Research Journal of Applied Sciences, Engineering and Technology 9(8): 655-664, 2015
DOI:10.19026/rjaset.9.1451
ISSN: 2040-7459; e-ISSN: 2040-7467
© 2015 Maxwell Scientific Publication Corp.
Submitted: November 13, 2014 Accepted: January 27, 2015 Published: March 15, 2015

Research Article

Authentication Methods in Cloud Computing: A Survey

[1]Mahnoush Babaeizadeh, [2]Majid Bakhtiari and [1]Alwuhayd Muteb Mohammed
[1]Department of Computer Science, Faculty of Computing, Universiti Teknologi Malaysia,
Skudai 81310, Johor, Malaysia
[2]Advanced Informatics School, Universiti Teknologi Malaysia, 54100 Kuala Lumpur, Malaysia

Abstract: This study presents a review on the various methods of authentication in cloud environment. Authentication plays an important role in security of Cloud Computing (CC). It protects Cloud Service Providers (CSP) against various types of attacks, where the aim is to verify a user's identity when a user wishes to request services from cloud servers. There are multiple authentication technologies that verify the identity of a user before granting access to resources.

Keywords: Authentication, biometric, cloud computing, information security, keystroke authentication, security and privacy

INTRODUCTION

Cloud computing is a model for enabling on-demand network access to a shared data, infrastructure, software, platform resources which can be rapidly provisioned and released with minimal management effort or service provider interaction. It helps to extend capability of Information Technology (IT) by providing different services.

Three important factors of cloud security requirements are confidentiality, integrity and availability. These factors are well known as CIA. Confidentiality means keeping user's data secret in CSP and only authorized customers (computers and users) allow accessing to protected data. It depends on numerous factors such as encryption methods (symmetric or asymmetric algorithm), length of key (in symmetric algorithm) and Cloud Service Provider (CSP) (Sharma *et al*., 2011).

In CC, confidentiality has a main role in preserving control on organizations' data situated across multiple distributed databases. Integrity means that an unauthorized person is not permitted to modify, fabricate and delete sensitive information in cloud servers. By preventing unauthorized access (confidentiality), organizations can achieve greater confidence in data and system integrity. The main goal of availability is to ensure that unauthorized person cannot access to shared information in cloud service provider (any time and any place). Cloud servers must have the ability to continue operations even in the possibility of a security breach. Denial of Service attacks (DOS), natural disasters, as well as equipment outages can threats to availability.

Cloud computing is an internet based technology which provides numerous services over the internet. These services considerably effects on economy in terms of cost reducing, efficiency, scalability as well as energy. A service is a mechanism that is able to provide functionalities for using in compliance with considering rules. Cloud Computing services can categories in three folds (Banyal *et al*., 2013; Krishna Shyam, 2013) Software as a Service (SaaS), Infrastructure as a Service (IaaS), Platform as a Service (PaaS). Gibson and Elveleigh (Behl, 2011) presented various benefits of these cloud services.

SaaS is an on-demand application or software service which is topmost layers. It delivers software as a service through the Internet such as Google Docs, Zoho, as well as Microsoft CRM. It eliminates the need of installing and running the application on the customer's own computers (Ziyad and Kannammal, 2014; Jog and Madiajagan, 2012; Bouayad *et al*., 2012). The second layer (outgrowth of IaaS) is PaaS. It allows users to rent storage, database management system, operating systems, hardware, tools for design and network capacity (hosting) through the Internet (Ramgovind *et al*., 2010). Subashini and Kavitha (2011) discussed about some security issue in this approach. IaaS Qiao *et al*. (2012) is bottommost layer. It provides basic computing infrastructure components such as CPU, storage and memory. It implies the combination of hosting, hardware provisioning and basic services needed to run on cloud.

Infrastructure is underlying physical components that are required for a system to perform its functionalities. Manvi and Krishna Shyam (2013) discussed about some issues in IaaS.

Corresponding Author: Mahnoush Babaeizadeh, Department of Computer Science, Faculty of Computing, Universiti Teknologi Malaysia, Skudai 81310, Johor, Malaysia

There are other types of cloud services such as Data Storage as a Service (DSaaS), Communication as a Service (CaaS), Software as a Service (SaaS) (Wu *et al*., 2012), Security as a Service (SecaaS), Business as a Service (BaaS) (Li *et al*., 2014) and Hardware as a Service (HaaS) (Jula *et al*., 2014).

Cloud services can be operated according to four different deployment models private cloud, community cloud, public cloud, as well as hybrid cloud. Private cloud is platform of cloud which is dedicated for specific user or organization. Unlike public cloud which the numerous layers may be offered by multiple providers the entire stack (IaaS, PaaS and SaaS) control by a single provider. Therefore, it has access and control over the various infrastructure, applications and middleware (Wu *et al*., 2012; Winkler, 2011). Community cloud is a type of cloud infrastructure which shared by several organizations and supports a specific community.

Furthermore, it may be managed by the organizations or a third party (Behl, 2011). Public cloud (Ramgovind *et al*., 2010) refers to a model which permits users access to the cloud through interfaces using mainstream web browsers (available to public users). It is the most dominant architecture when cost reduction is concerned. However, it is less secure than the other cloud models. Hybrid cloud is a combination of two or more clouds (private, community, or public) that remain unique entities (Bouayad *et al*., 2012).

However CC offers numerous advantages such as low cost cloud storage and shared infrastructure (Ricco and Chen, 2009) The most serious issue that CC faces concerns its inability to insure data privacy and confidentiality and there are different security and privacy issues in this area (Popovic and Hocenski, 2010; Bouayad *et al*., 2012). Pearson *et al*. (2009) presented numerous architectures of privacy manager in CC, which decrease the risk of steal and misuse of shared data in CSP. In fact, these methods help to manage the privacy of their sensitive and critical data in the cloud environment. Behl (2011) studied security approaches of cloud infrastructure and their weaknesses. The goal of this research is to formulate a security strategy and improve the security of cloud environment.

One of the important options which help to reduce security and privacy risks is Access Control (AC). It refers to mechanisms that permit to perform functions up to their authorized level and restrict users from performing unauthorized function. AC mechanisms can divide to three parts authentication of users, authentication of their privileges and auditing to monitor and record actions of users.

Authorization is the process of determining what an authenticated user can do. It is independent of authentication. Furthermore, authorization servers are responsible for receiving and validating the user access request to some specific services. It maintains a list of all the policies related to the users in the policy engine and updates them when required. If a request is successfully validated, the authorization server allow to the user access to the requested resource for a particular amount of time (Khalid *et al*., 2012). Auditing helps to ensure that users are accountable. Cloud servers record actions in audit trails and logs. For instance, a user attempting numerous failed logins might be seen as an intruder.

User authentication on cloud environment is as important issue, because it guarantees that somebody works or shares data with the right person and that only authorized users can access to data or application (Jivanadham *et al*., 2013). Authentication requires some form of "proof of identity". There is increasing demand for suitable authentication method for accessing to the shared information via the Internet through Cloud Service Provider (CSP). Therefore, numerous mechanisms used to authenticate users in CC environment. These methods are username and password, multi-factor, Mobile Trusted Module (MTM), Public Key Infrastructure (PKI), Single Sign On (SSO), as well as biometric authentication (Bhattacharyya *et al*., 2009; Jeong and Choi, 2012; Schmidt *et al*., 2008; Acucmez *et al*., 2008).

This paper reviews various methods of authentication in cloud environment. These methods are typically employed to enhance the security of CC.

AUTHENTICATION IN CLOUD ENVIRONMENT

Authentication is a main part of every secure communication system especially in wide spread network such as CC. It helps to protect shared information from unauthorized persons and it is a key technology for information security. AAA is a management module for authentication, authorization and accounting. When a user tries to access CSP, then AAA checks the user's authentication information. If the user is authenticated, then AAA gets the user's access level, which has been most recently generated, by inspecting the user's information in the database. In addition, authentication method determine "Who is the legal user" and "Is the user really who he claims himself to be". In addition, verification of user's identity is the most important goal behind an authentication.

In other words, an authentication mechanism determines how user identified and verified to access to sensitive information (Köse, 2011). Verification means confirm that demand is from the legal user. Identification implies on determining user's identity (by comparing the security question, image, voice, or other information which are available in database).

There are several authentication schemes (Pointcheval and Zimmer, 2008; Anzaku *et al*., 2010; Xie and Yao, 2013) which categorized in three types as follow:

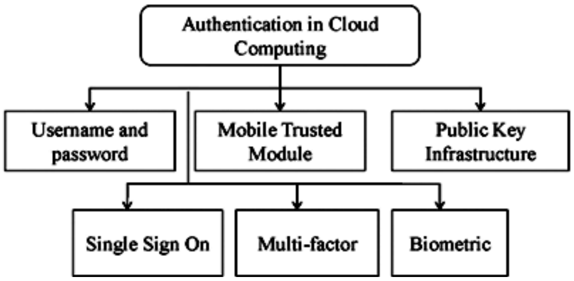

Fig. 1: Authentication methods in cloud computing

- Something user know (knowledge factors) such as username and password, PIN based authentication scheme and Implicit Password Authentication System (IPAS)
- Something user has (possession factor) such as smart cards or electronic tokens and identify card such as Automatic Teller Machine card (ATM card)
- Something user is (ownership factor) such as biometric authentication

Brainard *et al.* (2006) presented one more authentication scheme which is someone you know. It is well known as social networking. Strong method of authentication should cover one or several various factors of identification to improve security. The important drawback of authentication method which relies on possession or knowledge or both factors is their inability to distinguish between authorized users and unauthorized users who are in possession of valid passwords (Anzaku *et al*., 2010). Figure 1 shows all of the authentication method in cloud environment. Details of different techniques of authentication in cloud environment are discussed in next sections.

Username and password authentication: The most important point of authentication is to protecting the data from accessing of unauthorized person. It needs servers to reject requests from unknown visits and to manage the access of authenticated users. In this method of authentication, user should insert username and password to login to the system and can access to the information in CSP.

It is extensively supposed username and password is not very secure authentication mechanism because it is difficult to confirm that the demand is from the rightful or legal owner. Moreover, commonly users choose easy passwords for a machine to guess. Even the best password can be stolen by dictionary and brute force attacks (Karnan *et al*., 2011; Acar *et al*., 2013). In cloud computing the input constraints construct it hard for users to input complex passwords, often leading to the employ of short passwords and password managers. In addition, users reuse their passwords for identifying in different servers and they use weak passwords which cause to increase risks to the security of user's shared information.

The features of this method of authentication can be listed as follows (Abhishek *et al*., 2013):

- Easy to implement
- Requires no special equipment
- Easy to lost or forget
- Vulnerable to shoulder surfing
- Security based on password strength
- Cost of support increases
- Familiar with a lot of users

Increasing the password strength is a solution to avoid dictionary attacks or to make brute force attacks infeasible. It is generally accepted that the length of the password determines the security it provides. Password manager is one of the most common solutions which enable to mitigate these security problems. In general, password managers work by saving users' online passwords and later auto-filling the login forms on behalf of users. Therefore, the main benefit and reason behind designing numerous password managers is that users do not need to remember many passwords (Yassin *et al*., 2012).

Acar *et al*. (2013) presented numerous protocols which can permit a user to use a single password authenticate to identify in multiple services securely. These protocols help to protect users against cross-site attack, dictionary attack, phishing and malware. Main point of proposed protocols is, user's password remains secure even after the mobile device is stolen. Yassin *et al*. (2012) evaluated the phenomenal context according to three main components: data owner, users and service provider in cloud where users do not need to register their passwords in the service provider. Moreover, the data owner is contributed to make secure decisions. Advantages of this method are preserving privacy of password and secrecy of session key. Gurav *et al*. (2014) proposed graphical password authentication for improving security of CC. They presented an identification algorithm by using username and images as a password.

Multi-factor authentication: Traditional password authentication does not provide enough security for information in cloud computing environment to the most modern means of attacks. A more secure scheme is the multi-factor authentication which does not only verify the username/password pair, but also needs second factor such as biometric authentication. However, the feasibility of second factor authentication is limited by the deployment complexity, high cost. MFA technique uses combination of something you have, something you know as well as something you are to supply stronger authentication method. It is stronger user identification techniques. In fact, the trust of authenticity increases exponentially when more factors are involved in the verification process. For example, ATM transaction requires multifactor authentication, something the user possesses (i.e., the card) combined with something the user knows (i.e., PIN) (Karnan *et al*., 2011; Abhishek *et al*., 2013).

Ziyad and Kannammal (2014) proposed a multifactor biometric authentication system for cloud computing environment. These biometric methods are finger print and palm vein. The goal is to handle the biometric data in a secure fashion by storing the palm vein biometric data in multi-component smart cards and fingerprint data in the central database of the cloud security server. In this method, the processes of matching biometric data are performed on the card with Match-on-Card technology; therefore it helps to improve security. A type of multi-factor authentication using fingerprints and user-specific random projection was presented in Anzaku *et al*. (2010). The proposed method used the concept of random projection and fixed length fingerprint feature extraction to generate revocable and privacy preserving templates that yield high authentication accuracy. This feature vector is known as finger code.

Pointcheval and Zimmer (2008) introduces a security model for multi-factor authenticated key exchange, which combines, a secure device, a password, as well as biometric authentications. Anzaku *et al*. (2010) proposed a multi-factor authentication mechanism using user-specific pseudo random numbers (Chen and Li, 2013; Yassin *et al*., 2012; Arriaga and Vempala, 1999; Cardoso and Wichert, 2012) and fixed length fingerprint feature extraction (Jain *et al*., 2000; Liu, 2010) to provide privacy preserving biometric templates that yield high authentication accuracy. This feature vector is known as finger code. Obtained results shown that using this method helps to decrease Equal Error Rates (EER) to 0.4% (Anzaku *et al*., 2010). Dinesha and Agrawal (2012) proposed strong method of authentication using multi-level authentication technique which authenticates and produces the password in numerous levels to access the cloud services. First level is organization level password authentication/generation which able to protect cloud servers against unauthenticated organization or hackers. Second layer of authentication is team level password authentication/generation. It helps to identify teams for specific cloud service. In this manner, authentication system can have third, fourth, fifth etc., level. Final level is user level password authentication/generation, to ensure users have certain permission and privileges. Furthermore, they discussed about activities, architecture, algorithms, as well as data flows.

Ramgovind *et al*. (2010) presented a new agent based protocol uses multiple factors (password and face recognition) on the smart card and the user workstation. This protocol can use in computer and network security. Banyal *et al*. (2013) proposed a new multi-factor authentication framework by improving Cloud Access Management (CAM). Moreover, it used secret-splitting and encrypted value of arithmetic captcha in cloud computing environment. The goal of their research is to analyze the existing security threat to the cloud computing environment and developed a novel secure authentication system using dynamic secure multi-factor secret splitting approach.

Mobile trusted mobile: Trusted Computing Group (TCG) introduced a set of specifications to measure, store and report hardware and software integrity through a hardware root-of-trust, which are the Trusted Platform Module (TPM) and Mobile Trusted Module (MTM). MTM is a security factor for employ in mobile devices. Unlike Trusted Platform Module (TPM) that is for PCs, MTM is employed in mobile devices (Sidlauskas and Tamer, 2008; Sharma *et al*., 2011; Schmidt *et al*., 2008). However, for high levels of protection and isolation, an MTM could be implemented as a slightly modified TPM.

MTM checks all software and applications each time the underlying platform starts due to increase the security of mobile devices. Therefore, the MTM guarantees the integrity of a mobile platform. It has very constraints such as circuit area, as well as available power. Therefore, a MTM needs the spatially-optimized architecture and design method (Kim *et al*., 2010; Acucmez *et al*., 2008). TPM provides trusted information on the internal state of the system and stores cryptographic keys and identities. It is accessed by software using a well-defined command set. Through this command set, the TPM provides cryptographic functionality such as encrypting, signing, key generation and random number generation. It could also store a limited amount of information in nonvolatile memory.

Ekberg (2007) suggests that applying MTM, mobile users make sure that the device is organization under authorized hardware and software. It is mainly applied to authentication terminals from telecommunication to accomplished security functions such as, hash functions, signature schemes, as well as asymmetric encryption; however it is being considered as a cloud computing authentication method with Subscriber Identity Module (Subscriber Identity Module) because of generalization of smart phone. Employing these functionalities user include more confidence in the performance of a mobile platform or establish the reliability of it. Therefore, MTM ensure that reliability of a mobile platform where the mobile device modify into the application tools and open platform (Kim *et al*., 2010).

Grossschadl *et al*. (2008) identifies three main issues in the MTM and provides some possible solutions. The first concern is related to the need of balancing some contrasting goals at the system-level designs, such as power consumption and performance. A suggested solution integrates some TPM features

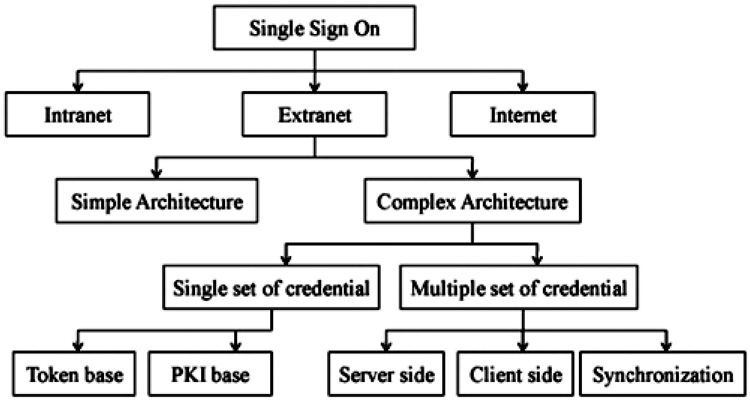

Fig. 2: Different type of SSO

directly into a processor core as opposed to a monolithic implementation of all the functions in a separate module. The second problem is about the cryptographic algorithms which should support by MTM. The suggested solution considers elliptic curve cryptography. Last issue is related to the implementation of cryptographic primitives. Authors propose a hardware/software solution as opposed to a hardware-based solution, which suffers from poor flexibility.

Public key infrastructure: The traditional authentication system is based on the secret key and is mainly support the deployment of traditional asymmetric cryptographic algorithms, such as RSA. It uses a private key to prove the user's identity. PKI has been used in the design of security protocols such as Secure Socket Layer (SSL/TLS) and Secure Electronic Transaction (SET) with the main aim is to provide authentication. The success of PKI like as other type of cryptographic system depends on controlling access to private keys. PKI mechanism has to provide data confidentiality, data integrity, non-repudiation, strong authentication, as well as authorization.

Zissis and Lekkas (2012) proposed assuring security characteristics of cloud environment by using combination of Public Key Infrastructure, SSO, cryptography techniques, as well as LDAP, to ensure the authentication, integrity and confidentiality of involved data and communications. Therefore, this model presented advantages of both single technologies and combination of them. Akyıldız and Ashraf (2014) proposed a survey about traced based public key cryptography over finite fields. This method uses for several cryptography application such as encryption, key agreement, digital signatures. Gordon *et al*. (2010) presented a construction which broad cast protocols still provide the usual grantees (agreement and validity) to the latter. Su and Lü (2012) evaluated definitions of a lever function, as well as coprime sequence. Moreover, they described five algorithms and six characteristics of a prototypal public key cryptosystem.

The main advantage of PKI is to provide authentication users in distributed systems like as cloud computing, mobile cloud computing and wireless sensor network. It is the source of many of the radical advances in the evolution of security solutions to authentication, authorization, confidentiality, integrity and accountability (Haidar and Abdallah, 2009). It has some drawbacks such as possibility of stolen or forgotten and cracked easily.

Single sign on: Single Sign on (SSO) is an identity management system (Chen *et al*., 2011; Brainard *et al*., 2006) which user can authenticate once to a single authentication authority and then they can entrance to other confined resources without re-authenticating. In the other words, this method produces authentication information by using the different applications. The SSO is a way to access the multiple independent software system in such a way that user logs in a system and gains the access to all the system without being prompted to re-login in each application (Radha and Reddy, 2012). Figure 2 shown classification of SSO. This method helps the users to access multiple services and decrease the risk for the administrators to direct users substantively. It supports to enhance user efficiency by preventing the user to remember numerous passwords. It causes to decrease the amount of time the user applies on typing different passwords to login. In addition, it can control the rights of users.

De Clercq (2002) classifies them to four types, where they are deployed, how they are deployed, credentials they use and protocols they use. Revar and Bhavsar (2011) presented a review and comparison on SSO architecture. They did analysis on threats, security requirements and development of new architecture in cloud environment. They considered different factors such as reliability, performance, as well as feasibility of integration.

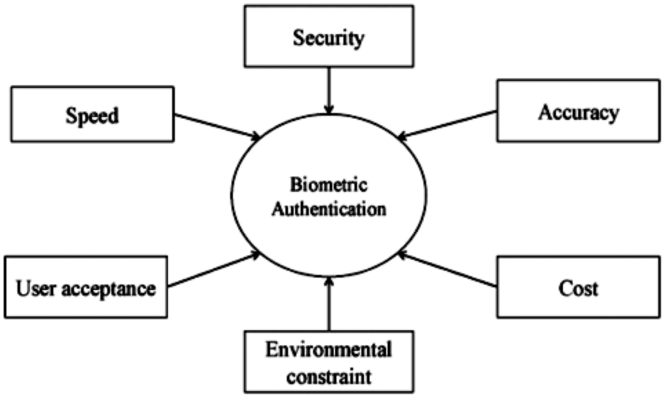

Fig. 3: Objective of biometric authentication

Advantages of SSO are as follow:

- Enhance user efficiency by preventing the user to remember various passwords
- Reducing the number of username/password that should be manage
- Decrease the amount of time the user needs to type different passwords to login
- Increase the security of the system
- Help to administrator by controlling single credential instead of various credentials
- Control rights of users
- Increase the productivity of the organization

BIOMETRIC AUTHENTICATION

Biometric authentication supports the three important factors of information security. These factors are authentication, identification and non-repudiation. It is an ancient Greek word bios = "life" and metron = "measure". This mechanism is based on identifying the living individual's physiological or behavioral attributes. In addition, it is a strong authentication mechanism by providing the factor what we are and what we know (Bhattacharyya *et al*., 2009; Karnan *et al*., 2011). Figure 3 shows five objectives of biometric authentication are security, cost, computation speed, accuracy, user acceptance and environment constraints (Akyıldız and Ashraf, 2014).

Biometric authentication has some advantages. These advantages are as follow:

- Cannot be lost or forgotten (Unlike PKI)
- Can be non-intrusive
- Extremely difficult to copy, share and distribute
- Require the person present to authenticate Difficult to forge (requires more time, money, experience and access privileges)

Therefore, biometric authentication is a suitable mechanism to replace traditional authentication based on cryptographic keys (PKI, as well as username/password authentication), by providing the complete authentication mechanism. However, all of these biometric techniques have their own advantages and disadvantages according to user acceptance, cost and performance. Biometric systems most generally are static authentication systems. In a static authentication system, the identity of the person is verified at the start of that session, for example using a fingerprint to get access to a computer or using an iris scan to get access to a room (Jiang and Zheng, 2014).

Two major vulnerabilities which specially have need more attention in the context of biometric authentication are ‘‘spoof attacks’’ at the user interface, as well as ‘‘template database leakage.’’ A spoof attack involves presenting an imitation biometric trait not obtained from a live person. Template database leakage implies on the situation which valid user's biometric template information becomes available to an adversary.

Biometric authentication (Babaeizadeh *et al*., 2014b) is categorized in two folds, physical and behavioral. Figure 4 shows classification of biometric authentication. Physiological biometrics perform authentication based on bodily characteristics such as fingerprint, hand geometry and face recognition, palm print and iris recognition. It relies on “something the users are”. By contrast, behavioral biometrics authentication is based on the way people do things, such as typing rhythm and signature (Clarke and Furnell, 2005; Karnan *et al*., 2011).

Physical features are more constant over time and under different conditions. Moreover, they are more trustable approaches. Therefore, physical biometric is suitable mechanism for identification based system. Behavioral features are not constant and depend on environment, mood, name a few, illness, previous events, as well as stress. For this reason, behavioral biometrics tends to be only used for authentication-based systems (Sidlauskas and Tamer, 2008). Behavioral biometric provides numerous advantages; it

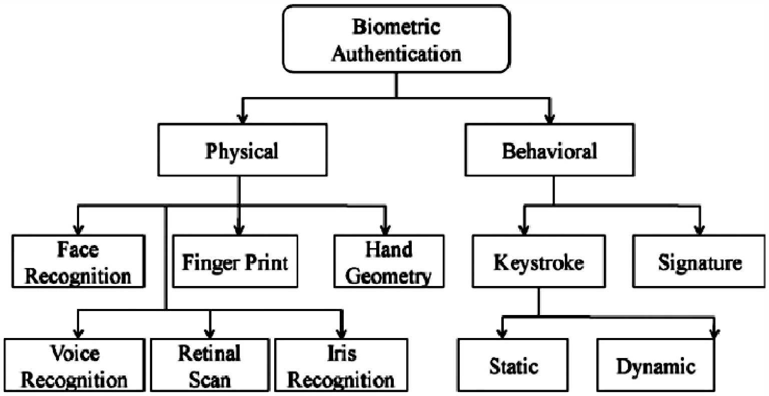

Fig. 4: Classification of biometric authentication

can be collected without knowledge of user (non-intrusive) and it uses in a transparent and continuous authentication system. It does not need any special hardware; therefore it is more cost effective (Bhattacharyya *et al*., 2009; Bhatt and Santhanam, 2013).

Physical biometric: Physical biometric is a type of authentication which is based on physical human characteristics. The main drawback of physical biometric is related to the situation that large numbers of customers are being verified at the same time, the mechanism will become slow. There are different techniques of physical biometric authentication such as hand geometry (Polat and Yıldırım, 2008; Ayurzana *et al*., 2013; Sidlauskas and Tamer, 2008; Kong *et al*., 2009), finger print (Choraś and Piotr, 2007; Duta, 2009), palm print (Dinesha and Agrawal, 2012; Banyal *et al*., 2013; Ziyad and Kannammal, 2014), voice recognition (Ferrer *et al*., 2007), face recognition (Cui and Xue, 2009; Jarng, 2011), retinal scan (Jafri and Arabnia, 2009; Lone *et al*., 2011; Kar *et al*., 2006; Al-Shebani *et al*., 2013), as well as iris scan (Ricco and Chen, 2009; Köse, 2011). However, some of these methods have been used on CC. This section covers these mechanisms.

Behavioral biometric: It is based on the user's behavior. It can identify users based on their location, typing pattern, user profiling and so on. Two important types of behavioral biometric are keystroke analysis (Babaeizadeh *et al*., 2014a; Babaeizadeh *et al*., 2014b; Crawford *et al*., 2013; Gurav *et al*., 2014; Wang *et al*., 2012) and signature recognition (Yassin *et al*., 2012; Qiao *et al*., 2012).

CONCLUSION

Authentication method is main factor of preserving security and privacy of each communication in cloud computing. In fact, the ability to perform suitable user authentication becomes more important issue in CC where it needs to contain some protecting system to preserve sensitive and critical information in CSP. Authentication mechanisms determine "Who is the legal user" and "Is the user really who he claims himself to be". There are numerous methods of authentication in this approach which are username/password, multifactor, MTM, PKI, SSO, as well as biometric authentication. In addition all of these methods have specific subsets.

REFERENCES

Abhishek, K., S. Roshan, P. Kumar and R. Ranjan, 2013. A comprehensive study on multifactor authentication schemes. Adv. Comput. Inform. Technol., 177: 561-568.

Acar, T., M. Belenkiy and A. Küpçü, 2013. Single password authentication. IACR Cryptology ePrint Archive, pp: 167.

Acucmez, O., A. Latifi, J.P. Seifert and X. Zhang, 2008. A trusted mobile phone prototype. Proceeding of 5th IEEE Consumer Communications and Networking Conference (CCNC, 2008).

Akyıldız, E. and M. Ashraf, 2014. An overview of trace based public key cryptography over finite fields. J. Comput. Appl. Math., 259: 599-621.

Al-Shebani, Q., P. Premarante and P.J. Vial, 2013. Embedded door access control systems based on face recognition: A survey. Proceeding of 7th International Conference on Signal Processing and Communication Systems (ICSPCS, 2013), pp: 1-7.

Anzaku, E.T., H. Sohn and Y.M. Ro, 2010. Multi-factor authentication using fingerprints and user-specific random projection. Proceeding of 12th International Asia-Pacific Web Conference (APWEB, 2010), pp: 415-418.

Arriaga, R.I. and S. Vempala, 1999. An algorithmic theory of learning: Robust concepts and random projection. Proceeding of 40th Annual Symposium on Foundations of Computer Science, pp: 616-623.

Ayurzana, O., B. Pumbuurei and H. Kim, 2013. A study of hand-geometry recognition system. Proceeding of 8th International Forum on Strategic Technology (IFOST, 2013), 2: 132-135.

Babaeizadeh, M., M. Bakhtiari and M. Aizaini Maarof, 2014a. Keystroke dynamic authentication in mobile cloud computing. Int. J. Comput. Appl., 90(1): 29-36.

Babaeizadeh, M., M. Bakhtiari and M.A. Maarof, 2014b. Authentication method through keystrokes measurement of mobile users in cloud environment. Int. J. Adv. Soft Comput. Appl., 6(3).

Banyal, R.K., P. Jain and V.K. Jain, 2013. Multi-factor authentication framework for cloud computing. Proceeding of 5th International Conference on Computational Intelligence, Modelling and Simulation (CIMSim), pp: 105-110.

Behl, A., 2011. Emerging security challenges in cloud computing: An insight to cloud security challenges and their mitigation. Proceeding of World Congress on Information and Communication Technologies (WICT, 2011), pp: 217-222.

Bhatt, Sh. and T. Santhanam, 2013. Keystroke dynamics for biometric authentication-a survey. Proceeding of International Conference on Pattern Recognition, Informatics and Medical Engineering (PRIME), pp: 17-23.

Bhattacharyya, D., R. Ranjan, A. Farkhod Alisherov and M. Choi, 2009. Biometric authentication: A review. Int. J. u-and e-Serv. Sci. Technol., 2(3): 13-28.

Bouayad, A., A. Blilat, N. El Houda Mejhed and M. El Ghazi, 2012. Cloud computing: Security challenges. Proceeding of IEEE Colloquium in Information Science and Technology (CIST, 2012), pp: 26-31.

Brainard, J.G., A. Juels, R.L. Rivest, M. Szydlo and M. Yung, 2006. Fourth-factor authentication: Somebody you know. Proceeding of ACM Conference on Computer and Communications Security, pp: 168-178.

Cardoso, Â. and A. Wichert, 2012. Iterative random projections for high-dimensional data clustering. Pattern Recogn. Lett., 33(13): 1749-1755.

Chen, D.R. and H. Li, 2013. Convergence rates of learning algorithms by random projection. Appl. Comput. Harmon. A., 37(1): 36-51.

Chen, J., G. Wu, L. Shen and Z. Ji, 2011. Differentiated security levels for personal identifiable information in identity management system. Expert Syst. Appl., 38(11): 14156-14162.

Choraś, M. and M. Piotr, 2007. Keystroke dynamics for biometric identification. In: Beliezynski, B. and *et al*. (Eds.): ICANNGA 2007. Part 2, LNCS 4432, Springer-Verlag, Berlin, Heidelberg, pp: 424-431.

Clarke, N.L. and S.M. Furnell, 2005. Authentication of users on mobile telephones-A survey of attitudes and practices. Comput. Secur., 24(7): 519-527.

Crawford, H., R. Karen and S. Tim, 2013. A framework for continuous, transparent mobile device authentication. Comput. Secur., 39: 127-136.

Cui, B. and T. Xue, 2009. Design and realization of an intelligent access control system based on voice recognition. Comput. Commun. Control Manage., 1: 229-232.

De Clercq, J., 2002. Single sign-on architectures. Infrastructure Secur., 2437: 40-58.

Dinesha, H.A. and V.K. Agrawal, 2012. Multi-level authentication technique for accessing cloud services. Proceeding of International Conference on Computing, Communication and Applications (ICCCA, 2012), pp: 1-4.

Duta, N., 2009. A survey of biometric technology based on hand shape. Pattern. Recogn., 42(11): 2797-2806.

Ekberg, J.E., 2007. Mobile Trusted Module (MTM) -an introduction. Retrieved form: http://research.nokia.com/files/NRCTR2007051.pdf.

Ferrer, M.A., A. Morales, C.M. Travieso and J.B. Alonso, 2007. Low cost multimodal biometric identification system based on hand geometry, palm and finger print texture. Proceeding of 41st Annual IEEE International Carnahan Conference on Security Technology, pp: 52-58.

Gordon, S.D., J. Katz, R. Kumaresan and A. Yerukhimovich, 2010. Authenticated broadcast with a partially compromised public-key infrastructure. In: Dolev, S. and *et al*. (Eds.), SSS 2010. LNCS 6366, Springer-Verlag, Berlin Heidelberg, pp: 144-158.

Grossschadl, J., T. Vejda and D. Page, 2008. Reassessing the TCG specifications for trusted computing in mobile and embedded systems. Proceeding of IEEE International Workshop on Hardware-Oriented Security and Trust (HOST 2008), pp: 84-90.

Gurav, S.M., L.S. Gawade, P.K. Rane and N.R. Khochare, 2014. Graphical password authentication: Cloud securing scheme. Proceeding of IEEE Electronic Systems, Signal Processing and Computing Technologies (ICESC, 2014), pp: 479-483.

Haidar, A.N. and A.E. Abdallah, 2009. Formal modelling of pki based authentication. Electron. Notes Theor. Comput. Sci., 235: 55-70.

Jafri, R. and H.R. Arabnia, 2009. A survey of face recognition techniques. J. Inform. Process. Syst., 5(2): 41-68.

Jain, A.K., S. Prabhakar, L. Hong and S. Pankanti, 2000. Filterbank-based fingerprint matching. IEEE T. Image Process., 9(5): 846-859.

Jarng, S.S., 2011. HMM voice recognition algorithm coding. Proceeding of International Conference on Information Science and Applications (ICISA, 2011), pp: 1-7.

Jeong, H. and E. Choi, 2012. User authentication using profiling in mobile cloud computing. AASRI Procedia, 2: 262-267.

Jiang, X.C. and J.D. Zheng, 2014. An indirect fingerprint authentication scheme in cloud computing. Appl. Mech. Mater., 484: 986-990.

Jivanadham, L.B., A.K.M. Islam, Y. Katayama, S. Komaki and S. Baharun, 2013. Cloud Cognitive Authenticator (CCA): A public cloud computing authentication mechanism. Proceeding of International Conference on Informatics, Electronics and Vision (ICIEV, 2013), pp: 1-6.

Jog, M. and M. Madiajagan, 2012. Cloud computing: Exploring security design approaches in infrastructure as a service. Proceeding of International Conference on Cloud Computing Technologies, Applications and Management (ICCCTAM, 2012), pp: 156-159.

Jula, A., E. Sundararajan and Z. Othman, 2014. Cloud computing service composition: A systematic literature review. Expert Syst. Appl., 41(8): 3809-3824.

Kar, S., S. Hiremath, D.G. Joshi, V.K. Chadda and A. Bajpai, 2006. A multi-algorithmic face recognition system. Adv. Comput. Commun., 3: 321-326.

Karnan, M., M. Akila and N. Krishnaraj, 2011. Biometric personal authentication using keystroke dynamics: A review. Appl. Soft. Comput., 11(2): 1565-1573.

Khalid, U., A. Ghafoor, M. Irum and M.A. Shibli, 2012. Cloud based secure and privacy enhanced authentication and authorization protocol. Procedia Comput. Sci., 22: 680-688.

Kim, M., H. Ju, Y. Kim, J. Park and Y. Park, 2010. Design and implementation of mobile trusted module for trusted mobile computing. IEEE T. Consum. Electr., 56(1): 134-140.

Kong, A., D. Zhang and M. Kamel, 2009. A survey of palmprint recognition. Pattern Recogn., 42(7): 1408-1418.

Köse, C., 2011. A personal identification system using retinal vasculature in retinal fundus images. Expert Syst. Appl., 38(11): 13670-13681.

Liu, M., 2010. Fingerprint classification based on Adaboost learning from singularity features. Pattern. Recogn., 43(3): 1062-1070.

Lone, M.A., S.M. Zakariya and R. Ali, 2011. Automatic face recognition system by combining four individual algorithms. Proceeding of International Conference on Computational Intelligence and Communication Networks (CICN), pp: 222-226.

Manvi, S.S. and G. Krishna Shyam, 2013. Resource management for infrastructure as a Service (IaaS) in cloud computing: A survey. J. Netw. Comput. Appl., 41: 424-440.

Pearson, S., Y. Shen and M. Mowbray, 2009. A privacy manager for cloud computing. In: Jaatun, M.G., G. Zhao and C. Rong (Eds.), CloudCom 2009. LNCS 5931, Springer, Berlin, Heidelberg, pp: 90-106.

Pointcheval, D. and S. Zimmer, 2008. Multi-factor Authenticated Key Exchange. In: Bellovin, S.M. (Eds.), ACNS. Springer-Verlag, Berlin, Heidelberg, pp: 277-295.

Polat, Ö. and T. Yıldırım, 2008. Hand geometry identification without feature extraction by general regression neural network. Expert Syst. Appl., 34(2): 845-849.

Popovic, K. and Z. Hocenski, 2010. Cloud computing security issues and challenges. Proceeding of the 33rd International Convention on MIPRO, 2010.

Qiao, Y., X. Jiang, H.W. Lin and J.S. Pan, 2012. Efficient identity based threshold proxy signature scheme in cloud environment. Proceeding of International Conference on Information Security and Intelligence Control (ISIC, 2012), pp: 53-56.

Radha, V. and D.H. Reddy, 2012. A survey on single sign-on techniques. Procedia. Technol., 4: 134-139.

Ramgovind, S., M.M. Eloff and E. Smith, 2010. The management of security in cloud computing. Proceeding of Information Security for South Africa (ISSA), pp: 1-7.

Revar, A.G. and M.D. Bhavsar, 2011. Securing user authentication using single sign-on in cloud computing. Proceeding of International Conference on Engineering (NUiCONE), pp: 1-4.

Ricco, S. and M. Chen, 2009. Classification of scan location in retinal optical coherence tomography. Proceeding of Biomedical Imaging: From Nano to Macro (ISBI'09), pp: 1031-1034.

Schmidt, A.U., N. Kuntze and M. Kasper, 2008. On the deployment of mobile trusted modules. Proceeding of IEEE Wireless Communications and Networking Conference (WCNC, 2008), pp: 3169-3174.

Sharma, P., S.K. Sood and S. Kaur, 2011. Security issues in cloud computing. In: Mantri, A. (Ed.), High Performance Architecture and Grid Computing. Springer-Verlag, Berlin, Heidelberg, pp: 36-45.

Sidlauskas, D.P. and S. Tamer, 2008. Hand geometry recognition. In: Jain, A.K., P. Flynn and A.A. Ross (Eds.), Handbook of Biometrics. Springer, US, Boston, pp: 91-107.

Su, S. and S. Lü, 2012. A public key cryptosystem based on three new provable problems. Theor. Comput. Sci., 426: 91-117.

Subashini, S. and V. Kavitha, 2011. A survey on security issues in service delivery models of cloud computing. J. Netw. Comput. Appl., 34(1): 1-11.

Wang, X., G. Fangxia and M. Jian-feng, 2012. User authentication via keystroke dynamics based on difference subspace and slope correlation degree. Dig. Signal. Process., 22(5): 707-712.

Winkler, 2011. Cloud computing architecture in securing the cloud. Syngress, pp: 29-53.

Wu, L., S. Kumar Garg and R. Buyya, 2012. SLA-based admission control for a software-as-a-service provider in cloud computing environments. J. Comput. Syst. Sci., 78(5): 1280-1299.

Xie, G. and B. Yao, 2013. Cloud storage identity design based on fingerprint identification. Proceeding of 6th International Conference on Information Management, Innovation Management and Industrial Engineering (ICIII), 1: 569-572.

Yassin, A.A., H. Jin, A. Ibrahim and D. Zou, 2012. Anonymous password authentication scheme by using digital signature and fingerprint in cloud computing. Proceeding of 2nd International Conference on Cloud and Green Computing (CGC, 2012), pp: 282-289.

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

Ziyad, S. and A. Kannammal, 2014. A Multifactor Biometric Authentication for the Cloud. Adv. Intell. Syst. Comput., 246: 395-403.