Journal of Engineering and Applied Sciences 13 (8): 2018-2022, 2018
ISSN: 1816-949X

Amalgamation of Iris Biometrics and Cryptography in Cloud Computing for Improved Authentication

[1]K. Priyadarsini and [2]S. Saravanakumar
[1]Department of Computer Science Engineering, Vels University, Chennai, India
[2]Department of Computer Science Engineering, Karpagam College of Engineering,
Coimbatore, Tamil Nadu, India

Abstract: In information and telecommunication technology has infiltrated deep into the human lives and is influencing human lifestyle in diverse aspects. The fast growth in information and telecommunication technology has embarked progress in computing devices and computing techniques. At present cloud computing is one of the most hyped improvements. It has several constructive impacts like reduced cost, augmented throughput, ease of use but it also had certain security problems that must be dealt with cautiously. There are several techniques that can be used to overcome this major setback. Cloud computing is offering a platform for sharing resources, services and information between the people and organizations across the world. The current developments in cloud computing technology illustrate an increase in security, privacy and trust related issues in many ways which haven't been visage by the ones who have been designing cloud environments. Still, most of the organizations are not moving to cloud computing due to lack of trust in the cloud environment. To overcome such issues authentication and data protection have to be enhanced. In this study novel, iris based authentication has been combined to cryptography for reduction of above-said issues.

Key words: Authentication, biometrics, cryptography, data protection, iris, public key, secret key

INTRODUCTION

The notion of cloud computing took recognition in 1990's though its concepts last back to 1960's. Cloud computing refers to the provision of scalable and IT related services to the users through internet. Iris based authentication is a technique of computing in which vigorously scalable and IT related resources are supplied as a service through internet. This model allows general, supportive and easy to use the system. The resources in cloud computing are rapidly allocated and are released with a minor organization's effort. Resources may include software, storage, systems, servers, platform and infrastructure. Cloud computing provides three different kinds of service models (Hogan *et al*., 2011).

Software as a Service (SaaS): SaaS has the capacity to provide user any software running on a cloud substructure. The software is deployed over the internet. In these type customers licenses, the applications and the cloud service providers offer the required facility to the end users when they need. Examples may include web browsers and Google docs.

Platform as a Service (PaaS): Platform can also be provided as a service. In this, any kind of platform (i.e., tools, library, services) is provided as a service of which user has no control but they can use it. The user can simply generate applications by using PaaS offered by CSP. Commonly virtual machines are used in this case. Most preferably diverse types of tools and applications are deployed to facilitate the users.

Infrastructure as a Service (IaaS): Infrastructure assists the user by providing computing resources where the user can run the software without having control on underlying infrastructure but has control over the operating system being used. IaaS may comprise IT resources such as servers, networking, and storage. Users get admission to the infrastructure with the help of virtual machines. It provides a flexible architecture which offers the high rate of availability. Four deployment models are used in cloud computing.

Public cloud: It facilitates general public and is owned by a specific organization.

Community cloud: Number of private organizations with similar need constructs and maintains community cloud.

Private cloud: It facilitates a private organization. They can be secured privately.

Corresponding Author: K. Priyadarsini, Department of Computer Science Engineering, Vels University, Chennai, India

Hybrid cloud: This structure consists of two or more than two cloud models. Cloud computing services are being provided by different organizations known as Cloud Service Providers (CSPs) (Krutz and Vines, 2010). CSPs offer the services to users on pay only for use approach. Cloud computing deal with various types of security concerns that include virtualization technology security, vast distributed processing technology, availability, massive traffic, application security, access control and authentication. Cloud computing platform has not provided suitable physical protection procedures and all protection mechanisms depend extremely on the mechanism of authenticating the user. User authentication calls for a particularly assured security (Sudhan and Kumar, 2014, 2015).

Security issues are solved in cloud computing by different techniques. One of the most accepted authentication mechanism is password authentication. Most clients pick something easy to memorize for example, phone numbers and names as their passwords. These passwords are very easy to remember but vulnerable. Thus, the adversary can easily accumulate a chart of significant names or numbers to intervene the security. This procedure is known as the dictionary attack (Sudhan and Kumar, 2016; Vielhauer, 2005; Zissis and Lekkas, 2012).

"Biometrics" is a Greek word, "Bio" means life and "metric" means to measure. Biometric authentication states the evidence of the identity of humans by their characteristics or traits. Biometric traits are unanimously unique. Biometric frameworks permit identifiable proof of people taking into account behavioral or physiological attributes. To achieve more dependable confirmation or ID we have to utilize something that truly describes the individual (Jain *et al*., 2006).

Biometrics is largely centered on the face, fingerprint and iris verification and identification systems. In detection procedure, the system checks whether face, iris, fingerprint be present for reading procedure and do not match with the existing data. After enrollment when the user needs to use the service of cloud, detection is pursued by the verification process. During this process data detected by the system is matched with the previously existing data. If any match occurs then the user is authorized to use the service otherwise not. Biometrics deal with character checking or distinguishing proof on the standard of quantifiable physiological or behavioral qualities. A biometric system consists of four levels including sensor level, feature extraction, matching module and the decision module (Raghava, 2011) (Fig. 1).

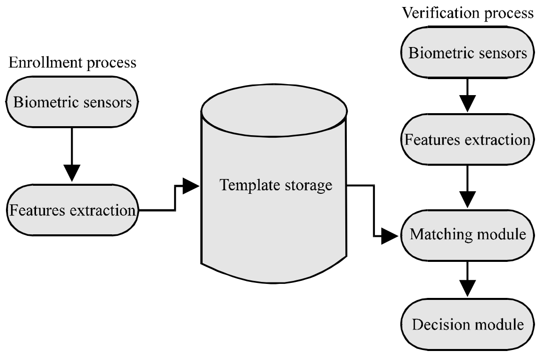

Fig. 1: Biometric authentication processes

Existing work: Iris is a round part surrounding the pupil within the human eye. It consists of diverse complex preparations and is green, blue, black or gray in color. Iris recognition is a method used to appreciate individuals based on unique preparations in iris. Patterns present in iris are identifiable and are distinctive to every human. It is used as an important and highly reliable biometric recognition technique (Bowyer *et al*., 2008).

In this method identification and verification processes are carried out. In identification procedure image of the eye is taken by means of a digital camera of high resolution. The image can be treated by using infrared or visible waves. It is stored in the database of the CSP. In verification procedure, the computer checks whether the image was taken match with the already stored image of the iris or not. The computer program used for the matching function is called a matching engine. The correctness of iris recognition is more as compared to finger print recognition. Twins also have different iris structures. This practice provides a secondary verification (Chong *et al*., 2006; Ratha *et al*., 2001). In this verification, the iris is subjected to light as reactions of the iris changes in light and these responses are also different. The iris should not be far than a few meters from the camera and it must be ensured that the iris must be motionless for getting the precise results. Different measures are used to ensure that the image is real instead of a photograph. The image can be vague if the contact lens is being used. Make sure that reflections should not be formed by the light source. If it occurs image can be unclear. Particular sorts of contact lenses can darken the iris design (Daugman, 2004; He *et al*., 2009).

MATERIALS AND METHODS

Iris biometrics and cryptography has been combined in a novel way to provide proper authentication and the data protection will be released only when the encrypted biometric authentication is successfully completed. During enrollment user's iris image has been scanned and it has been converted into digital template format using x and y coordinate values and some special features.

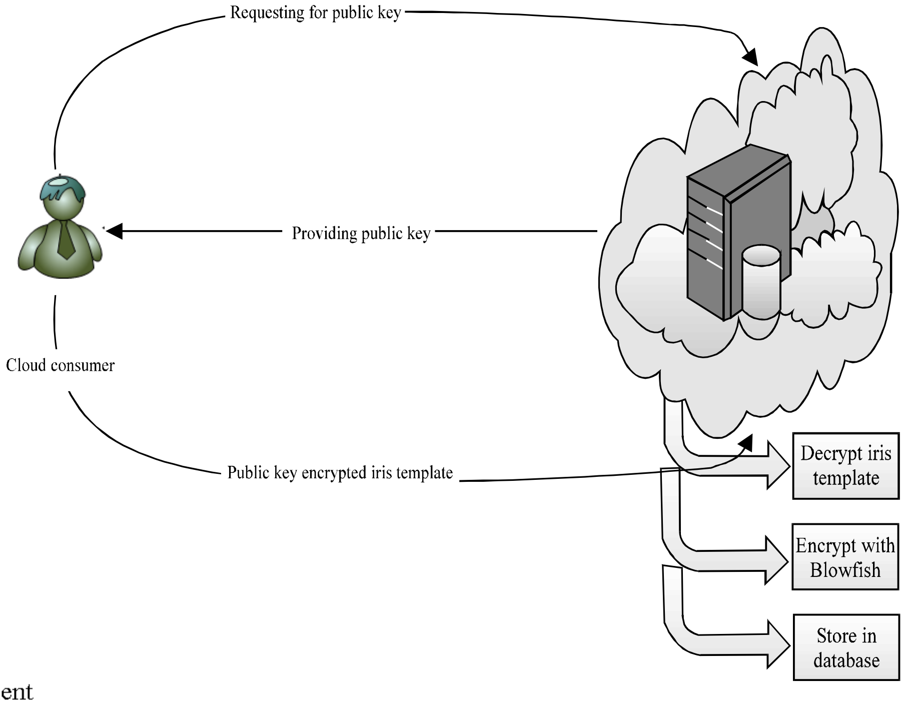

Fig. 2: Enrollment

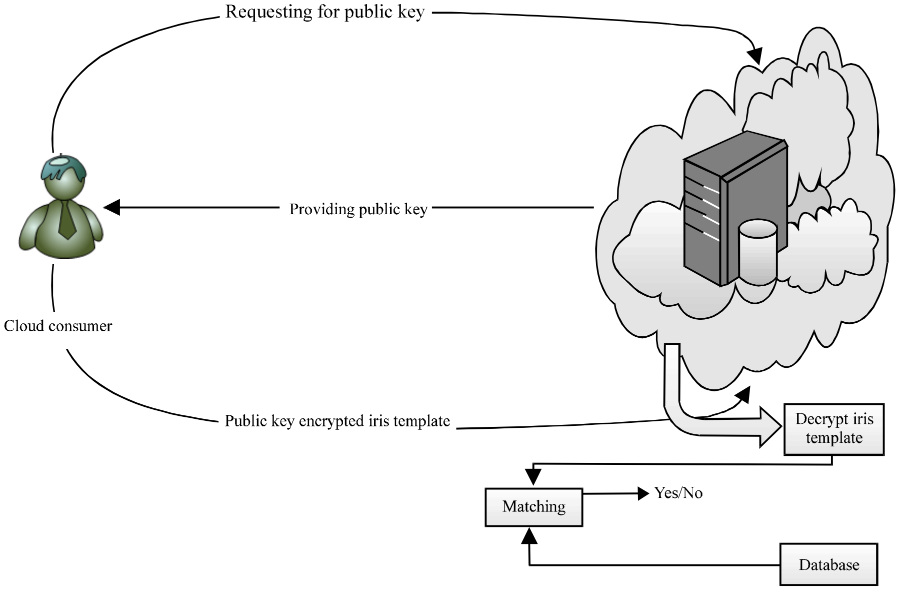

Fig. 3: Authentication

Then the iris digital template is encrypted using ElGamal public key cryptosystem using the key fetched from the cloud provider. The encrypted template is forwarded to the provider where digital template is decrypted and once again encrypted by Blowfish encryption algorithm and stored in the cloud provider's database (Fig. 2).

During authentication, the same set of work has been carried out up to the digital iris template conversion, Elgamal encryption and forwarding the encrypted template to cloud provider end. In cloud provider end the iris template is decrypted and customers enrollment iris template has been fetched from the database and decrypted by using blowfish algorithm and matching will be done with the plain iris templates. The comparison is with plain templates reduces the dilemma between security and privacy and security of stored template (Fig. 3).

Algorithms used; Elgamal public key crypto system: ElGamal encryption works with Diffie-Hellman key exchange (Schnorr and Jakobsson, 2000), Alice and Bob have a (publicly known) prime number p and a generator g:

- Alice selects a random number a and computes $A = g^a$
- Bob selects a random number b and generates $B = g^b$
- Alice's public key is A and private key is a. Similarly, Bob's public key is B and private key is b
- If Bob needs to send a message m to Alice, then he picks a number k which is smaller than p. then computes:
- $c_1 = g^k \bmod p$
- $c_2 = A^{k*}m \bmod p$
- And sends c_1 and c_2 to Alice
- Alice can use this to recreate the message m by computing
- $c_1^{-a} * c_2 \bmod p = m$
  Because
- c1-a*c2 mod p
- = (gk)-a*Ak*m
- = g-a*k*Ak*m
- = (ga)-k*Ak*m
- = A-k * Ak*m
- = 1*m = m

Blowfish algorithm: Blowfish algorithm follows, Feistel network, iterating an encryption function 16 times. The block size is 64 bits and the key can be any length up to 448 bits. Each round consists of a key dependent permutation and a key and data dependent substitution. All operations are XORs and additions on 32 bit words. The only additional processes are four indexed array data lookups per round (Schneier, 1994).

Sub keys: Blowfish employs a huge number of subkeys. These keys must be preprocessed before any data encryption or decryption. The P-array consists of 18, 32 bit subkeys called as P1, P2, ..., P18. There are also four 32 bit S-boxes with 256 entries each: S1, 0, S1, 1, ..., S1, 255; S2, 0, S2, 1, .., S2, 255; S3, 0, S3, 1, ..., S3, 255; S4, 0, S4, 1, ..., S4, 255.

Encryption and decryption: Blowfish has 16 rounds. The input is a 64 bit data element, x. Divide x into two 32 bit halves: xL, xR. Then, for i = 1-16: Xl = xL XOR Pi xR = F(xL) XOR xR And Swap xL and xR After the sixteenth round, swap xL and xR again to undo the last swap. Then, xR = xR XOR P17 and xL = xL XOR P18. Finally, recombine xL and xR to get the cipher text. Function F looks like this: divide xL into four eight-bit quarters: a-d. Then, F(xL) = ((S1, a+S2, b mod 232) XOR S3, c)+S4, d mod 232. Decryption is precisely the same as encryption, except that P1, P2, ..., P18 are used in the reverse order.

Sub key generation; Blowfish algorithm: The sub keys are estimated using the Blowfish algorithm:

1: Initialize the P-array and then the four S-boxes, in order with a fixed string. This string consists of the hexadecimal digits of pi (less the initial 3): P1 = 0×243f6a88, P2 = 0×85a308d3, P3 = 0×13198a2e, P4 = 0×03707344, etc

2: XOR P1 with the first 32 bits of the key, XOR P2 with the second 32 bits of the key and so on for all bits of the key (possibly up to P14) Repeatedly cycle through the key bits until the entire P-array has been XORed with key bits (For every short key, there is at least one equivalent longer key for example if A is a 64-bit key, then AA, AAA, etc. are equivalent keys)

3: Encrypt the all-zero string with the Blowfish algorithm using the subkeys described in steps 1 and 2

4: Replace P1 and P2 with the output of step 3

5: Encrypt the output of step 3 using the Blowfish algorithm with the customized sub keys

6: Replace P3 and P4 with the output of step 5

7: Continue the process, replacing all entries of the P array and then all four S-boxes in order with the output of the continuously changing Blowfish algorithm

In total, 521 iterations are required to generate all required sub keys. Applications can supply the sub keys rather than execute this derivation process multiple times.

RESULTS AND DISCUSSION

The above-said implementation has been tested against many types of attacks and it has been tested for two different metrics such as FAR (False Acceptance Rate) and FRR (False Rejection Rate) of 75 different user's Iris patterns. And the results are tremendous with approximately zero false acceptance rate. Some higher level of false rejection rate, since, I used 85% threshold value. If the threshold is reduced then FRR can be reduced but FAR can be increased. We are in the need of higher security FAR should be reduced at most. Threshold and FRR are directly proportional, threshold and FAR are inversely proportional to each other (Table 1) (Fig. 4).

Table 1: FPR and FAR metrics

Iterations	Users	FAR	FRR
1	25	0	2
2	35	0	2
3	50	1	3
4	65	1	4
5	75	1	6

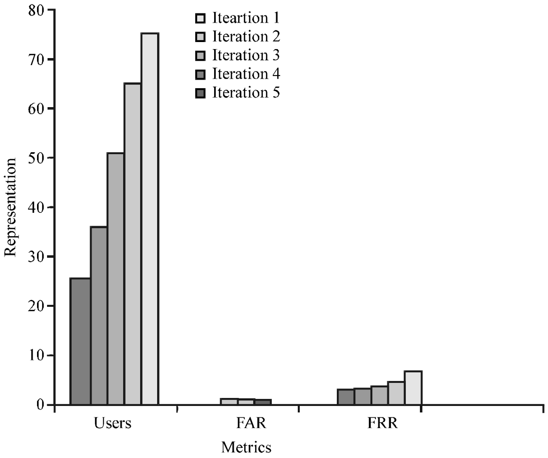

Fig. 4: Bar representation of various metrics

CONCLUSION

Cloud-based biometric authentication services have a massive potential market value and invite research and development. In this study, some directions on how to move existing biometric technology to a cloud platform were presented and issues that need to be considered when designing cloud-based biometric services have been discussed. An inclusive system for web applications and data management over the cloud, powered by strong iris-based biometric authentication is presented. The system guarantees the identity of the users and makes easy and secure the access to data and services by providing strong authentication. Moreover, the adoption of biometrics with cryptography which ensures template protection is proposed.

REFERENCES

Bowyer, K.W., K. Hollingsworth and P.J. Flynn, 2008. Image understanding for iris biometrics: A survey. Comput. Vision Image Understand., 110: 281-307.

Chong, S.C.A., T.B. Jin and D.N.C. Ling, 2006. Iris authentication using privatized advanced correlation filter. Proceedings of the International Conference on Advances in Biometrics, January 5-7, 2006, IEEE Xplore, pp: 382-388.

Daugman, J., 2004. How iris recognition works. IEEE Trans. Circuits Syst. Video Technol., 14: 21-30.

He, Z., T. Tan, Z. Sun and X. Qiu, 2009. Toward accurate and fast iris segmentation for iris biometrics. IEEE Trans. Pattern Anal. Mach. Intell., 31: 1670-1684.

Hogan, M., F. Liu, A. Sokol and J. Tong, 2011. Nist Cloud Computing Standards Roadmap. National Institute of Standards and Technology, Gaithersburg, Maryland, USA., Pages: 76.

Jain, A., R. Bolle and S. Pankanti, 2006. Biometrics: Personal Identification in Networked Society. Vol. 479, Springer, Berlin, Germany, ISBN: 978-0387-28539-9, Pages: 407.

Krutz, R.L. and R.D. Vines, 2010. Cloud Security: A Comprehensive Guide to Secure Cloud Computing. Wiley, New York, ISBN: 9780470921449, Pages: 504.

Raghava, N.S., 2011. Iris recognition on hadoop: A biometrics system implementation on cloud computing. Proceedings of the 2011 IEEE International Conference on Cloud Computing and Intelligence Systems (CCIS), September 15-17, 2011, IEEE, Beijing, China, ISBN:978-1-61284-203-5, pp: 482-485.

Ratha, N.K., J.H. Connell and R.M. Bolle, 2001. Enhancing security and privacy in biometrics-based authentication systems. IBM Syst. J., 40: 614-634.

Schneier, B., 1994. The blowfish encryption algorithm. Dr. Dobbs J. Software Tools Prof. Programmer, 19: 38-43.

Schnorr, C.P. and M. Jakobsson, 2000. Security of Signed ElGamal Encryption. In: Theory and Application of Cryptology and Information Security, Okamoto, T. (Ed.). Springer, Berlin, Germany, ISBN:978-3-540-41404-9, pp: 73-89.

Sudhan, S.K. and S.S. Kumar, 2014. A panoptic survey on cloud computing. Intl. J. Res. Eng. Technol., 2: 1-5.

Sudhan, S.K.H.H. and S.S. Kumar, 2015. An innovative proposal for secure cloud authentication using encrypted biometric authentication scheme. Indian J. Sci. Technol., 8: 1-5.

Sudhan, S.K.H.H. and S.S. Kumar, 2016. Gallant use of cloud by a novel framework of encrypted biometric authentication and multi level data protection. Indian J. Sci. Technol., 9: 1-7.

Vielhauer, C., 2005. Biometric user Authentication for IT Security: From Fundamentals to Handwriting. Vol. 18, Springer,Berlin,Germany,ISBN:13-978-0-387-26194-2, Pages: 284.

Zissis, D. and D. Lekkas, 2012. Addressing cloud computing security issues. Future Gener. Comput. Syst., 28: 583-592.