Middle-East Journal of Scientific Research 24 (12): 3755-3762, 2016
ISSN 1990-9233

DOI: 10.5829/idosi.mejsr.2016.3755.3762

A Novel Framework for User Authentication and Data Security in Mobile Cloud Using Gait

[1]S. Sengole Merlin and [2]A Chandrasekar

[1]Loyola-ICAM College of Engineering and Technology, Chennai, India
[2]St. Joseph's College of Engineering, Chennai, India

Abstract: Cloud services has captured significant place in technology breakthrough in recent years. Combining the advantages of Grid computing, Distributed systems, utility computing with client server model, it renders its services under different manifesto, such as Software (SaaS), Infrastructure (IaaS) and Platform (PaaS). In comparison to traditional IT services, where we have physical, logical and personnel control, Cloud Services are dependent on large data centers where trustworthiness of a person becomes a big question and cloud data security is of great importance and treated as main obstacle towards industries opting the cloud based model. As user authenticity plays a major role in providing better cloud data security, we propose a Gait based authentication for the users and define different authorization levels in such kind of open source model. Virtual Machines (VM) in cloud server are used for computational analysis. We discuss on the Identity Based Encryption (IBE) systems incorporated in VM's to increase the security further. Data authorization levels are also defined using the users.

Key words: Cloud Security · Identity Based Encryption (IBE) · Gait Authentication · Virtual Machine

INTRODUCTION

Cloud computing is an important prototype in cloud era. This technology can transform and has obvious ability to marvel the IT (Information Technology) services, security being the most obvious threat. This innovation has various potentials that are yet to be unveiled and there are research going on every aspect of cloud. Cloud Computing delivers the services over the internet and its services varies as per the request of each user. The services are mainly Software as a Service (SaaS), Infrastructure as a service (IaaS) or Platform as a Service (PaaS). Deployment of cloud also has its own divisions and again depends on the requirements of the customers, as explained in Figure 1.

Public Cloud: A Public Cloud is shared by multiple organizations and used by multiple users from different origin. The implementation of cloud involves data center, infrastructure of hardware and software which is also shared and not a dedicated one. The data center is usually at the off-premises. This type of cloud provides services to user who wants to access the services. Eg: IBM LotusLive, Google AppEngine, Amazon Web Services and many more.

Private Cloud: A Private Cloud is implemented using a dedicated data center, hardware and software and is not shared with any other organization. The data center can be on-premises or off-premises. It is dedicated to a particular organization. If the data center is shared, then it becomes a Virtual Private Cloud. Users will have to be employees of that organization.

Hybrid Cloud: A Hybrid Cloud is any combination of above discussed Clouds. It varies with combination of Private Cloud and one or more Public Clouds. Similarly it could be combination of Virtual Private Cloud and one or more Public Clouds. There needs to be resources shared among the Clouds. It is mostly used in science and technology requirements, but many organizations are resorting to this as it has blended advantages of other cloud.

Corresponding Author: S. Sengole Merlin, Loyola-ICAM College of Engineering and Technology, Chennai, India.

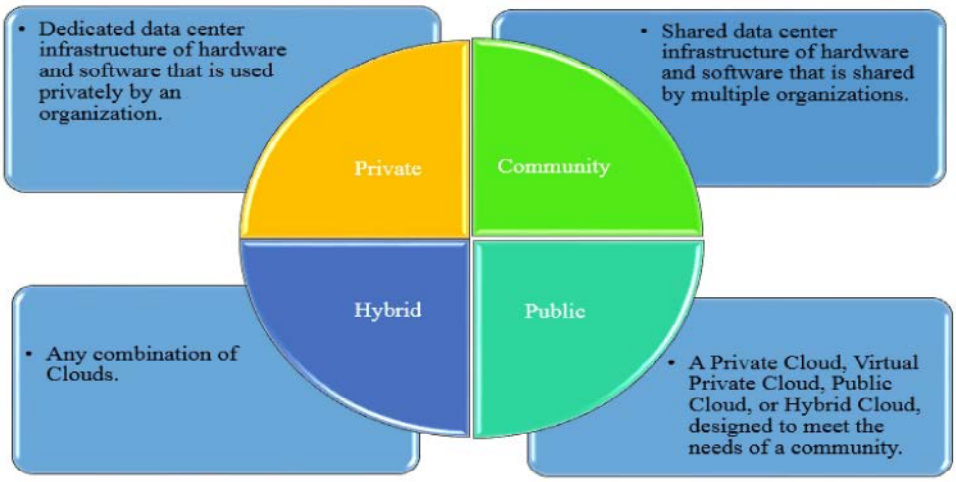

Fig. 1: Different types of Cloud

Community Cloud: A Community Cloud is designed for specific need of a community. Community can be group of people or an organization that have shared interests, includes industrial groups, research groups, standards groups and so on. This setup is more suitable where a multiple organizations share the same cloud. A Private Cloud, Virtual Private Cloud, Public Cloud, or Hybrid Cloud can act as a community cloud. Best examples would be a company, which has many sister companies and share the same sort of interest in providing the services.

The rapid development of cloud computing has brought three core technologies together- Multitenancy, Virtualization and Web Services. Virtualization embraces the concept of hiding the physical characteristics of a computing platform and uses multitenancy feature thereby allowing different instances of application software for multiple users. A web service integrates the software system designed to support interoperable machine to machine interaction over a network, preferably internet Virtual Machines in cloud server are the means by which users authenticate themselves and access the services.

Authentication and Encryption are very important, when it comes to Cloud Data Security. There are multiple users who have access to cloud, be it any type of cloud setup or Services. It becomes imperative that rigid authentication systems should be in place to make sure the person accessing the cloud services are genuine. When it comes to Data Security, it has to be made unquestionably clear that the person who is accessing the data is authentic and has proper authorization. This warrants modern authentication systems to provide a definitive model that can keep away the hackers at bay. To define one, we have discussed on different existing authentications systems in the next section.

Related Works: The existing authentication schemes rely on the client-server architecture is discussed along with various other schemes that were developed subsequently. Lamport [1] in 1981 discuss about the popular and aged, remote schemes where hashed values generated from the user's password are stored in server and used for authentication later. Password database which is used to verify the users legitimacy, is compromised or altered by an adversary, then whole system is threatened and is vulnerable to attack from hackers. Moving to next level of authentication schemes, which brought in card based password authentication proposed in. This took the authentication to next level but again crippled with many flaws discussed in papers by Hwang *et al*. [2] Kim *et al*. [3] discussed on the smart card and fingerprint based authentication scheme where the password list were not centrally maintained in servers and users were in under liberty to change it any point in time. More over Nonce Technology was used to protect against Replay attacks which avoids the clock synchronization at the hosts. However it is prone to imitation attacks giving way to hackers to judge the authentication value in few network packets. This is discussed in detail by Scott [4]. Cloud computing can be seen as a modified version of client server architecture in which many users try to access the same infrastructure at a large scale. Subsequently, Cloud requires a better and a rigid authentication than traditional client server system. Proposal for usage of public key and

Table 1: Comparison of different Biometric system.

Biometric Technology	Accuracy Level	Cost per User	Devices Required	Social Acceptability
Iris Recognition	High	High	Yes – High Resolution Camera	Medium - Low
Retinal Scan	High	High	Yes – High Resolution Camera	Low
Facial Recognition	Medium – Low	Medium	Yes - Camera	Medium - Low
Voice Recognition	Medium	Medium	Microphone	Medium
Finger Print	High	High - Medium	Scanner	High - Medium
Signature Recognition	Low	Medium	Optic Pen Touch Panel	High - Medium

mobile based authentication, card based, for cloud computing by Lee *et al* [5]. The scheme transmits data (e.g. ID, PW and PKI) as a plaintext form. This can be easily intercepted and can be used in a wrong way or modify the data by the adversaries. The scheme also lacked the discussion on data confidentiality, integrity, user privacy and moreover the users are prohibited of changing their password, which again is prone to issues. As a result, their scheme is not fit for real time cloud computing. Biometrics, another means of authentication, leverages the uniqueness of physical or behavioral characteristics across individuals. Detailed discussion on fingerprint biometrics is discussed by Ross *et al*. [6]; on remote authentication application to see if the indiviual is really asserted to be person requesting the access. It assumes unsupervised biometric hardware as built in client-devices e.g., at an airport supervised by officials. Fingerprint biometrics advantages from usability perspective, by presenting the characteristics like Effortless Memory, Easily Scalable based on Users and Nothing-to-Carry. Though Biometrics provide a better solution towards authentication than their rivals, password and card based accessing, it suffers by few disadvantages which are critical in current scenario, like failure to offer Easy-Recovery-from-Loss, Deploy-ability is poor and costly, Failure-to-Register biometric issues, not Negligible Cost with respect to each User, neither Server-Compatible nor Browser-Compatible, needing both client and server changes as discussed by Joseph Bonneau *et al*. [7]. Table 1 shows the various levels of acceptability in biometric systems.

During this survey it is seen that, authentication system requires a certain minimum set of phases through which determines the data flows and comparison decision are made through certain process.

Architecture of Proposed Authentication System: We propose a novel protocol using remote authentication for cloud based services. This system uses Gait as a medium to justify a user is authenticated to enter the premises and provide him with the access based on his authorization grade. The initialization phase usually consists of generating and sending the data from the users Gait – walking patterns using the sensors and send it to the Virtual machine. The Registration phase is used to make the system train on the Gait of the user, generate the pattern based on the data feed from sensors and save it in the data base for the future reference. The Virtual machine in the cloud is in handshake with the authentication system to access the pattern whenever necessary. Handshake is done to keep the session key in common, so the data encryption and decryption can happen at any point in time. This gives a better shield from the intruders [8-15].

Most often Authentication system has 3 phases

- Analysis of the customer details
- Extraction of features
- Comparison & Decision making

In order to check whether the details match every model will have these basic steps and involves its own processing procedures [Figure 2].which makes it an exclusive based on the method chosen during the Authentication phase, when the user enters the premise, the sensors automatically send the data to the cloud server where the virtual machines decodes the pattern from the feed.

Meanwhile the virtual machine gets the template pattern from authentication system. The patterns are then matched and a decision is arrived at to provide the access to the user. (Figure 3). The sequential flow of data at each phase is shown in Figure 4.

Computational Analysis: Gait based authentication systems are in the path of revelation of its influence towards authentication in future era and is a futuristic approach to provide users a facility of authenticating themselves on the go, without requiring any physical acquaintances with the system. Our proposed gait based authentication model is more pertinent for a mobile cloud based organization, which provides the users the power of agility, scalability and on the go access, without even physically touching. A mobile application “m-Cloud” is an

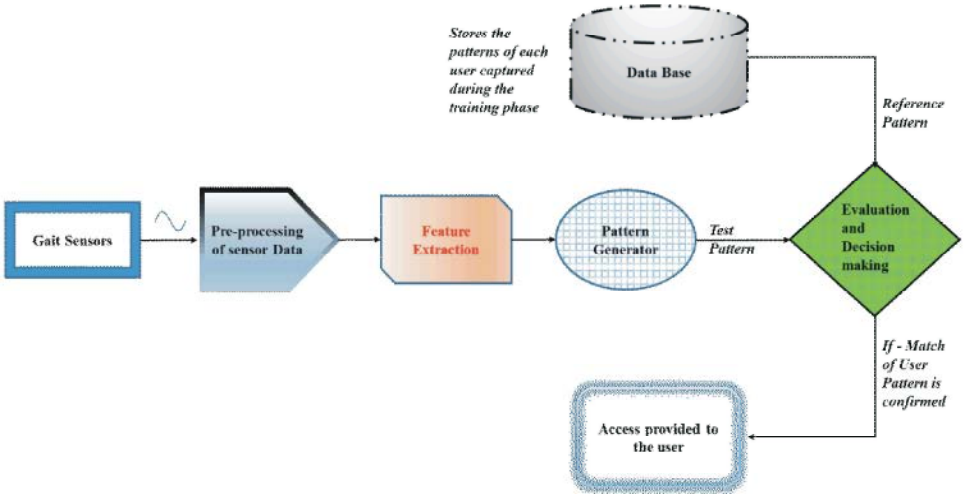

Fig. 2: Basic Architecture of authentication system

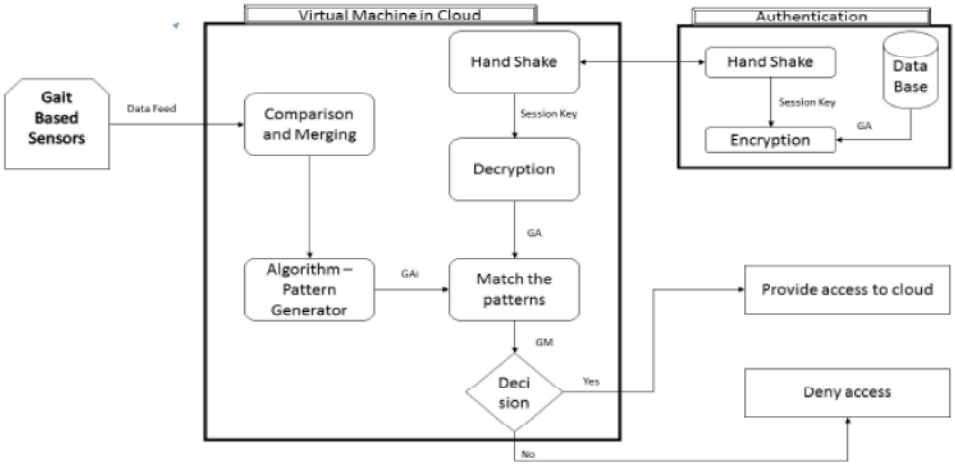

Fig. 3: Architecture of proposed system

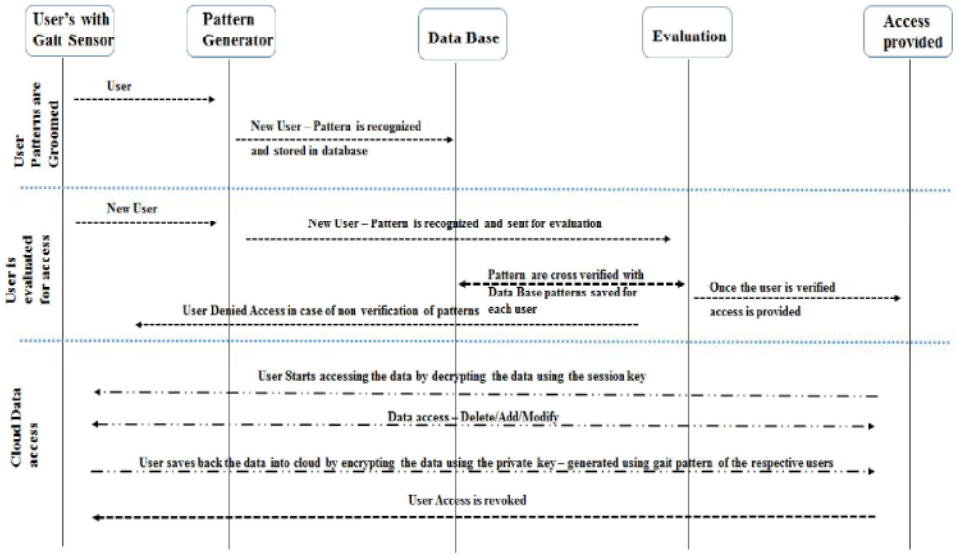

Fig. 4: Sequential diagram of Data flow

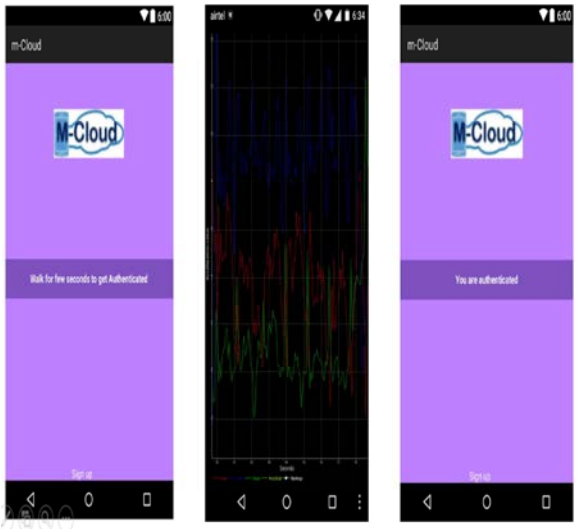

Fig. 5: (i). "**m-cloud"** Mobile application installed in mobile (ii). Data Capture. (iii) Authentication

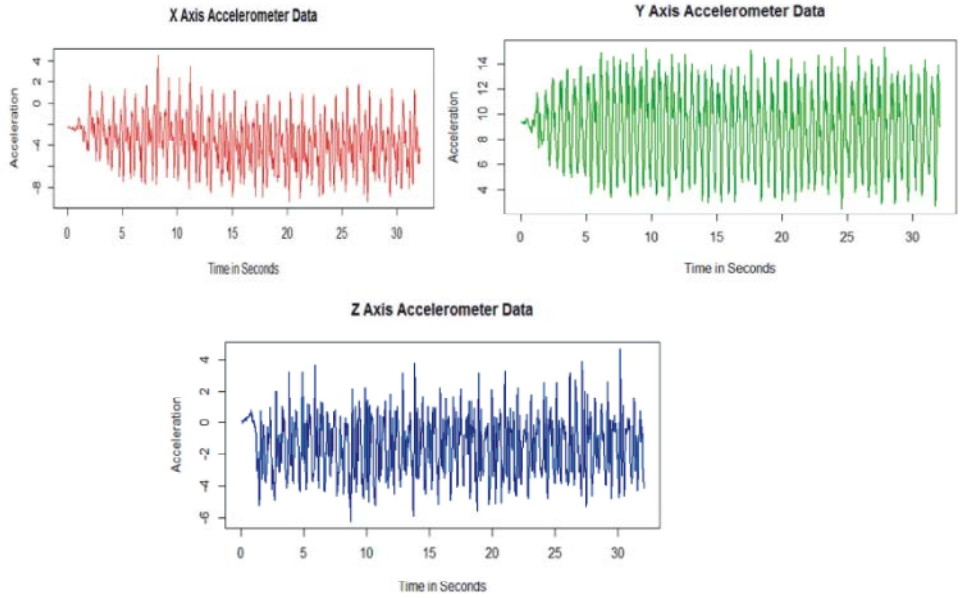

Fig. 6: Raw Data - Accelerometer data for each axis

indigenously built application, for this research purpose and is deployed in the mobile device to capture the data and transfer to cloud server. (Figure 5). Users gait patterns are referred to the person's manner of walking. The readings are captured using the mobile application providing accurate X, Y, Z coordinate values, which are further groomed and converted into patterns. The graphs are then generated using these patterns [16-19].

Individual patterns are created for each users and is saved in the data base which act as the reference pattern. The application detects the acceleration in three directions - X, Y, Z (Figure 6) at each given instance and it produces the raw data and transfers it to cloud server. The mobile device collect the data between ± 2g (g= 9.8m/sec^2) with the sampling rate of 16 samples per second. Noise signals is filtered and reduced using Multilevel Wavelet Decomposition and Reconstruction as discussed by Thang Hoang etl.[8]. The final combined cyclic patterns are arrived (Figure 7).

During the authentication phase, the user details are collected and is denoted by $\mathbf{GA}_i$ for each and respective users $\mathbf{U}_i$. $\mathbf{GA}_i$represents the vectorial combination of X, Y and Z coordinate values.

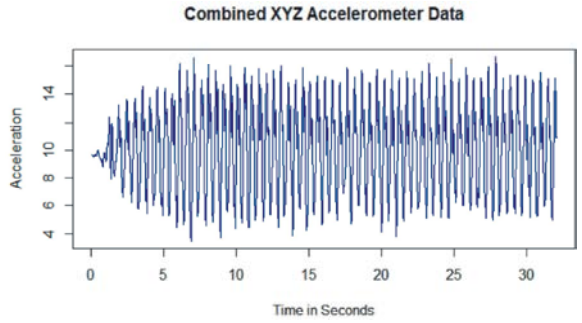

Fig. 7: Cyclic Patterns of XYZ coordinates

Here, $\mathbf{a} \clubsuit \mathbf{R}_3$

where, $\mathbf{R}_3$ denote three real coordinates and a is value at given instance

Sums, differences and scalar multiples of three-dimensional vectors are performed on each component and is represented by below equations.

Consider x=[x1, x2, x3] and y= [y1, y2, y3]

$$X_i\,[x+y] = [x1+y1,\ x2+y2,\ x3+y3] \quad (1)$$

$$Y_i\,[y-x] = [y1-x1,\ y2-x2,\ y3-x3] \quad (2)$$

$$Z_i\,[\lambda x] = [\lambda x1,\ \lambda x2,\ \lambda x3] \quad (3)$$

$$Ga_i = [X_i, Y_i, Z_i] \quad (4)$$

Based on the obtained gait data GA_i Cloud User Authentication is done by our proposed Security algorithm [Algorithm 1]. The algorithm steps are given below. The data encryption is done at the cloud server and the decryption at the terminal virtual machine.

At Authentication Server:

Algorithm for Data Encryption

Step 1: Generate a one-time private key $\mathbf{P}_k$ and Session key $\mathbf{S}_k$.

Step 2: Compute $\mathbf{N= P_kS_k}$

Step 2: Share Session Key between the terminal and server.

Step 3: Compute $\mathbf{C = E_{sk}(GA||\ P_k) = H_1(GA}$ mod $N)$, whereas **C** is the encrypted data and is sent to the terminal and $\mathbf{H}_1$ is a hash function

At Terminal Virtual Machine:

Algorithm for Data Decryption

Step 1: Compute Decrypt $\mathbf{D_{sk}\ (M) = H_2(C \oplus S_k)}$ to obtain **GA** and $\mathbf{P}_k$

Step 2: If $\mathbf{GA}_i$ = = **GA**,

then **CM** = TRUE;

Else **CM** = FALSE

Step 3: If **CM** == TRUE,

then accept the request of $\mathbf{U}_i$ login.

return Comparison Message **(CM)** and $\mathbf{GA}_i$ Encryption

$RM = E_{PK}\,(GA_i \| GM)$.

At Authentication Server:

Provide the access to the user $\mathbf{U}_i$ based on the Comparison Message (**CM**).

Algorithm 1: Proposed Gait Encryption and Decryption Algorithm for user Authentication in Mobile Cloud Data Access.

We discuss now the computational complexity. The scheme proposed by Fan *et al*. uses the Rabin algorithm to protect the symmetric keys while transmitting the data between the servers. The approach although reduces the time required by exponential operations, the communication security could not be guaranteed in an environment between the virtual machine and the authentication server. Distinctively, in the proposed scheme we use the Diffie-Hellman method for key exchange and algorithm to protect the terminal-server communications. The proposed scheme is compared with that of the other existing schemes presented. In analyzing all the various computations performed in the different papers, it is seen that the exponential operation implemented in decryption procedure takes a considerable amount of time. The current scheme has advantage over the other systems by reducing the computational overhead and time, since the scope of authentication is specific to Gait analysis only and the number of symmetric decryption operations is significantly reduced [10, 12].

Experiment Results: The proposed work was implemented and analyzed in terms of time taken for authentication. It was observed that the time taken is comparatively better with the traditional systems. In our proposed work we also encrypt gait pattern which increases over all security and reduces the risk of unauthorized access in mobile cloud. We analyzed the results for the Encryption/Decryption time which is provided in the Table 2. The results are provided considering the Gait pattern size of 32 KB to 256KB. It is seen that though the time increases with the size of the Gait pattern, the time increase is not substantial. This gives the proposed system an edge towards using it with systems where 256KB data is used and considerably

Table 2: Time analysis for different sizes (in KB) of Gait patterns

Gait Pattern Size (KB)	Encryption Time (Milli Seconds)	Decryption Time (Milli Seconds)	Authentication Time (Milli Seconds)
32 KB	2.3	3	5
64 KB	3	3.2	6.2
128 KB	4	3.5	7.5
256 KB	4.2	4.1	8.1

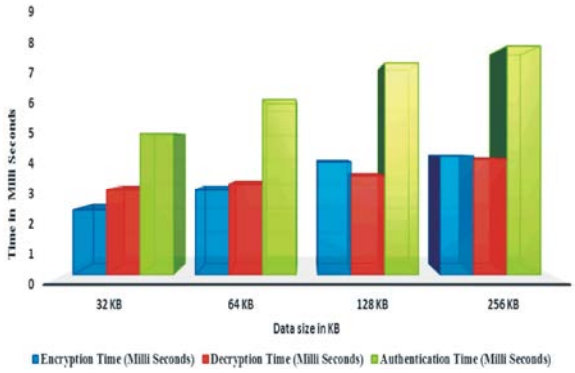

Fig. 8: Graphical representation of time analysis for Encryption, Decryption and Authentication

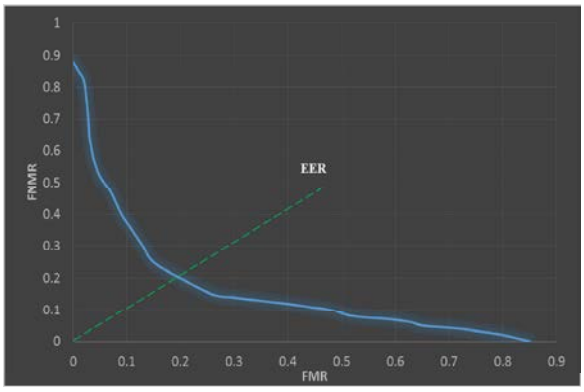

Fig. 9: Gait Authentication with equal error rate of 20%.

increases the security as well, without much compromising on the time. The details of the time is shown in blocks as graphical representation showing the difference in increase as the byte size increases (Figure 8). The overall performance of our authentication is measured in terms of False Match Rate (FMR) against False Non Match Rate (FNMR). The results are shown in the Figure 9 using Detection Error Trade-off curve. The experiment results clearly shows that Equal Error Rate of our proposed method is only 20%.

CONCLUSION

The phenomenal growth in Mobile Cloud poverties innovative ideas in authenticating a user. This requires research to cope up with the advancing technologies as the traditional methods like Password, Card readers and bio-metric systems will become, systems of the past, in years to come. Users will be in need of a more sophisticated, unique and more trustworthy authentication systems for their cloud servers, so as to make sure of their data is integral. Gait based authentication is one of the promising and growing field which can be tapped to satisfy the need of the users. It can further be linked with authorization of users, with different levels of data and software access, to make sure the sensitive data are kept safe.

REFERENCES

1. Lamport, L., 1981. Password authentication with insecure communication, Communications of the ACM, 24(11): 770-771.
2. Hwang, M.S., 1999. Cryptanalysis of a remote loginauthentication scheme, Computer Communications, 22(8): 742-744.
3. Kim, H.S., S.W. Lee and K.Y. Yoo, 2003. ID-based Password Authentication Scheme Using Smart Cards and Fingerprints, ACM SIGOPS Operating Systems Review, 37(2): 32-41.
4. Scott, M., 2000. Cryptanalysis of an ID-based authentication scheme using smart cards and Fingerprints, ACM SIGOPS Operating Systems Review, 38(2): 73-75.
5. Lee, J.K., S.R. Ryu and K.Y. Yoo, 2002. Finger print-based remote user authentication scheme using smart Cards, Electronics Letters, 38(12): 554-555.
6. Ross, A., J. Shah and A.K. Jain, 2007. From template to image: reconstructing fingerprints from minutiae points, IEEE Transactions on Pattern Analysis and Machine Intelligence, 29(4): 544-560.
7. Bonneau, J., C. Herley, P.C. van Oorschot and F. Stajano, 2012. The quest to replace passwords: A Framework for comparative evaluation of Web authentication schemes, In Proc. IEEE Symposium on Security and Privacy.
8. Hwang Min-Shiang, Cheng-Chi Lee and Yuan-Liang Tang, 2001. An improvement of SPLICE/AS in WIDEAgainst guessing attack, International Journal of Informatica, 12(2): 297-302.
9. Armbrust, M., A. Fox, R. Griffith, A.D. Joseph, R. Katz, A. Konwinski, G. Lee, D. Patterson, A. Rabkin, I. Stoica and M. Zaharia, XXXX. A view of cloud computing, Communications of the ACM, 53(4): 50-58.

10. Sharma, S. and U. Mittal, 2013. Comparative Analysis of Various Authentication Techniques in Cloud Computing, International Journal of Innovative Research in Science, Engineering and Technology, 2(4): 994-998.
11. Marston, S., Z. Li, S. .Bandyopadhyay, J. Zhang and A. Ghalsasi, 2011. Cloud computing - the business perspective, Decision Support Systems, 51(1): 176-189.
12. Yuping Xing and Yongzhao Zhan, 2012. Virtualization and Cloud Computing, Future Wireless Networks and Information Systems, 143: 305-312.
13. Hwang, M.S. and L.H. Li, 2000. A New Remote User Authentication Scheme using Smart Cards, IEEE Transactions on Consumer Electronics, 46(1): 28-30.
14. Khan M.K., 2007. Cryptanalysis and Security Enhancement of Two Password Authentication Schemes with Smart Cards, Proc. IEEE International Multi-topic Conference (INMIC), Lahore, Pakistan, pp: 1-4.
15. Chien H.Y.J.K. and Y.M. Tseng Jan, 2002. An efficient and practical solution to remote authentication: Smart card, Computers and Security, 21: 372-375.
16. Liao I-En, Cheng-Chi Lee and Min-Shiang Hwang, 2005. A password authentication scheme over insecure networks, Journal of Computer and System Sciences, 72(4): 727-740.
17. Lee, S., I. Ong, H.T. Lim and H.J. Lee, XXXX. Two factor authentication for cloud computing, International Journal of KIMICS, 8: 427-432.
18. Jain, A.K., A. Ross and S. Pankanti, 2006. Biometrics: a tool for information security, IEEE Transactions on Information Forensics and Security, 1(2): 125-143.
19. Fan, C.I., Y.H. Lin and R.H. Hsu, 2006. Remote Password Authentication Scheme with Smart Cards a Biometrics, IEEE Global Telecommunications Conference (GLOBECOM), pp: 1-5.