011.

[11] Vouk, A., M-Cloud Computing–Issues, Research andImplementations, CIT. Journal of Computing andInformation Technology, 16(4), 235–246, 2008.

[12] Kavinhariharasudhan S., Saravanakumar, S., An Efficientand Secure Dynamic Multidimensional Cloud Confidence,International Journal of Applied Engineering Research-2015.

Authors Profile

JYOTHSNA YEDDULA, received Bachelor of Computer Science degree from Sri Venkateswara University, Tirupati in the year of 2013-2016. Pursuing Master of Computer Applications from Sri Venkateswara University, Tirupati in the year of 2016-2019. Research interest in the field of Computer Science in the area ofArtificial Intelligence, Machine learning, Big Data, Network Security, Networkingand Software Engineering.