ISSN 2320-9984
Volume 4 Issue 2 | June 2016 ISSN: 2320-9984 (Online)
International Journal of Modern Engineering & Management Research
Website: www.ijmemr.org

Review of Authentication Mechanisms in Cloud Computing

Dharmendra Likhare
Lecturer CSE
Department of Computer Science and Engineering
Kalaniketan Polytechnic College,
Jabalpur (M.P.), [INDIA]
Email: dlikhare103@rediffmail.com

Saket Kumar Soni
M. Tech. Research Scholar
Shriram Group of Institutions
Jabalpur (M.P.), [INDIA]
Email: sonisaket1@rediffmail.com

Anupam Choudhary
Lecturer CSE
Department of Computer Science and Engineering
Kalaniketan Polytechnic College,
Jabalpur (M.P.), [INDIA]
Email: choudharyanupam7@yahoo.com

Abstract*—Cloud Computing is the most emerging trend in Information Technology now days. It is attracting the organizations due to its advantages of scalability, throughput, easy and cheap access and on demand up and down grading of SaaS, PaaS and IaaS. Besides all the salient features of cloud environment, there are the big challenges of privacy and security. In this paper, a review of different security issues like trust, confidentiality, authenticity, encryption, key management and resource sharing are presented along with the efforts made on how to overcome these issues.*

Keywords:— *cloud security, Authentication, encryption, decryption, attacks, and cryptography.*

1. INTRODUCTION

Cloud computing is new boon in IT sector were companies needs storage on different scale. The facility to unlimited data storage, infinite data usage, cost efficiency, recovery, automatic software integration, back-end storage, accessible information. It is divided into three main categories: Software – as-a-Service (SaaS), Platform-as-a-Service (PaaS), and Infrastructure- as-a-Service (IaaS) [1], [11]. It does not limit on data and expands or compress on demand. The Cloud has many security issues in the field of networking, virtualization, memory and database.

With emerge of cloud usage security issues are also emerging as well. Various scheme is provided for the security in cloud computing on user side, transmission of data, and server side. Most vulnerable attacks in cloud computing are data leakage, Dos attacks, DDos attack. The openness of cloud causes emerging of many laws which are vulnerable to attack [5].

In cloud computing many papers are proposed for the security of cloud services. In cloud computing authentication is a major concern. Authentication stop attackers to misuse the content stored in cloud storage. In cloud computing still require a well-defined authentication scheme. First step required to identify the user is to verify through authentication. Authentication is referred to as a process that forms the authorization of the respective identity of the individuals [6],[19].

Authentication is done through different ways:

1. Things he/she knows: Passwords, Personal Id.
2. Things he/she possesses: Tokens, card.
3. Things he/she has: biometric identification –voice, iris, and fingerprint.
4. Thigs he/she does: History of internet usage Many researcher use one method or include more than one mechanism to form more secured authentication scheme. Therefore it became inevitable to review different authentication scheme.

2. DIFFERENT AUTHENTICATION SCHEME IN CLOUD COMPUTING

In cloud computing there are many ways for authentication and as per there are many kind of attacks developed. Different kind of attacks has been identified since authentication scheme has been introduced [12]. The comprehensive list of different kind of attacks are given below:

To counter these attacks many different authentication scheme and protocols has been introduced so far either one or authenticate the user and verifier and verifies the client to verifier and so verifier to the client. This overview will formulate the different authentication scheme and protocols to understand the designing a security system [2], [20].

A. Passwords

Passwords most common way for authentication. Users provide the identity details, and password in word, phrase, or token formed card etc. Passwords are easy to crack, brute force is the most common way to get it. The risk of eavesdropping can cause high risk.

Table 1. Authentication Attacks

Attacks	Description
Brute Force	Repeatedly entering the data as hit and trial method entering it manually.
Weak password recovery validation	The attackers access the website which allow them to get or access to third persons passwords, login's and other important data required for authentication.
Replay attack	The authentication session is replayed by an attacker to fool the computer for granting the access details in a fraudulent manner.
Insider assisted attack	The system manager intentionally compromise the authentication details, thieve.
Phishing attack	Fake web pages, emails or other way of electronic communication methods which looks alike of original. They are made to get the details from user.
Masquerade attack	The attacker pretends to be authenticator on server side to user and ask him to verify his/ her authentication details falsely.
Man-in-the-middle attack	The attacker put himself/herself of middle the client and verifying server system in an authentication process. It acts as a verifier to user and to verifier as user.

B. One-time passwords

To avoid the problems linked to all time passwords one time passwords were created. These passwords are created by the server side and remain for defined time period. No user can alter or re-use it. Mostly these passwords are of number format, strings, or the combination of all [8].

C. Zero-knowledge proofs

The client will first convince the host to convince another one to allow the access without leaking any important data. The client will solve the random problems to convince that he has authenticated person. Its backdrop is that if host A is identifying the host B, it is possible that on the basis of host

A's credentials can identify the host C [15], [7].

D. Secure Shell

Secure Shell (SSH) is a protocol which provides secured login and secure networking. With SSH (version 2) every host can check on is he connected to the right server or not. The server keys are either stored on client side or may be distributes by using a key distribution protocol [10], [17].

E. Kerberos

Massachusetts Institute of Technology (MIT) has developed the authentication technique Kerberos. It has two main features: a ticket and authenticator. Ticket is used for authentication, securing data and authenticator checks whether it's the same client who was given the ticket. If user provide the right password the system can decrypt the key. Ticket granting service (TGS) expires after a duration. Backdrop of Kerberos is its scalability. The Kerberos server need to secure the keys of users and each of the TGSs [9].

F. Bio-metric authentication

Biometric authentications scheme are known to be more secured in security schemes methods. It needs the personal fingerprint, voice recognition, thumb impressions, retina recognition, palm print, face recognition. These biometric recognition scheme can be measured based on different factor and such as geometry, formation of patterns, acceptable, unique pattern, and number of false alarms. These scheme required special hardware and specific method for accurate results. It changes with time and causes main backdrop because of its non- consistency. Many research has been carried for development of these authentication proposals. Zhu. et.al. [13] proposed voiceprint template for authentication. It consists two phase: enrollment phase and the matching phase. The scheme only uses the biometric trait to authenticate. Few researcher developed the combination of more than one biometrics methods/traits to authorize like face and fingerprint, face and voice recognition, fingerprint and iris recognition. Wang et al.

[14] proposed an enterprise-based gateway combined with a multi-factor authentication for security scheme. Security gateway provides an identity to the host and begins with the single sign on method. These values are matched in credential directory and multi biometric data.

3. SURVEY ON AUTHENTICATION SCHEME IN CLOUD COMPUTING

With growth of development in software world, cloud has emerged as a most valuable thing. This lead to research in the field of security for cloud computing. In these papers we are overviewing over latest and significant research done which mainly focus on the authentication phase of cloud security. Reviewing of authentication, some new approaches are developed that can help the researchers in cloud computing.

Wang et.al. [18] Proposed a distributed scheme containing dynamic data support, with block update, delete, and append. It integrates the storage correctness insurance and data localization, i.e., the identification of misbehaving server(s). Whenever a data corruption has occurred it detects during the storage, checking the verification in the distributed servers, it identify misbehaving server(s). It is efficient for malicious attacks like for data modification, byzantine failure and server colluding attacks. This works at the middle attack and server attack but could fail at client side attack.

Bleikertz et.al [20] developed a query and policy language for the analysis to understand the configuration and provide the desired and un-desired configurations. Proposed method provides the end-user configuration of multi-tier architectures formed on infrastructure clouds. It consists the reachability and services vulnerabilities of the services. Policy language make allow to access the specification of the condition in

system after verification. It is effective at security audits, reducing vulnerabilities, AMI security and multi-tenancy.

Berger et.al [21] proposed managing security in the trusted virtual datacenter (TVDc). The proposed paper allows connection all together in different virtual machine including operating system, applications, and middleware on shared physical hardware platforms. It is formed to address the requirement for isolation and integrity accuracy which helps to enhance the security and system management in virtualized environments. It forms the trusted platform module (TPM), the virtual TPM, the IBM hypervisor security architecture (sHype) and the associated systems management software. The paper provides the facility to make datacenter visible to services carrier. Its work in a homogenous environment. It can be implemented to heterogeneous for future aspects which consists different hypervisors.

Yang et.al [22] proposed a cloud password manager using privacy-preserved biometrics where password manager addresses the security convenience dilemma. It keeps the access of different password by accessing one master password which is generated for centralizing the password storage and shifts the risk of passwords leakage from distributed service authenticated by a single master password. This master password is created by biometrics traits of the person which is more privacy-enhanced way and secure in cloud service. It is efficient to deploy and secure against the un-trusted cloud service providers.

Eldefrawy et.al [23] improved the wu et.al [3] password- based authentication scheme and maintains security features. Hash functions are used in basic blocks on password -based authentication. Wu et.al's[3] hash type password based authentication is open to theft attacks and Denial-of-service (Dos) attacks. Using the hash function obtaining the secret key which is calculated using a random password. The functions are concatenated and checks on the value. If comparison is not equivalent then authentication session fails.

Huimin Zhao et.al [24] formed a video authentication scheme with secure CS-watermark in cloud. CS-watermark data are generated from the block compressed sensing (CS) measurements which rely on the matrix used for sensing I frame's DCT coefficients. The paper shows that the CS- watermark signal has higher authentication accuracy than cloud watermarking method. It cost high computation.

Islam et.al [25] used a trust matrix using swarm intelligence in cloud computing. Trust matrix is generated using the input by user which is verified by the ant formed on three level, i.e. user, cloud data storage (CDS), cloud service provider (CSP). At each level ants keep check on the trust matrix. The authentication of user can be dropped at any level if matrix if found non-comparative [16]. It lacks at the overhead of the matrix formation.

Shilpi et.al [27] formulated a authentication scheme using Elliptic Curve Cryptography (ECC) and Elliptic Curve Diffie - Hellman (ECDH) key exchange. This method also provide the privacy to data storage access in cloud computing. The encryption of data is done at client side using a symmetric key algorithm, further key is encrypted by ECC. It is uploaded on cloud. At the time of data required to download by user the data is decrypted again by using ECC decryption method which is further decrypted the data by symmetric key. It forms a secured method for authentication and data storage privacy. It fails when a data is shared among different users and when one owner wants to share it with customized user but not for altering the data.

Yassin et.al [27] uses the biometric method to authenticate the client with the canny's edge detection. It consists the two factor, first is canny's edge detection and then symmetric encryption. It helps to authenticate providing security performing with image encryption. It provides the single as well as mutual authentication, session key agreement, defend from replay attack, impersonation attack, forgery attack, reflection attacks, and

parallel session attacks. It has lower transmutation cost with high security. Valid user can select the valid password.

Manuel et.al. [29] Proposed authentication scheme using kerberos and PERMIS (Privilege and role management infrastructure standard) for trustee and truster. It provides security as well as creates a trust in user towards the resource provider. The trust management system consists three major categories: Security Level Evaluator, Feedback Evaluator and Reputation Trust Evaluator. Each part works on their block. Security Level Evaluator is responsible for checks on different security levels in cloud computing. It further consists three next categories: Authentication type, Authorization type, and Self security competence mechanism incorporated. These parts works upon the authentication check on user which lies in security attributes repository. Feedback Evaluator performs the evaluation on feedback by user and cloud service provider. It is to ensure the dependability and to improve the performance of the resources in accordance the requirement of the user. Feedback Evaluator consists its further parts, Feedback collector which collects the feedback. Feedback verifier verifies the feedback given by the user about the service provider's. Last is Feedback updater which receives the verified feedback and updates them with time in feedback repository. Kerberos based authentication works on network authentication protocol. Kerberos provide a client-server model for mutual authentication between the user and service provider for identity checks. PERMIS authorization manager provides a policy controlled authorization system. After evaluating the trust values of all the resources, they are sorted in accordance so that the resource broker select with the higher trust value. Due to the selection of trust value improves the selection of trustworthy resource enabling the enhanced trust value. It lacks at overheads in the matrices of the trust values in the cloud/grid environment.

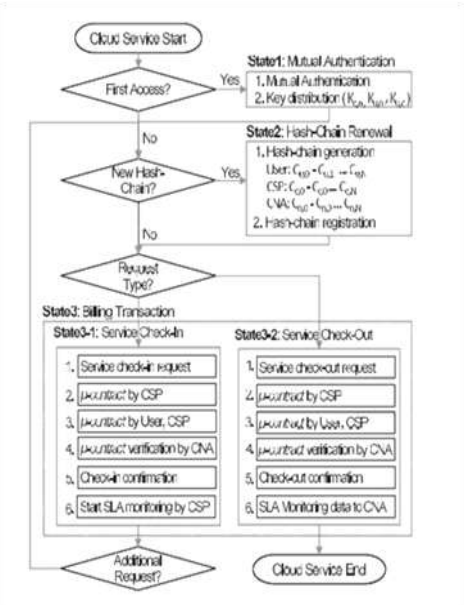

Figure 1. The proposed billing system [29]

Park et.al [30] proposed a THEMIS method for verifiable billing transaction in cloud environment. Today online transaction is done on large scale needs to be verified and authenticated. The transaction of fine-grained, mutually verifiable billing causes an overhead and computation cost high. To tackle these problem park proposed THEMIS methods, using a private key infrastructure (PKI) based digital signature. The different billing system had different approach. Some of them are Native billing systems, the consumption is based on the usage with the upfront cost. In this method the mutual verifiability and integrity required verifiable billing system which take the count on usage of cloud. Next is Security - enhanced billing systems where electronic payment systems were introduced which enhanced the security on billing mechanisms. Most the scheme are based on hash functions which uses the values. Billing transaction done by user generates a hash values in the hash chains. But these method doesn't provide any security facility for mutual verifiability of resources. Overheads is decreased by using different encryption method using the PKI method with RSA operations for the billing system while used by the user causing heavy load on resources. The THEMIS methodology consists three major categories: Cloud service provider

(CSP), Users, Cloud notary authority (CAN). PKI based billing protocol consists much more latency in billing transactions as it has a countable private and public key for all entities. This method has less overheads optimization of the storage requirements for billing system.

Squicciarini et.al [31] implemented the security to tackle the privacy problem caused due to indexing. It defines a portable data binding technique with nested JAR (Java Archives) files to get tight coupling of user's data and indexing prevention policies.

Table 2: Different Authentication Scheme Provided in Cloud Computing.

Methods/Scheme	Year	Type	Advantages	Disadvantages	Future directions
Cloud Authentication Based on Encryption of Digital Image Using Edge Detection [27]	2015	Biometric	It is robust and efficient against Phishing, security to stored data and replay attacks	Image alteration, offline image tempered is a backdrop	Image with better quality and
Security Audits of Multi-tier Virtual Infrastructures in Public Infrastructure Cloud [32]	2010	policy language and multi tier checks	Session key, Multi factor authentication increases the security level	More overheads in multi-tier architecture	Look over to strength the security levels
TVDc: Managing Security in the Trusted Virtual Datacenter [21	2008	Biometric	Rigidly-irreversible template protection use of master encrypted key and biometric method for password binding	Biometric method and binding of the key cost high	More efficient way to bind with biometric methods to encrypt the key
Cloud password manager using privacy preserved biometrics [22]	2014	Biometric	Rigidly-irreversible template protection , use of master encrypted key and biometric method for password binding	Biometric method and binding of the key cost high	More efficient way to bind with biometric methods to encrypt the key
Cryptanalysis and enhancement of a password-based authentication scheme [23]	2015	Cryptography	Use hash function to form blocks. Work against theft attacks, Dos attacks	Relatively high cost to function the hash values and storage of the multi hash	Work need to implement for the removal of its limitations.
Trust Management System for Grid and Cloud Resource [29]	2009	Multi-level Authenticator	Multi level append, delete, authenticator PERMIS Authorization strengthen the security for data	Large Overheads evaluating the matrices for the trust value	Work on overheads and strengthen the security levels.
THEMIS: Towards mutually verifiable billing transactions in the cloud computing environment [30]	2010	Cryptography	PKI method with RSA model for secure billing transactions.	More latency in billing transactions with countable private and public key entities	Work on optimization and scalability of the storage requirements
Preventing Information Leakage from Indexing in the cloud[31]	2010	Cryptography	Role based access control and use of SAML for security at service provider level for security at service provider level	Fails on the large data asset and increased computation cost	Increase the security at DDos and Dos. The clustered documents can be worked in graphs.
A Novel video Authentication Scheme with Secure CS-Watermark in Cloud[24]	2015	Biometric	Block compressed sensing measurement for the image with I frame's DCT coefficients and CS Watermark provide high security in cloud	High computation cost	Better homographic method can work with reliable biometric feature for security of cloud.
Collaborative Swarm Intelligence based trusted Computing[25]	2012	Encryption	Swarm intelligence using matrix for authentication comparison increases the security of data in cloud	Better homographic method can work with reliable biometric feature for security of cloud. Calculation of matrix increases the Overheads	Better method to compute matrix and reliable learning in swarm intelligence can be implemented

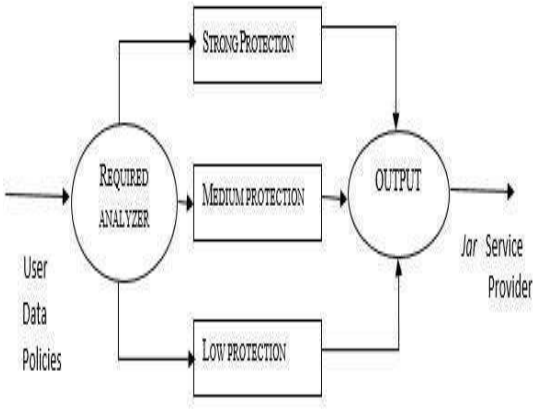

Figure. 2 Three tier Data Protection Architecture [31]

4. CONCLUSION

This paper summarizes the different authentication scheme provided in cloud computing. It provides the information of evolution of different authentications scheme. In cloud computing the authentication can be done on client side, middle of client and server, and server side. Many researches used different approached. Using encryption-decryption, image solutions, bio-metric traits, password manager etc. Different method have different cost with different computation. Every proposed model defends from different attacks but lack at some points. The researches still developing for finding new approaches and more secured authentication scheme in cloud security.

REFERENCES:

[1] Reshmi G., Rakshmy C.S., "A survey of Authentication Methods in Mobile Cloud Computing", 10th International Conference for Internet Technology and Secured Transactions (ICITST), 2015.

[2] Shikha Choski," Comparative study on Authentication Schemes for Cloud Computing", IJEDR, Vol. 2, Issue 2, 2014.

[3] H.-C. Wu, M.-S. Hwang, and C.-H. Liu, "A secure strong- password authentication protocol," Fundamental Informatics, vol. 68, no. 4, pp. 399-406,2005.

[4] S. Ziyad, S. Rehman, "Critical Review of Authentication Mechanism in cloud Computing", International Journal of Computer Science Issues (IJCSI), Vol. 11, Issue 3, 2014

[5] Antonio Celesti, Francesco Tusa, Massimo Villari and Antonio Puliafito," Security and cloud computing: InterCloud Identity Management Infrastructure", Workshops on Enabling Technologies: Infrastructure for Collaborative Enterprises, 2010.

[6] Zeeshan Javaid, Imran Ijaz, "Secure User Authentication in Cloud Computing", 5th Information and communication Technologies (ICICT), 2013.

[7] David Jablon, "Methods for Knowledge- Based Authentication", KBA Symposium, 2004.

[8] K. Ramesh S.Ramesh, "Implementing One Time Password based security mechanism for securing personal health records in cloud", Control, Instrumentation, Communication and Computational Technologies (ICCICCT), 2014.

[9] Mehdi Hojabri, K. Venkat Rao, "Innovation in Cloud Computing: Implementation of Kerberos version5 in Cloud Computing in order to enhance the security issues", Information Communication and Embedded System (ICICES), 2013.

[10] Sura Khalil Abd, S.A.R Al-Haddad, Azizol Abdullah, "A Review of Cloud Security based on Cryptographic Mechanisms", International Symposium on Biometrics and Security Technologies (ISBAST), 2014.

[11] David Fernandez-Lopez, Luis Lopez-Fernandez, Micael Gallego, Boni Garcia, Francisco Javier Lopez, "Authentication, Authorization, and Accounting in WebRTC PaaS Infrastructures, The Case of Kurento", IEEE Internet Computing, 2014.

[12] Abdul Wahid Al Abdulwahid, Natham Clarke, Ingo Stengel, Steven Furnell, Christoph Reich, "The Current Use of Authentication Technologies: An Investigation Review", Biometrics and Security Technologies (ISBAST), 2014.

[13] Hua-Hong Zhu, Qian-Hua He, "Voiceprint-Biometric Template Design and Authentication Based on Cloud Computing Security", International Conference on Cloud and Service Computing.

[14] Ping Wang, Chih-Chiang Ku, Tzu Chia Wang," A New Fingerprint Authentication Scheme Based on Secret-Splitting for Enhanced Cloud Secuirty, www.intechopen.com, 2011.

[15] Nivedita data, "Zero knowledge Password Authentication protocol", New Paradigms in Internet computing, AISC, Springer, 2013.

[16] Bakshi. K., "Cisco Cloud Computing-Data Center strategy, Architecture and solutions", Point of View White Paper for U.S. public Sector, 1st Edition

[17] T. Ylonen, "The Secure Shell (SSH) Protocol Architecture", SSH Communications Security Corp, Cisco systems, 2006.

[18] Alvaro Retana, Don Slice, Russ White, "Advanced IP Network Design", Cisco Press, 1999.

[19] Qiwei Lu, Yan Xiong, Xudong Gong, Wenchao Hung, "Secure Collaborative Outsourced Data Mining with Multi-owner in Cloud Computing", 11th International Conference on Trust, Security and Privacy in Computing and Communications, 2012.

[20] F. Omri, R. Hamila, S. Foufou, and M. Jarrraya, "Cloud-ready Biometric System for Mobile Security Access," Networked Digital Technologies, pp. 192-200, 2012.

[21] S. Berger, R. Careces, D. Pendarakis, R. Sailer, and E. Valdez., "TVDc: Managing Security in the Trusted Virtual Datacenter". ACM SIGOPS Operating Systems Review, 42(1), 2008.

[22] Bian Yang, Huigaung Chu, Guoqiang Li, Slobodan Petrovic, Christoph Busch, "Cloud password manager using privacy preserved biometrics", ieee international conference on cloud engineering, 2014.

[23] Mohamed H.Eldefrawy, Jalal F.Al-Muhtadi, "Cryptanalysis and enhancement of a password-based authentication scheme", IEEE, 7th intenration conference on cloud computing technology and science, 2015.

[24] Huimin Zaho, "A Novel video Authentication Scheme with Secure CS-Watermark in Cloud", IEEE International Conference on Multimedia Bio Data, 2015.

[25] Md. Rafiqul Islam, "Collaborative Swarm Intelligence based trusted Computing", IEEE/OSA/IAPR International Conference on Infromatics, Electronics and Vision, 2012.

[26] Shilpi Singh, "Secured User's

Authentication and private data storage access scheme in cloud computing using Elliptic Curve cryptography", 22nd International Conference on Computing for sustainable Global development (INDIA Com), 2015.

[27] Ali A.Yassin, Abullah A. Hussain, Keyan Abdul-Aziz Mutlaq, "Cloud Authentication Based on Encryption of Digital Image Using Edge Detection", International Symposium on Artificial Intelligence and signal Processing (AISP), 2015.

[28] J. Clerk Maxwell, "A Treatise on Electricity and Magnetism", 3rd ed., vol. 2. Oxford: Clarendon, 1892, pp. 68–73.

[29] Paul D Manuel, S. Thamarai Selvi, Mostafa Ibrahim Abd-El Barr, "Trust Management System for Grid and Cloud Resources" Research Grant by Kuwait University, IEEE, 2009.