Applied Mathematics & Information Sciences
An International Journal

http://dx.doi.org/10.18576/amis/120126

Biometric Encoding and Biometric Authentication (beba) Protocol for Secure Cloud in M-Commerce Environment

R. ArunPrakash[1,*], *T. Jayasankar*[2] *and K. Vinothkumar*[3]

[1] Department of Computer Science and Engineering, University College of Engineering, Ariyalur, Tamilnadu, India.
[2] Department of ECE, University College of Engineering, Anna University, BIT Campus, Tiruchirappalli,Tamilnadu, India
[3] Department of ECE, K. Ramakrishnan College of Engineering, Tiruchirappalli, Tamilnadu, India

Received: 13 Nov. 2017, Revised: 22 Dec. 2017, Accepted: 27 Dec. 2017
Published online: 1 Jan. 2018

Abstract: In this paper we introduce a new projected protocol, BEBA (Biometric encoding and Biometric authentication) to overcome 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.

1 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 affects 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

* Corresponding author e-mail: arunitvijay@yahoo.com

innovative method will change the vision about cloud environment and increase the number of consumers for using cloud environment.

2 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 [10, 11].

One of the foremost fashionable user authentication schemes was the server stores the encrypted value of a user's password. In this theme, password table was wont to verify the legitimacy of users, however if this password table is compromised, stolen, or changed by an adversary, then the system may well be part or fully compromised. Some more modern smart card primarily based password authentication schemes have additionally been projected in. Another model that relies on three half key distribution protocols. Smartcard is employed to store the long run secret key and it's assumed that the smartcard is rarely compromised. Thus essentially the theme falls in one issue schemes will be broken by compromising each the factors solely. Authentication consolidate variety of positive identifications and smartcard based mostly properties and planned to issue smartcard, password authentication theme, that continues to be prone to several attacks [16–19].

Cloud computing may be a variant of client server design, where, thousands of clients use a similar infrastructure at an oversized scale. Consequently, it desires stronger authentication than standard client server inter-networking system have planned public key and mobile out of band based mostly authentication for cloud computing. Some systems use a lot of difficult authentication using the smartcard system. wherever a user usually has an ID, a password, and conjointly a time-generated master key from the smart card that changes each sixty seconds [20–22]. This represents the case possessing one thing physically. Biometrics authentication is safer mechanism within user should demonstrate what you're. Biometrics credentials will take several dimensions, from finger prints, to retinal scans to pupil pictures etc. As we are able to see from higher than, authentication is that the key for info security [23, 24].

Most of the prevailing user authentication schemes have several security flaws. password authentication is that the most typically used theme, however this technology is susceptible to eavesdropping, replay, thorough and wordbook attacks etc. during this paper we've addressed most of the safety issues of cloud computing and have developed a secure user authentication framework for cloud computing. Most of the prevailing authentications area unit supported static passwords whereas the planned theme relies on dynamic secure multi-factor out-of-band secret-splitting mechanism that is safer, economical and user friendly [25–27].

Specifically in public and hybrid cloud the valuable data has been processed in off premise. 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 [28, 29]. But template security is the major issue in biometrics [12, 13]. 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 a un-trusted 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 [14, 15]. In this BEBA 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.

3 Proposed work

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. Our 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

Table 1: Algorithms used in BEBA protocol.

S. No.	Algorithms	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

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].

Table 1 gives the list of algorithms used in our proposed BEBA protocol. 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 as shown in Fig. 1 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. 3

The key (Kd) which is used to encrypt the cloud consumers data is encrypted by his finger print template as key(Kk). After the authentication is completed the key (Kd) is decrypted (3DES) by finger print template as key(Kk). Then cloud consumers valuable data will be encrypted by blowfish algorithm with the key Kd [29].

4 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 (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).

4.2 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 (PU_{KEY}) 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 DP_{KEY}
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.

4.3 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 of customer.

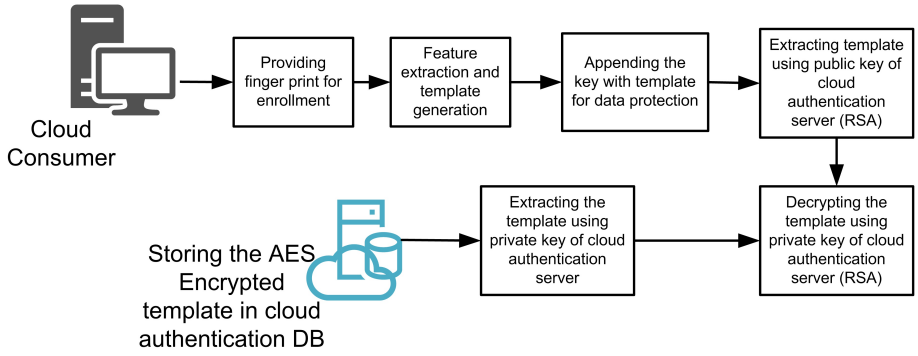

Fig. 1: Enrollment.

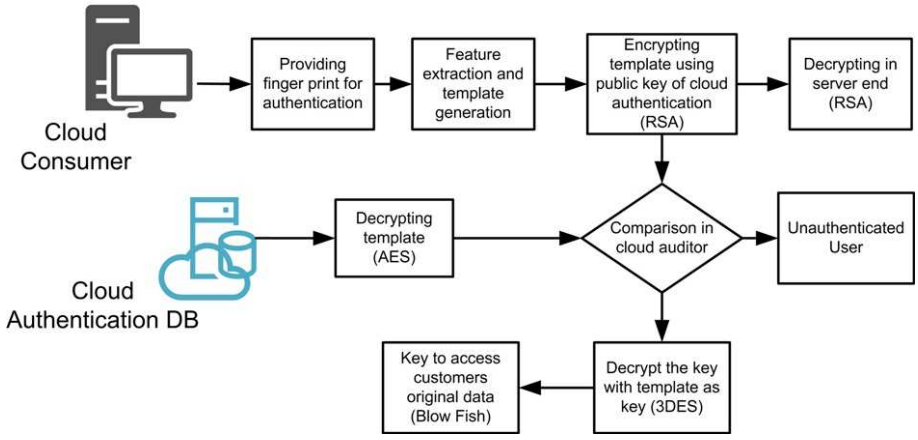

Fig. 2: Authentication.

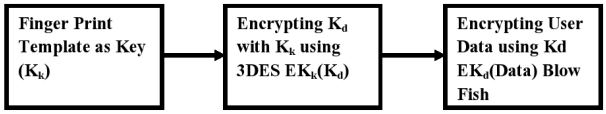

Fig. 3: Data Protection.

1: If the result of authentication is yes then decrypt the Key (K_d) using 3DES algorithm.
2: This K_d is used to encrypt and decrypt the user data using blow fish algorithm.

4.4 Algorithms used in this protocol

After binarization and thinning of the image, Minutiae features is extracted from the resultant image. In this algorithm, the white pixels as 1 and black pixels as 0 is considered. The algorithm used 3×3 windows to scan the image and the bifurcation and termination in the final output image is represented by a dot. Then, the concept of Crossing Number (CN) is applied for extracting the minutiae. The CN for a pixel P is calculated by using Eq. (1) as follows

$$CN = \frac{1}{2}\sum_{i+1}^{\beta} P_i - P_{i+1} \tag{1}$$

where, P_i is the binary pixel value in the neighborhood of P with $P_i = (0 \text{ or } 1)$ and $P_9 = P_1$. Based on the CN value, it is considered that the minutiae point may have ridge ending or bifurcation.

4.4.1 Minutiae Extraction Algorithm

The Minutiae Feature Extraction Algorithm (MEA) is calculated by sample finger print which is shown in Fig. 4 by ridge and bifurcation. The steps in our minutiae feature extraction algorithm are given below.

1. In Client end gather multiple samples of biometric of User.
2. Feature vector X_i is calculated from the given sample.
3. Situate the central core of the finger print.
4. Establish the x and y coordinates values of each feature vector.
5. The distance from each feature vector value from core has been computed.

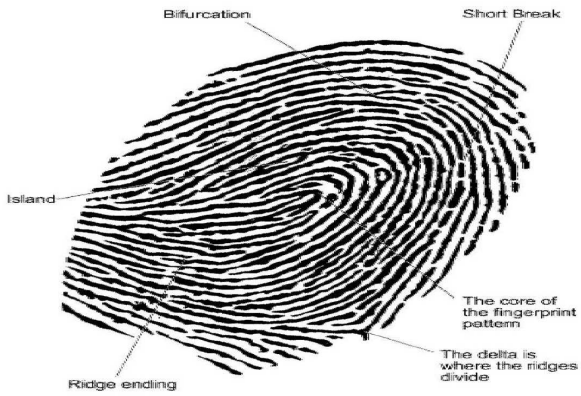

Fig. 4: Sample image of finger print model represented with features.

6. (x,y) and distance D is jointly called as minutiae.

4.4.2 Cryptographic Algorithms

The trustful M-commerce transactions can be made only in the system containing above said traits. For obtaining such traits, the help of techniques like cryptography in M-commerce transactions is considered. There is two kind of the cryptographic techniques that are:

–Symmetric key cryptographic techniques (RC4, DES, 3DES, AES)
–Asymmetric key cryptographic techniques (RSA, DSA, HECC)

When symmetric algorithms are compared with the asymmetric one, the former is the simplest one than the latter. The simplicity of symmetric algorithm is because only one key is utilized for both encryption and decryptions; hence it quickly processes the data as compared to Asymmetric algorithms.

5 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 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 BEBA protocol have been designed and implemented.

6 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 open source software codes from internet. For test data we used Biometrics ideal test website with the URL of http://biometrics.idealtest.org.

The accuracy of the system is determined based on the two parameters i.e. False Match Rate (FMR) and False Non Match Rate (FNMR). The false match is occurring when an unregistered finger is falsely matched. 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,

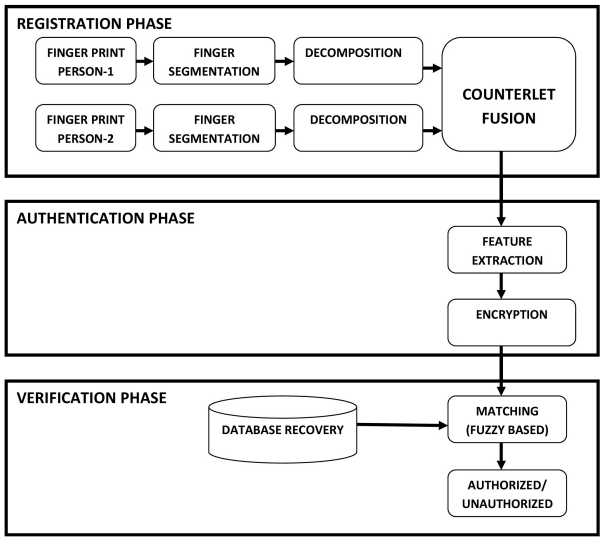

Fig. 5: Authentication using BEBA Protocol.

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 Fig. 6. The Figs. 7 and 8 show 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. The *FRR* and *FAR*, is then computed according to the following Eqs. (2) and (3).

$$FRR = ((X^i/Y^j) \times 100\%) \tag{2}$$

where X^i is the Number of genuine claims,
Y^j is the Number of genuine accesses.

$$FAR = \sum(P/Q) + CZ \tag{3}$$

where P is the number of false positives,
Q is the number of false positives and
Z is the number of true negatives.

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 BEBA 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.

The simulated secrecy value results indicate that the RC4 algorithm using BEBA protocol has greatest secrecy value as compared to other algorithms like AES, DES, and 3DES is shown in Fig. 9. Lowest secrecy value is shown by AES, although it is closely related to DES also.

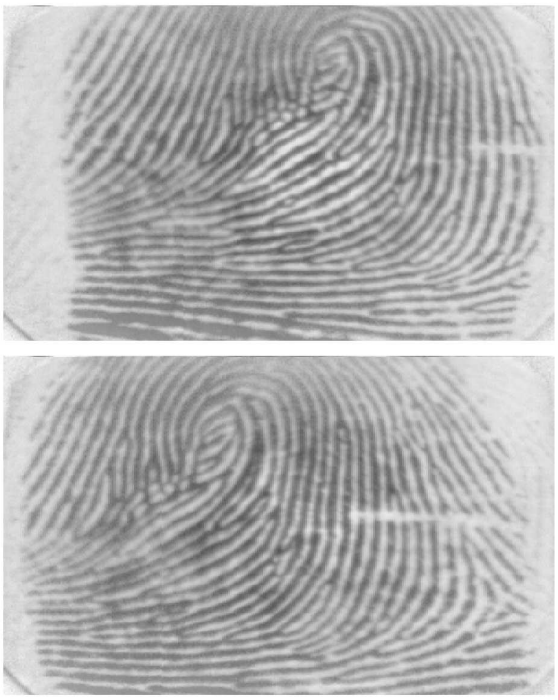

Fig. 6: Test data.

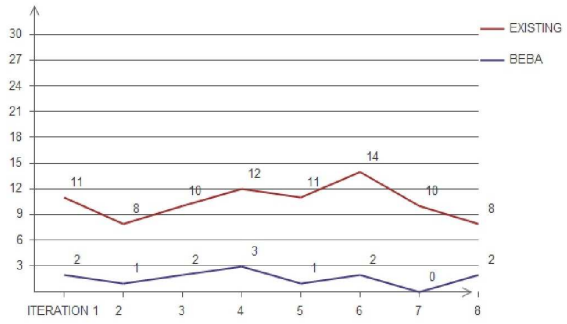

Fig. 7: *FRR* (False Rejection Rate).

According to Shannon's theory, an algorithm with highest secrecy value is the most secured one. Hence based on this analysis BEBA Protocol is the most secured one, unlike other algorithms.

7 Conclusion

The proposed BEBA protocol uses four different types of encryption algorithms each has some unique features based upon the place where it has been used. By implementing BEBA protocol the trust of cloud usage will be increased drastically. The experimental results revealed that the RC4 algorithm using BEBA protocol is

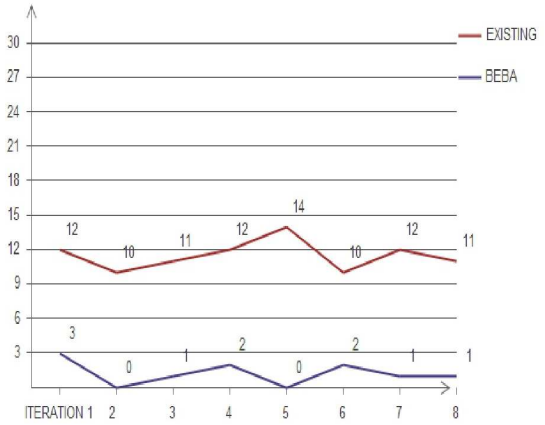

Fig. 8: *FAR* (False Acceptance rate).

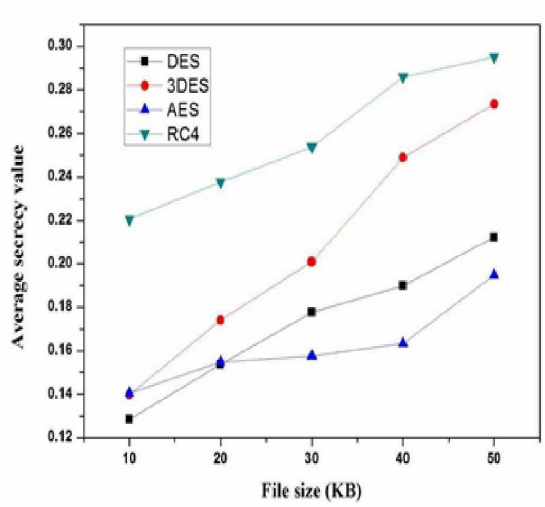

Fig. 9: Average secrecy values vs. file size for different cryptographic attacks for algorithm.

faster and more effective in execution time and security concern as compared with other algorithms. The secrecy is analyzed and compared among DES, 3DES, AES, RC4 algorithms 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 only difference while increasing/decreasing the mobile processor speed and RAM size. From these experiment results, it is inferred that the execution time is not completely dependent on the processor speed and RAM of the mobile. So the advantage of this architecture is that it can be implemented in any mobile environment irrespective of the processor speed and RAM size.

Our proposed model also puts the light on certain vulnerability and wireless link threats in commerce transactions, such as payment security risks that need certain improved security solutions. Though the authentication is very much secure enough it reduces identity theft, un authorized access, Denial of service etc. 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. and Lee, H.J., Two factor authentication for cloud computing, Journal of Information and Communication Convergence Engineering, **8(4)**, 427–432, 2010.

[2] NIST SP 500–292, Cloud Computing Reference Architecture: An Overview National Institute of Standards and Technology, 3–4, 2011

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

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

[5] Sudhan, S.K.H.H. and Kumar, S.S., An Innovative Proposal for Secure Cloud Authentication using Encrypted Biometric Authentication Scheme, Indian Journal of Science and Technology, **8(35)**, 2015

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

[7] Gorman, L.O., Comparing Passwords, Tokens, and Biometrics for User Authentication, Proceedings of the IEEE, **91(12)**, 2021–2040, 2003.

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

[9] Kavinhariharasudhan S. and Ramamoorthy, S., Double Encryption Based Secure Biometric Authentication System, International Journal of Engineering Trends and Technology, **3(1)**, 64–70, 2012.

[10] Kadam, Y., Security Issues in Cloud Computing A Transparent View, International Journal of Computer Science Emerging Technology, **2(5)**, 316–322, 2011.

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

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

[13] Brunette, G. and Mogull, R., Security guidance for critical areas of focus in cloud computing, **v2.1**, Cloud Security Alliance, 1–76, 2009.
[14] Ristenpart, T., Tromer, E., Shacham, H. and Savage, S., Hey, You, Get off of My Cloud: Exploring Information Leakage in Third-Party Compute Clouds, In Proceedings of the 16th ACM conference on Computer and communications security ACM., November 2009, pp. 199–212.
[15] Lampson, B., Abadi, M., Burrows, M. and Wobber, E., Authentication in Distributed Systems: Theory and Practice, ACM SIGOPS Operating Systems Review, **25(5)**, 165–182, 1991.
[16] Kavinhariharasudhan S, Saravanakumar S., A Review On Approaches to Shield Against Ddos Attack in Cloud Computing, International Journal of Emerging Technology & Research-2014.
[17] Lamport, L., Password Authentication with Insecure Communication, Communications of the ACM, **24(11)**, 770–772, 1981.
[18] Lin, C.L. and Hwang, T., A Password Authentication Scheme with Secure Password Updating. Computers & Security, **22(1)**, 68–72, 2003.
[19] Peyravian, M. and Zunic, N., Methods for Protecting Password Transmission, Computers & Security, **19(5)**, 466–469, 2000.
[20] Saravanakumar, S., Secure Services for Efficient Online Data Storage Using Cloud Computing, International Journal of Advanced Research in Computer Science and Software Engineering, **3(11)**, 195–200, 2013.
[21] Jain, A.K., Ross, A. and Pankanti, S., Biometrics: A Tool for Information Security, IEEE Transactions on Information Forensics and Security, **1(2)**, 125–143, 2006.
[22] Hwang, M.S. and Li, L.H., A New Remote User Authentication Scheme Using Smart Cards, IEEE Transactions on Consumer Electronics, **46(1)**, 28–30, 2000.
[23] Kavinhariharasudhan S., Saravanakumar, S., A Panoptic Survey on Cloud Computing, International Journal of Research in Engineering Technology and Management, **2(3)**, 1–5, 2014.
[24] Chien, H.Y., Jan, J.K., and Tseng, Y.M., An Efficient And Practical Solution to Remote Authentication: Smart Card, Computers & Security, **21(4)**, 372–375, 2002.
[25] Liao, I.E., Lee, C.C., and Hwang, M.S., A Password Authentication Scheme Over Insecure Networks, Journal of Computer and System Sciences, **72(4)**, 727–740, 2006.
[26] Buyya, R., Yeo, C.S., Venugopal, S., Broberg, J., and Brandic, I., Cloud Computing and Emerging IT platforms: Vision, Hype, and Reality for Delivering Computing as the 5th Utility, Future Generation Computer Systems, **25(6)**, 599–616, 2009.
[27] Saravanakumar S., Efficiency Method for Storing a Information over Secure Cloud Computing, International Journal of Innovative Research in Computer and Communication Engineering, **3(10)**, 9936–9940, 2015.
[28] Sharif, A.M., It's written in the Cloud: The Hype and Promise of Cloud Computing. Journal of Enterprise Information Management, **23(2)**, 131–134, 2010.
[29] Subashini, S. and Kavitha, V., A Survey on Security Issues In Service Delivery Models of Cloud Computing, Journal of Network and Computer Applications, **34(1)**, 1–11, 2011.

R. Arun Prakash received B.Tech. degree in Information Technology from Bharathidasan University, Trichy in 2003, M.Tech. degree in Information Technology at Sathyabama University, Chennai in 2005 and Ph.D. degree in M-Commerce at Anna University Chennai 2016. At present, he is an Assistant Professor in the Computer science and Engineering Department, University College of Engineering, Ariyalur, Anna University, Tamilnadu, India. He is a member of ISTE. He has been a lecturer at graduate and post-graduate level and has participated in a number of International and National level conferences and workshops. He has published around 18 papers in the reputed international journals and more than 10 papers in the international and national conferences and contributed two book chapters. His main interest is currently M-commerce, Mobile computing, image processing and wireless networks.

T. Jayasankar received the B.E. degree in Electronics and Communication Engineering from Bharathiyar University, Coimbatore in 2001 and M.E. degree at Madurai Kamaraj University,Madurai in 2003 and Ph.D.in Speech Processing at Anna University Chennai 2017. At present, he is an Assistant Professor in the Electronics and Communication Engineering department, University College of Engineering, Anna University, Bharathidasan Institute of Technology Campus, Tiruchirappalli, Tamilnadu, India. He is a member of IEI, ISTE. He has been a lecturer at graduate and post-graduate level and has participated in a number of International and National level conferences and workshops. He has published around 25 papers in the reputed international journals and more than 15 papers in the international and national conferences. His main interest is currently speech synthesis, speech and image processing and wireless networks.

K. Vinoth Kumar working as Assistant Professor in K. Ramakrishnan College of Engineering, Tiruchirappalli, Tamil Nadu, India. He received the Bachelor's degree in Electronics and Communication Engineering from the Kurinji College of Engineering and Technology, Manapparai, Tamilnadu, India, in 2009. He received the Master's degree in Applied Electronics from the J.J. College of Engineering and Technology, Tiruchirappalli, Tamil Nadu, India, in 2011. He received the Ph.D. in Karpagam University Coimbatore, Tamil Nadu, India in 2017. He is a member in Universal Association of Computer and Electronics Engineer (UACEE) and member in International Association of Engineer (IAENG). He published more than 25 International Journals. His research interests include wireless communication, Mobile Ad hoc networks, and Sensor Networks and Communication networks. He has published in 2 science indexed journals and 5 Scopus Indexed journals.