ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 11, November 2016

A Survey of Authentication Methods in Cloud Computing

Ankita Yadav[1], Nagendra Kumar[2]

M.Tech Student, Dept. of CSE, SRIST, JBP, India.[1]

Assistant Professor, Dept. of CSE, SRIST, JBP, India.[2]

ABSTRACT: Cloud Computing is a transpire technology which attempts to combine the storage and processing resources of cloud environment with the dynamicity and accessibility of cloud resources. Cloud computing is a newfound service which has a rapid growth in IT industry recent years. Despite it has a huge contribution to the development of the technology and society, the cloud still exists some security deficiencies to block its development such as data leakage, illegal access and privacy risks. Hence, access control and user authentication is very important in cloud environment. Some related access control schemes has been proposed to solve the security problems in cloud, however, the high computation cost is a crucial factor in practical use. In this paper we propose a novel lightweight identity authentication based access control scheme for cloud.Security, mainly authentication, is fast evolving as a focal area in cloud computing research. We propose a offbeat classification system for existing authentication methods in cloud computing. Further, the pros and cons of the various methods are discussed. We present an analogously analysis and recommends future research in improving the surveyed implicit authentication in Cloud Computing.

KEYWORDS: cloud computing, security, user authentication.

I. INTRODUCTION

Ever since its genesis, cloud computing has been revolutionizing the way data storage and processing mechanisms are envisioned and implemented. It enabled the on-demand availability of services such as Software, Platform, Infrastructure (through SaaS, PaaS, IaaS respectively) and thus formed an economic solution to meet the ever-fluctuating demand for storage and computational resources by growing businesses. Cloud computing as a business paradigm has gone a long way from the early innovations of Salesforce.com and Amazon web services [**1**]. Today, in 2016, a whopping $32 billion is calculated to be spent on cloud IT infrastructure per year, according to International Data Corporation, the market intelligence firm [**2**]. This accounts for 33 percentage of the total IT infrastructure spending. Further, cloud infrastructure spending is expected to reach $52 billion in 2019 which is 43 percentage of the total IT expenditure.The cloud is responsible for providing real time services such as storing the data, giving application and processing the data for consumers through the internet. The consumers can remotely store their data into the cloud and can enjoy the scalable services pay-on-demand [**3**]. As an emerging technology, it holds great potential albeit with its fair share of issues, perhaps the most prominent among which is ensuring security and privacy. As in traditional paradigms, authentication plays a major role in security in cloud computing. User authentication is an important scheme to ensure only the authorized users can access the server. This paper summarizes the existing authentication methods in CC, presents a classification system for the various methods and point out the advantages and disadvantages of each.

II. SECURITY IN CLOUD COMPUTING

Nowadays, cyber warfare is arguably the most complex challenge in a distributed and multi- tenant environment. It is a complex job within the client-server architecture. When the data transfer to the cloud services, the requirements of security should be the most important. The European Network Information Security Agency (ENISA) enumerated the risks, recommendations and benefits for cloud computing [**4**]. It also lists the infection on confidential document, loss of governance, malicious insider, and insecure incomplete data. The Elastica 2015 shadow data report [**5**] it focuses on

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 11, November 2016

unauthorized apps discovered in an organization. It examines which type of data typically found in sharing apps, riskiest exposure, and what steps take to mitigate these security problems.
In this section, we briefly introduce about the major security concerns of cloud computing.

- *Software security:* It provides basic idea of software security come from the engineering software department that it continues to function correctly under the malicious activities. To build a cloud environment a central and critical problem is software security problem. It defects with security including implementation bugs, buffer overflow, designed flaws, error handling promises and much more [**6**].
- *Infrastructure security:* The most common and fundamental challenges is to demonstrate that the virtual and physical infrastructure of the cloud can be trusted. The attestation of the third party is not enough for the critical business process. It's absolutely essential for the organization to be able to verify business requirements that the underlying infrastructure is secure.
- *Storage security:* In cloud storage system, end user stores the data in the cloud and no longer owns the data and where it's stored. This always has been an important aspect of quality of service. It ensures the correctness of user's data in the cloud and by utilizing homomorphism token with distributed verification of erasure-coded data [**7**].

- *Network security:* In cloud computing, communication is via the internet and it is the backbone of the cloud environment. Network security concerns about both internal and external attacks. These attacks in the network can either occur in the virtual or physical network. Hanqian W., et al. [**8**] focuses on the virtual network in a Xen platform by discussing and analysing its security problems.

III. TRADITIONAL AUTHENTICATION IN CLOUD COMPUTING

Authentication is one of the key aspects of any security system. An authentication service is the ever-vigilant guard at the gateway to the digital fortress; its responsibility is to check the identity of any party seeking entrance (i.e., access) to the system; it verifies certain credentials to ensure that an entity is indeed what it claims itself to be. Authentication is used for establishing confidence in users and also is a brilliant way for finding access to stored data.
Assurance levels of authentication should be as per the sensitivity of application, the information assets accessed and the risk involved.
In Table 1, we present a comparison of traditional authentication mechanisms with advantages and disadvantages.

Mechanism	**Idea**	**Advantages**	**Disadvantages**
User ID/ Password	Pre-registered username and secret password	Simple, popular, easy-to-deploy	Must be renewed frequently
Public Key Infrastructure	Trusted Certificate authority issues private keys	No sharing of secret key	Single point of trust; challenges in scalability
Kerberos	Trusted authority issues tickets	Mutual authentication between client and server	Single point of failure; requires Time synchronization
Single Sign-On	One step authentication to multiple applications	User friendly	Any breach in sign-in security affects multiple applications
One Time Password	PIN typically used in multi-factor authentication	Easy-to-use; Compatible with password based authentication	Secure generation and transmission of OTP is challenging
Mobile Trusted Module	Chip for hardware authentication	Optimized for mobile devices; small footprint	Deployment and management is challenging

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 11, November 2016

IV. RELATED WORK

This survey **encompasses** most of the major authentication schemes proposed in cloud computing so far. We briefly discuss the principles behind each authentication method. Further, based on the authentication criteria, we propose a classification scheme for the surveyed methods. A comparative analysis of the methods, highlighting the advantages, disadvantages, implementation stage and future research possibilities is given next.
The surveyed authentication methods for cloud computing scenario can be broadly classified as follows:

1. User profile Based methods
2. Cryptographic and Hashed methods
3. Image-based methods
4. Port-knocking methods

A. USER PROFILE METHODS

These methods make use of information about the user for identification. Here, 'user' is a generic term; it can mean either the person using the mobile device or the device itself. Typically, user behavioural patterns, biometrics, location information etc. are gathered during a registration phase and verified later for authenticated logins.

Biometrics-based schemes form a major chunk of the user profile methods. Rassan et al. discusses fingerprinting as a possible authentication method in [9]. The paper briefly discusses similar user authentication methods using handwriting [10], a quick response code based on user's image [11] and proceeds to the design and implementation of the proposed method.

Keystroke authentication is a behavioural biometric feature which has been recently discussed as an authentication parameter [13]. Babaeizadeh et al. in [4] presents a method to authenticate users in mobile cloud environment using keystroke pattern. Among the various parameters associated with keystroke biometrics, keystroke duration is chosen as the authentication base in this method. At a successful user registration, the keystroke duration is stored in a database. A tolerance limit for the duration is set.

B. CRYPTOGRAPHIC METHODS

Cryptographic methods have been traditionally used for user authentication in various computing platforms. There are several similar methods proposed for mobile cloud computing scenarios too. They typically involve exchange of keys or establishment of tickets with a trusted third party and use the same for establishment of identity. Shelke and Soni describe an enhanced authentication scheme based on Kerberos in [5]. Meshach and Babu [6] discuss some authentication tools such as signature tokens, Open ID etc. This scheme needs a Certificate Authority as in Public Key Infrastructure. Participants are issued certificates signed with a public key, so that the certificates and hence the identity of the party can be verified (through the signatures). Zhang et al. discussed the idea of elastic devices in [7] which are consumer electronic devices attempting to overcome the resource limits by integration with cloud resources.

C. IMAGE-BASED METHODS

Schwab and Yang proposes a novel authentication scheme for cloud computing entities in [8]. This system integrates certain techniques such as fuzzy vault, picture authentication and zero-knowledge authentication. Fingerprint, retinal scanning and facial recognition systems are some of the most advanced security systems in the world. Since no two people's fingerprints are the same, not even identical twins (who share exactly the same genes) (28, Plants), fingerprints are one of the best biometric authenticators to use as a password for protected systems. Unfortunately, the installation of fingerprint scanners is not always applicable to Internet applications. The same issues apply to retinal scanning and facial recognition systems.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 11, November 2016

D. PORT-KNOCKING METHODS

In port-knocking authentication method, the client sends no-reply synchronization packets (SYN) to the closed ports of the server firewall. The sequence of ports to which the packets are sent can be selected statically or dynamically. This sequence is logged by the server and is a secret key which, when validated opens the appropriate server (and corresponding service) for the port-knocker client. Reference [8] presents a comprehensive survey of the port-knocking authentication methods which authenticate the user by sending packets to the sequential ports of server. The discussed methods are compared based on the platforms, protocols, and existence of third party dependency.

Table II summarizes and compares the surveyed methods for authentication, highlighting the advantages, disadvantages and implementation stage of each. In most of the works, the authors have sketched out the likely direction of future research.

Authors	Paper	Key-points	Limitations
Abderrahim Abdellaouia,*, Younes Idrissi Khamlichib, Habiba Chaouia, Procedia Computer Science 85 (2016) [10].	A Novel Strong Password Generator for Improving Cloud Authentication	One-time Password and SHA1.	Pass Generator apps such as (Smartphone, PDA, Tablet) is required. Image Pass has to be changed manually.
Thabet Kacem, Duminda Wijesekera, Paulo Costa 2015 IEEE [11]	Integrity and Authenticity of ADS-B Broadcasts	Key management Schema for authentication and rely on a keyed (HMAC) for integrity.	128-bit HMAC Digest ,Expensive Equipment
Dindayal Mahto, Dilip Kumar Yadav, 2015 IEEE [12]	Enhancing Security of One-Time Password using ECC with Biometrics for E-Commerce Applications	ECC with palm Bio-Metrics. Hash value is generated by using MD5.	Palm vein recognition device required. Implementation is expensive.
Vikash Mainanwal[1], Mansi Gupta[2], Shravan Kumar Upadhayay, 2015 IEEE[13]	Zero knowledge protocol with RSA Cryptography Algorithm for Authentication in Web Browser Login System	RSA cryptography, OTP is generated plain text.	Complexity is not best as compare to ECC. Plain text OTP is not secure.
Jian Shen1,2,3, Dengzhi Liu3, Shaohua Chang3, Jun Shen3, Debiao He, 2015 IEEE[14]	A Lightweight Mutual Authentication Scheme for User and Server in Cloud	one-way hash functions, string concatenation and XOR operations, the authorized agency will check its legitimacy	Involved Third party authentication. Data is not Encrypted in transmission.
Kawser Wazed Nafi1,2, Tonny Shekha Kar2, Sayed Anisul Hoque3, Dr. M. M. A Hashem, (IJACSA)-2012.[15]	A User Authentication, File encryption and Distributed Server Based Cloud Computingsecurity architecture	AES based file encryption system onetime password system for user authentication process	MD5 hashing method is used.OTP is not encrypted.
Akashdeep Bhardwaja, GVB Subrahmanyamb, Vijay Avasthic, Hanumat Sastry, Elsevier B.V. 2016 [16]	Security Algorithms for Cloud Computing	Compared all the Encryption Techniques and review Symmetric and Asymmetric algorithms	DES and SHA-256 is used to secure cloud data.
Lt. Col. Jatinder Paul Singh1, Dr. Mamta2 and Sunil Kumar3, 2015 IEEE [17].	Authentication and Encryption in Cloud Computing	An image set will be provided to users. Digital signature is used for generation of OTP for authentication.	Numeric values are assigned to user name and password which is easy foe Brute –force-attack.
Ali A.Yassin*, Abdullah A. Hussain, Keyan Abdul-Aziz Mutlaq, 2015 IEEE [18].	Cloud Authentication Based on Encryption of Digital Image Using Edge Detection	used image partial encryption, the edge pixels of image are encrypted using the stream cipher	The disadvantage of merging the above schemes will causes to increase the key space of digital images and suffers from resisting the extensive attack

V. CONCLUSION

The hype of cloud paradigm is changing the IT industry; it brings many benefits to companies, organizations and even countries. Despite bringing several advantages, the cloud still is vulnerable to many security challenges. This is why

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 11, November 2016

security is the major challenge in the adoption of the cloud. The customer and vendors are well aware of security threats. This research attempted to show various security challenges, vulnerabilities, attacks and threats that hamper the adoption of cloud computing. Our paper provided a state-of–art survey on cloud security issues and challenges that arise from unique characteristics of the cloud like the sharing and virtualization of resources, resource pooling and the public nature of the cloud. We explored various cloud services and what they provide as well as analyzed the security concern on each provider.

REFERENCES

[1] S. Marston, Z. Li, S. Bandyopadhyay, J. Zhang, and A. Ghalsasi, "Cloud computing – The business perspective," Decision Support Systems, Volume 51, Issue 1, pp. 529-551, April 2011.
[2] International Data Corporation (IDC) Worldwide Quarterly Cloud IT Infrastructure Tracker, "Worldwide Cloud IT Infrastructure Market Growth Expected to Accelerate to 21% in 2015, Driven by Public Cloud Datacenter Expansion, According to IDC," Press Release, 21 April 2015.
[3] K. Ren, C. Wang , and Q. Wang, "Security Challenges for the Public Cloud", IEEE Internet Computing, vol. 16, no. 1, 2012.
[4] Juraj Somorovsky, Mario Heiderich, Meiko Jensen, Jörg Schwenk, Nils Gruschka, Luigi Lo Iacono, "All your clouds are belong to us: security analysis of cloud management interfaces", The 3rd ACM workshop on Cloud computing security workshop in Proceedings of, ACM, pp. 3-14. 2011.
[5] Zhaolong Gou, Shingo Yamaguchi, B. B. Gupta. "Analysis of Various Security Issues and Challenges in Cloud Computing Environment: A Survey", In Handbook of Research on Modern Cryptographic Solutions for Computer and Cyber Security, IGI Global, pp. 393-419. 2016.
[6] Dawei Sun, Guiran Chang, Lina Sun, Xingwei Wang, "Surveying and analysing security, privacy and trust issues in cloud computing environments,"Procedia Engineering, Vol. 15, pp. 2852-2856, 2011.
[7] Nguyen, Thanh Cuong, Wenfeng Shen, Zhaokai Luo, Zhou Lei, and Weimin Xu. "Novel Data Integrity Verification Schemes in Cloud Storage." In Computer and Information Science, Springer International Publishing, pp.115-125, 2015.
[8] Wu, Hanqian, Yi Ding, Chuck Winer, Li Yao. "Network security for virtual machine in cloud computing." IEEE Conference in Computer Sciences and Convergence Information Technology (ICCIT), 2010 5th International Conference on, pp. 18-21, 2010.
[9] I. Rassan, and H. Shaher, "Securing Mobile Cloud Using Finger Print Authentication", International Journal of Network Security & Its Applications (IJNSA), vol. 5, no. 6, pp.41-53, 2013.
[10] Abderrahim Abdellaouia,*, Younes Idrissi Khamlichib, Habiba Chaouia," A Novel Strong Password Generator for Improving Cloud Authentication" Procedia Computer Science 85 (2016).
[11] Thabet Kacem, Duminda Wijesekera, "Integrity and Authenticity of ADS-B Broadcasts "Paulo Costa IEEE,2015.
[12] Dindayal Mahto, Dilip Kumar Yadav, "Enhancing Security of One-Time Password using Elliptic Curve Cryptography with Biometrics for E-Commerce Applications" IEEE,2015.
[13] Vikash Mainanwal[1], Mansi Gupta[2], Shravan Kumar Upadhayay, "Zero knowledge protocol with RSA Cryptography Algorithm for Authentication in Web Browser Login System"IEEE, 2015.
[14] M Jian Shen1, Dengzhi Liu2, Shaohua Chang3, Jun Shen4, Debiao He," A Lightweight Mutual Authentication Scheme for User and Server in Cloud" IEEE, 2015.
[15] F. Kawser Wazed Nafi1, Tonny Shekha Kar2, Sayed Anisul Hoque3, Dr. M. M. A Hashem," A Newer User Authentication, File encryption and Distributed Server Based Cloud Computing security architecture" (IJACSA)-2012.
[16] Akashdeep Bhardwaja, GVB Subrahmanyamb, Vinay Avasthic, Hanumat Sastry, the Authors." Security Algorithms for Cloud Computing" Published by Elsevier B.V. 2016.
[17] Lt. Col. Jatinder Paul Singh1, Dr. Mamta2 and Sunil Kumar3," Authentication and Encryption in Cloud Computing" IEEE,2015.
[18] Ali A.Yassin*, Abdullah A. Hussain, Keyan Abdul-Aziz Mutlaq," Cloud Authentication Based on Encryption of Digital Image Using Edge Detection" IEEE, 2015.

BIOGRAPHY

Ankita Yadav is a Research Scholar in the Computer Science Department, Shri Ram Institute of Science & Technology, Jabalpur -M.P.