International Journal of
Scientific Engineering and Technology Research

ISSN 2319-8885
Vol.06,Issue.03
January-2017,
Pages:0458-0464

www.ijsetr.com

Cloud Computing Authentication Techniques: A Survey

DR. V. V. S. S. S. BALARAM
Professor & HOD, Dept of IT, Sreenidhi Institute of Science and Technology, Ghatakesar, Hyderabad, TS, India.

Abstract: Cloud computing model is a newly upcoming technology for sharing the resources for complicated systems with large scale among different clients. So that authentication of each client and services is very important issue for the security and trust of the cloud computing technology. For this purpose cloud computing model implements a protocol called Secure Socket Layer Authentication Protocol (SAP), once this protocol is implemented in cloud computing model then it becomes sophisticated at clients can loaded in each communication and computation. At the time of this study presents a review on the assorted ways of authentication in setting cloud computing environment. In cloud computing Authentication plays a very important role to provide security. Authentication protects Cloud Service suppliers against various types of attacks; here the aim of authentication is to verify a client's identity once a client needs to request services from cloud servers. There are various types of authentication technologies that verify the identity of a client before giving the access to resources.

Keywords: Cloud Computing, Authentication Protocol, Cloud Service Provider, Access, Environment.

I. INTRODUCTION

Cloud computing is standard architecture for providing on demand network access to a software, shared data, infrastructure and platform resources which can be quickly granted and released with minimum organizing effort or service provider interaction. It helps to improve the effectiveness of Information Technology by providing various services. Cloud computing (CC) is an architecture of computing in which dynamically expandable and often virtualized resources are granted as a service over the Internet. Cloud customers need not have proficient in, Knowledge of, or control over the technology infrastructure 'in the cloud' that supports them. Authentication, thus, becomes pretty important for cloud security. Applied to cloud computing and depending on standard X.509 certificate-based PKI authentication framework, SSL Authentication Protocol (SAP) is low efficient. The researchers of Grid Security Infrastructure accepted that the current GSI technique has a poor scalability. W.B. Mao et al [28] analyzed that this scalability problem is an inherent one due to the use of SSL Authentication Protocol. Grid computing and cloud computing is so similar that grid security technique can be applied to cloud computing. Dai et al[11][12][13][14]. made great contribution to Grid security. There are basically four kinds of authentication methods:

- Something an individual KNOWS (e.g. password, Personal ID)
- Something an individual POSSESSES (e.g., a token or card)
- Something an individual IS (e.g. fingerprint or voice pattern).
- Something an individual DOES.

Recently many security researchers are focusing on different new techniques of authentication in cloud computing that incorporate one or more of the above notified methods of authentication. Therefore it becomes necessary to survey the various authentication methods recently proposed and implemented in the Cloud computing environment.

II. LITERATURE SURVEY

In recent times, identity-key-based cryptography (IBC) is developed very quickly. The main theme of applying IBC to grid security was basically explored by Lim et al [24][25]. Mao et al.[28] initiated an identity-key-based non-interactive authentication Frame work for grid. The framework is certificate-free. But the same Private Key Generator (PKG) becomes the bottleneck of framework. Lim and Robshow [24][25] proposed a hybrid method for combining IBC . The method solves escrow and distribution of private key. Anyway, the non-interactive and certificate-free quality is lost. Chen (2005)[9] revised the GSI in the GT version2 and improved the GSI architecture and protocols. It is significant to study IBC and cloud computing. Three important aspects of cloud security requirements are availability, confidentiality, and integrity. These aspects are well known as CIA. Confidentiality means keeping customers information secret in CSP and only authorized customers (computers and users) grant accessing to protected data. It depends on various aspects such as encryption methods (symmetric or asymmetric algorithm), key length (in symmetric algorithm) and Cloud Service Provider (CSP) (Sharma et al., 2011)[32].

In Cloud Computing, confidentiality has a major role in protect control on organizations' data situated across multiple distributed databases. Integrity means that an unofficial person is not permitted to modify, fabricate and delete

sensitive data in cloud servers. By protecting unauthorized access (confidentiality), organizations can achieve greater assurance in information and system integrity. The main aim of availability is to ensure that unauthorized person cannot approach to shared data in cloud service provider (any time and any place). Cloud servers must have the ability to extend operations even in the possibility of a security breach. Denial of Service attacks (DOS), natural disasters, as well as equipment outages can risk to availability. Cloud computing is an internet based technology which provides various services over the internet. These services appreciably effects on economy in terms of efficiency, scalability as well as energy, cost reducing. A service is a method that is capable of providing functionalities for using in compliance with considering rules. Cloud computing services can divided in three types by Banyal et al., 2013[4].

Platform as a Service (PaaS), Software as a Service (SaaS) Infrastructure as a Service (IaaS), Gibson and Elveleigh (Behl, 2011)[5] given various advantages of these cloud services. SaaS is an on-demand application in the first layers. It provides software as a service through the Internet such as Google Docs, Zoho, as well as Microsoft CRM. Software as a Service over comes the problem of installing and running the application on the customers end (Jog and Madiajagan, 2012[19]; Ziyad and Kannammal, 2014[39]).The second layer (outgrowth of IaaS) is PaaS. It allows users to rent database management system, operating systems, hardware, tools for design and network capacity (hosting) through the Internet (Ramgovind et al., 2010)[30]. Subashini and Kavitha (2011)[34] discussed about some security issue in this model. IaaS is bottommost layer. IaaS provides basic computing infrastructure components such as Storage, CPU and memory. It implies the combination of hosting, hardware provisioning and basic services needed to execute on cloud computing. Infrastructure is underlying physical components that are required for a system to perform its operations. Manvi and Krishna Shyam (2013)[27] discussed about some problems in IaaS.

There are other types of cloud services such as Monitoring as a Service (MaaS), Data Storage as a Service (DSaaS), Communication as a Service (CaaS), Business as a Service (BaaS) and Security as a Service (SecaaS).Cloud services can be organized based on four different deployment models private cloud, public cloud, hybrid cloud, as well as community cloud. Private cloud is platform of cloud which is dedicated for precise user or organization. Unlike public cloud which the numerous layers may be offered by multiple providers the entire stack (IaaS, PaaS and SaaS) managed by a single provider. Therefore, it has access and control over the various applications, infrastructure and middleware (Wu et al., 2012)[36]. Community cloud is a type of cloud model which shared by various organizations and supports a precise community. Furthermore, it may be operated by the organizations or a third party (Behl, 2011)[5]. Public cloud (Ramgovind et al., 2010)[30] refers to a model which grant client access to the cloud through interfaces using mainstream web browsers (available to public users). It is the most dominant model 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 keeps same entities (Bouayad et al., 2012)[7]. However cloud computing offers numerous advantages such as low cost cloud storage and shared infrastructure (Ricco and Chen[31], 2009) The most dangerous issue that cloud computing faces concerns its inability to insure data privacy and confidentiality and there are different security and privacy issues in this area implemented various models of privacy manager in Cloud Computing, which decrease the hazard of steal and misuse of shared information in CSP. In fact, these techniques help to provide security for their sensitive and critical data in the cloud models. Behl (2011)[5] studied security approaches of cloud infrastructure and their Weaknesses. The goal of this research is to implement a security strategy and improve the security of cloud environment.

One of the important ways which will help to reduce privacy and security risks is Access Control (AC). It refers to techniques that allow performing operations up to their authorized level and restricting users from performing unauthorized function. AC mechanisms can categorized to three parts authentication of users, authentication of their privileges and auditing to monitor and record actions of customers. It is the process of certainty of what an authenticated user can do. It is self-reliant of authentication. Furthermore, authorization servers are responsible for receiving and validating the user access request to some specific utilities. It manages a list of all the policies related to the users in the policy engine and updates them when needed. If a request is successfully validated, the authorization server allow to the user access to the desired resource for a particular amount of time (Khalid et al., 2012[21]). Auditing helps to ensure that users are accountable. Cloud servers accounts actions in audit trails and logs. For instance, a user attempting numerous failed logins might be seen as an intruder. Customer authentication on cloud computing model is very important issue, because it guarantees that somebody works or shares information with the right person and that only authenticated users can access to data or application. Authentication compelling some form of “proof of identity”. There is increasing appeal for suitable authentication technique for accessing to the shared information via the Internet through Cloud Service Provider (CSP). Therefore, numerous mechanisms used to authenticate users in cloud computing model. These methods are multi-factor, Single Sign On (SSO), Mobile Trusted Module (MTM), username and password, Public Key Infrastructure (PKI), as well as biometric authentication. This paper reviews various techniques of authorization in cloud environment. These methods are typically employed to enhance the security of CC.

III. SECURITY IN CLOUD COMPUTING

Cloud computing paradigm has many benefits in lowering cost, sharing resources, time saving for new service

implementation. While in a cloud computing model, most of the data and applications that clients use stay back on the Internet, it gets some new problems for the system, especially privacy and security of the system. Since each service may use resource from different multiple servers. The servers are geographically located at multiple locations and the services offered by the cloud may use different infrastructures with various organizations. All these characteristics of cloud computing make it more difficult to provide security in cloud computing. To provide improved security in cloud computing, various security issues like data authentication, data integrity, data confidentiality and non-repudiation all need to be considered into account. Now days, maximum of cloud services used WS-Security service to provide security for the system. In WS-Security, XML encryption and XML signature are used to enable data integrity and confidentiality. Mutual authentication can be backed by adding Kerberos tickets and X.509 certificate into SOAP message header. As discussed in the previous section, there are three types of major clouds in general they are: private cloud, public cloud and hybrid cloud. In a public cloud, dynamically resources are provisioned on a self-service, fine-grained basis over the Internet.

Services in the cloud are given by an off-site third-party provider who shares resources and bills on a fine-grained utility computing basis. While in most private clouds, with minimum computing resources, it is very complex for a private cloud to provide all services for their clients, as some services may more resources than internal cloud can provide. Hybrid cloud is a possible solution for this issue since they can get the computing resources from external cloud computing providers. Private clouds have some advantages in managing the company and it provide reliable services, as well as they grant more management over public clouds do. For the security reasons, when a cloud environment is enabled inside a firewall, it can provide less publicity to the Internet security risks to its clients. Also in the private cloud, the services of cloud can be acquired by internal connections only, it makes easier to use existing security measures and standards. Because of these reasons private clouds more appropriate for services with sensitive data that must be protected. But in case of hybrid cloud, it combines more than one domain; it will increase the complexity of security provision, especially mutual authentication and key management.The hybrid cloud domains can be heterogeneous networks; so there may be gaps between these different networks and between the different services providers.

In the case of Public and private clouds provide well guaranteed security because of their unique network models. But in the case of hybrid clouds it is very difficult to provide guaranteed security because of its different set of network conditions and different security policies, For example, cross domain authentication can be a problem in a hybrid cloud with different domains.Although some authentication services such as Kerberos can provide multi-domain authentication, but one of the requirements for the multi-domain Kerberos authentication is that the Kerberos server in each domain needs to share a secret key with servers in other Kerberos domains and every two Kerberos servers need to be registered with each other. The problem here is if there are N Kerberos domains and each of them want to trust each other, then the number of key exchanges is N(N-1)/2. For a hybrid cloud with a large number of domains, this will bring a problem for scalability. If different networks in a hybrid cloud using different authentication protocols, this problem can be more complex.

IV. AUTHENTICATION TECHNIQUES IN CLOUD

Authentication is a major criteria of each secure communication system especially in wide networks such as Cloud Computing. It guides to protect shared data from unauthorized access and it is a major technique of information security. AAA is a security organizing module for authentication, authorization and accounting. When a user tries to access cloud resources from CSP, then AAA verifies the user's authentication information. If the user is authenticated, then AAA gets the user's access level, which has been most recently pro, by inspecting the user's information in the database. In addition, authentication technique says that “Who is the authorized customer” and “Is the customer really who he claims himself to be”. In addition, verification of customer’s identity is the most important aim behind an authentication. In other words, an authentication mechanism tells how customers identified and verified to access to sensitive data (Köse, 2011)[23]. Verification means confirm that demand is from the legal user. Identification implies on determining users. There are several authentication schemes (Pointcheval and Zimmer, 2008[29]) which categorized in three types as follow:

- 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.

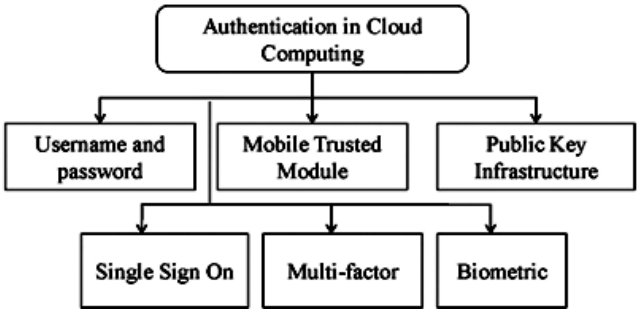

Fig.1. Authentication methods in cloud computing.

Brainardetal.(2006)[28] 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 impotence to distinguish between authorized customers and unauthorized customers who are in possession of valid passwords. Fig.1 shows all of the authentication method in cloud environment. Details of different techniques of authentication in cloud environment are discussed in next sections.

A. 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 enter 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 strong password can be stolen by brute force attacks and dictionary (Karnan et al., 2011;[20]). 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 benifit of this technique of authentication can be listed as follows :

- 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

Providing stronger password is a solution to avoid dictionary attacks or to make brute force attacks infeasible. It is generally popular and everyone says 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)[37]. Acar et al. (2013)[1] 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)[37] evaluated the phenomenal context according to three main components: data owner, customers and cloud service provider in cloud where customers do not need to register their passwords in the cloud service provider. Moreover, the authorized owner of data is contributed to make secure decisions. Advantages of this method are preserving privacy of password and secrecy of session key. Gurav et al. (2014)[17] proposed graphical password authentication for improving security of CC. They presented an identification algorithm by using username and images as a password.

B. Multi-Factor Authentication

Traditional password authentication technique does not afford ample 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 customer possesses (i.e., the card) clubed with something the customer knows (i.e., PIN) (Karnan et al., 2011[20]).Ziyad and Kannammal (2014)[39] 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)[3]. 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)[29] 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)[3] proposed a multi-factor authentication mechanism using user-specific pseudo random numbers (Chen 2013[9]; Yassin et al., 2012;[37])and fixed length fingerprint feature extraction (Banyal et al., 2000[4];Liu, 2010[26]) 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[3]). Dines ha and Agarwal (2012)[15] 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)[30] 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)[4] proposed a new multifactor 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.

C. Mobile Trusted Module

Trusted Computing Group (TCG) introduced a group of specifications to report, store and measure hardware and software integrity through a hardware root-of-trust, which are the Trusted Platform Module (TPM) and Mobile3 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[33]; Sharma et al., 2011[32]). 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[22]). TPM provides trusted information on the internal state of the system and stores cryptographic identities and keys. It is accessed by software using a well-defined command set. Through this command set, the TPM gives cryptographic functionality such as random number generation, key generation, signing and encrypting. It could also store a limited amount of information in nonvolatile memory.

D. Public Key Infrastructure

The conventional authentication system is based on the secret key and is mainly support the deployment of conventional asymmetric cryptographic algorithms, such as RSA. It uses a private key to prove the user's identity. PKI has been used in developing 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)[38] proposed assuring security characteristics of cloud environment by using combination of Public Key Infrastructure, SSO, cryptography techniques, as well as LDAP, to ensure the integrity, confidentiality and authentication of involved data and communications. Therefore, this model presented advantages of both single technologies and combination of them. Akyıldız and Ashraf (2014)[2] 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)[16] presented a construction which broad cast protocols still provide the usual grantees (agreement and validity) to the latter. Su and Lu (2012)[35] 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 profound improvements in the evolution of security solutions to authentication, authorization, confidentiality, integrity and accountability (Haidar and Abdallah, 2009[38]). It has some drawbacks such as possibility of stolen or forgotten and cracked easily.

E. Single Sign On

Single Sign on (SSO) is an identity management system (Chen et al., 2011[9]; Brainard et al., 2006[8]) 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

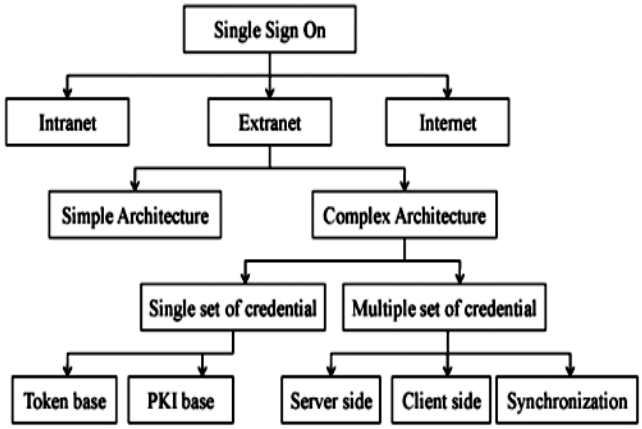

Fig.2. Types of SSO.

Independent software system in such a way that user logs in a system and gains the access to every system without being further to re-login in each application. Fig.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.

F. Biometric Authentication

Biometric authentication strongly supports the three important points of information security. These factors are non-repudiation, identification and authentication. It is an ancient Greek word bios = "life" and metron = "measure".

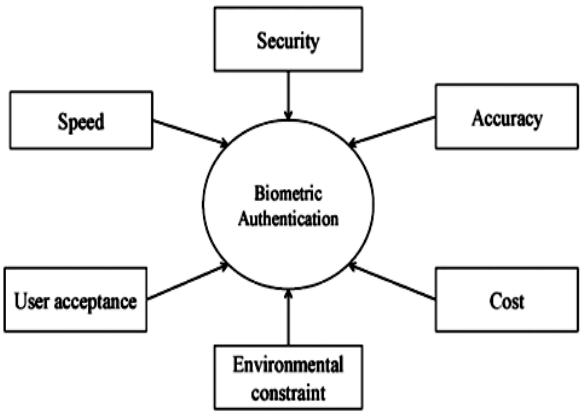

Fig. 3. Objective of Bio Metric Authentication.

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[6]; Karnan et al., 2011[20]). Fig. 3 shows five objectives of biometric authentication are accuracy, user acceptance, computation speed, security, cost and environment constraints (Akyıldız and Ashraf, 2014[2]).

V. CONCLUSION

Authentication method is main factor of preserving security and privacy of each communication in the cloud environment .In fact the ability to perform suitable user authentication become major important issue in cloud computing where it needs to have some secure system to preserve sensitive and critical information in CSP. Authentication technique is to find out "who is the authorized customer and is the customer really who he climes himself to be .There are numerous methods of authentication in this approach which are username and password, multifactor, MTM,PKI, SSO and biometric authentication. In addition all of this has specific sub sets.

VII. REFERENCES

[1]Acar.T,M.Belenkiy and A.Kupcu 2013 single password authentication.IACR cryptology ePrint Archive,PP:167.

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

[3]Anzaku,E.T,H.Sohn and Y.M.Ro,2010.Multifactor Authentication using fingerprints and user specific random projection.Proceding of 12th International Asia-Pacific web conference (APWEB,2010),pp:415-418.

[4]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.

[5]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.

[6]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.

[7]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.

[8]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.

[9]Chen, L., Lim, H.W., Mao, W.B.: User-friendly grid security architecture and protocols.In: Proceedings of the 13th International Workshop on Security Protocols (2005).

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

[11]Dai, Y.S., Levitin, G.: Reliability and Performance of Tree-structured Grid Services. IEEE Transactions on Reliability 55(2), 337–349 (2006).

[12]Dai, Y.S., Levitin, G., Trivedi, K.S.: Performance and Reliability of Tree-Structured Grid Services Considering Data Dependence and Failure Correlation. IEEE Transactions on Computers 56(7), 925–936 (2007).

[13]Dai, Y.S., Pan, Y., Zou, X.K.: A hierarchical modelling and analysis for grid service reliability. IEEE Transactions on Computers 56(5), 681–691 (2007)

[14]Dai, Y.S., Xie, M., Wang, X.L.: Heuristic Algorithm for Reliability Modeling and Analysis of Grid Systems. IEEE Transactions on Systems, Man, and Cybernetics, Part A 37(2), 189–200 (2007).

[15]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.

[16]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.

[17]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.

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

[19]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.

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

[21]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.

[22]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. Electrical., 56(1): 134-140.

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

[24]Lim, H.W., Robshaw, M.: On Identity- Based. Cryptography and Grid Computing. In: Bubak, M., van Albada, G.D., Sloot, P.M.A., Dongarra, J. (eds.) ICCS 2004. LNCS,vol. 3036, pp. 474–477. Springer, Heidelberg (2004).

[25]Lim, H.W., Robshaw, M.: A dynamic key infrastructure for GRID. In: Sloot, P.M.A.,Hoekstra, A.G., Priol, T., Reinefeld, A., Bubak, M. (eds.) EGC 2005. LNCS, vol. 3470,pp. 255–264. Springer, Heidelberg (2005).

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

[27]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.

[28]Mao, W.B.: An Identity-based Non- interactive Authentication Framework for Computational Grids, May 29 (2004), http://www.hpl.hp.com/ techreports/2004/HPL-2004-96.pdf

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

[30]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.

[31]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.

[32]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. Yassin, A.A., H. Jin, A. Ibrahim and D. Zou, 2012.

[33]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.

[34]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.

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

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

[37]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.

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

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