Current Trends in Technology and Science
ISSN: 2279-0535. Volume: VII, Issue: II

Comprehensive Analysis of Various Authentication Techniques to Enhance the Security of Cloud Environment

*Manreet Sohal
Research Scholar, Department of Computer Engineering and Technology, Guru Nanak Dev University, Amritsar,India
manreet.cetrsh@gndu.ac.in

Sandeep Sharma
Professor, Department of Computer Engineering and Technology, Guru Nanak Dev University, Amritsar,India
sandeep.cse@gndu.ac.in

Abstract — Cloud computing is overpowering the means by which data storage, transmission and execution are altering. But while exploiting services of the cloud, there are enormous security concerns. Among this authentication of the cloud user is the greatest security roadblock for cloud computing. Authentication is an incredible part of data security that can be used to prevent unauthorized users to penetrate into the cloud environment. There are many types of authentication schemes available for cloud environment. Several research works have been done on these schemes to formulate new and enhanced authentication techniques that provide greater security for the data stored on the cloud. In this paper several such authentication techniques have been studied and evaluated. A comparative analysis has been done to figure out the contributions of these techniques towards cloud security and privacy. Besides this the shortcomings of these existing techniques have also been enlisted so that they can be focused for research in the future to enhance the security of the data.

Keyword — Cloud Computing, Authentication, Security, Privacy, Access Control.

1. INTRODUCTION

With the cloud computing being adopted extensively, the industries have started focusing on scaling up with minimal requirements. Industries have started to recognize the influences of shared environments on the efficiencies and savings. But along with these abilities come the security and privacy concerns which are still the major stumbling blocks in the way of cloud computing. Therefore, discovering stout cloud security solutions have become a major area for research.

Cloud computing is vulnerable to various security threats such as denial of service attacks, distributed denial of service attacks, eavesdropping etc [2]. To uphold cloud standards and to provide quality of service, various steps are required to be bothered. Mostly the cloud stores extremely sensitive data like data of social networks, banking operations and medical records and release this data on demand when the users make request. The user must prove his/her authentication before trying to access the data stored on the cloud. Besides this, the user must make sure that the outsourced data is not being tampered by the cloud [1]. But, while managing a vast amount of data, the chances of security breaches are very high. Therefore, a stout security access mechanism should be created in order to maintain the security of data and the trustworthiness of the data owner. Cloud storage authorizes a vast number of users with different roles and access rights for storing and sharing their data [2]

In the Cloud, a large number of users share the data in a communal behavior. For example, a lecturer may allow his colleagues and students to access and share the files stored in the cloud. These files can be personal information of students, their attendance, notes, internal assessments, research related files etc. The students and the coworkers make request to gain access to the cloud and they receive appropriate information according to their authorization and access rights. For each user an identity is generated and each time the user desires to access the data on the cloud, he has to verify his identity which can be validated or rejected according to its legitimacy. Every time an authentication is carried out, the service provider has to believe in the identity presented by the user. However this system is serious with regard to the data protection as the control of the service depends on the outcomes of authentication [2]. If the authentication is weak, then it can wreck the security of the service which is dependent on it and there is also a danger of impersonation [2]. On the other hand, the security and privacy threats may occur due to the outside users and the cloud servers that cannot be fully trusted by the data owners. So, in these cases proper authentication and access control mechanisms have to be implemented to safeguard the outsourced data.

The remainder of this paper is arranged as follows: In Section two, types of authentications present is cloud computing have been explained. In Section three, various types of authentication techniques present in literature have been detailed out. Comparative analysis of these techniques has been done in the fourth section. Finally, section 5 contains the conclusions.

2. TYPES OF AUTHENTICATION IN CLOUD ENVIRONMENT

The user authentication is a significant factor in cloud environment as it ensures that the entity which is trying to communicate is the one it claims to be. There are several methods of authentication available in cloud computing which are going to be discussed in detail in this section.

2.1. Username and Password Authentication

In this method of authentication, confidentiality and privacy can be sustained up to some stage. For the users to gain access to the information stored on the cloud, they are entailed to enter the username and password to the system. It has been scrutinized that this authentication scheme does not succeed in offering an advanced and reliable security since it is difficult to make sure whether the requesting user is authorized or not. Moreover, this method is very prone to dictionary and brute force attacks [1]. Due to the input controls in cloud computing environment, the users cannot use complex passwords which lead to the usage of easy and short passwords. In addition to this, the users reuse their passwords so that they can be recognized in numerous servers which further weaken the security of user's information. The security provided by this method depends upon the length of the chosen password.

2.2. Multifactor Authentication

To provide advanced security to the information stored in cloud computing environment, a amalgamation of different authentication schemes is required to be done. This combination is known as Multifactor Authentication. This technique provides higher security and confidentiality as it not only requires the validation of the username and password but also requires additional factors or some other form of authentication [1]. It is considered to be a strong authentication method. In fact, the prospect of authenticity climbs up exponentially with the inclusion of additional factors in the confirmation process.

2.3. Mobile Trusted Module

Trusted Computing Group (TCG) brought in a set of constraints to store, evaluate and report software and hardware integrity by using a hardware root-of-trust, known as the Mobile Trusted Module (MTM) and Trusted Platform Module (TPM)[1]. As Trusted Platform Module (TPM) is used for PCs, MTM is a security feature provides work for mobile devices.MTM guarantees the integrity and reliability of a mobile platform.

2.4. Single Sign-On

The SSO is a technique by which numerous autonomous software systems can be accessed by logging in a system only once without any need to re-login in every application. This course of action holds up the users for accessing various applications and lessens the risks for the supervisors to aid the users practically [1]. By using this technique the efficiency of the users is enhanced as the users are not required to commemorate various passwords [1].

2.5. Public key Infrastructure

The conventional authentication design is founded on the basis of secret key and primarily supports the position of conventional asymmetric cryptographic algorithms, for example, RSA. In order to verify user's identity a private key is used. Secure Electronic Transaction (SET) and Secure Socket Layer (SSL/TLS) has been designed using PKI for authentication [1]. PKI system has to guarantee integrity and confidentiality of data, non-repudiation, strong authentication, in addition to authorization. In distributed environments similar to cloud computing , mobile cloud computing and wireless sensor networks PKI has a major contribution in ensuring security and authentication of users.

2.6. Biometric Authentication

It is the method of authenticating whether the user is whom he is claiming to be [1]. Biometric authentication supports three significant aspects of information security. These aspects incorporate identification, authentication and non-repudiation. This scheme involves recognizing the behavioral and physiological characteristics of an individual. It is a very strong authentication scheme as if provides biological attestation of what we are and what is we know. Biometric authentication can be categorized into two types: behavioral and physiological [1]. The behavior biometric deals with the behavior of the users and involves signatures, keystrokes and voice prints. On the other hand, Physiological biometric deals with the physical traits of the individuals and its involves fingerprints, palm prints, retina etc.

3. AUTHENTICATION TECHNIQUES

Till date lots of work has been done on authentication of user wanting to gain access to the cloud. In this section twelve enhanced cloud authentication techniques from $\mathbf{T_1}$ to $\mathbf{T_{12}}$ have been explained and analyzed. These techniques involve advanced versions of different types of authentications which have been discussed in the previous section. These techniques provide a strong authentication for the users who want to access the data stored on the cloud and prevent unauthorized access to the cloud.

T_1: Privacy preserving multi factor authentication using trust management [2]-In this technique, the authors have given a proposal for safeguarding the privacy of the system by offering multifactor authentication excluding any supplementary physical tool, in case of big data used in cloud system [2]. In this technique, the client machine is identified by making use of trust model. Trust is calculated according to the client machine and the reduction of user process will take place from multifactor to single factor. Further, the performance evaluation of the system depicted an optimum false positive rate and average resource utilization.

T_2: Anonymous RFID authentication for cloud services [3]- This technique, includes authentication procedures that are anonymous and forward secure . The RFID technique for cloud services have been used to design this system. In this system, the data owners cannot be traced from the previous acts of authentication even though the private keys are leaked from the sullied tags. The protocol has been implemented in 2 steps. In first step, RFID protocol based on Homomorphic Encryption has been proposed but it does not offer tag revocation. Then the second version is presented which provides tag revocation. The proposed system provides anonymity, authentication, unlinkability and privacy.

T_3: Kerberos: secure single sign-on authentication protocol framework for cloud access control [4]- This is a cloud based authentication system which works as third party between users and cloud servers to permit secure access to the cloud. It offers single sign-on and

thwarts DDOS attacks [4]. The proposed model is based upon Kerberos V5authentication protocol which offers access control based on roles. This System filters the unauthorized access and offers reduction in computational overheads and memory usage of the cloud which is involved in performing authentication checks for every user. Since the proposed system makes use of a standard symmetric key encryption algorithm, it is possible to do all types of encryption with it. In the proposed technique a variable block cipher is used along with cipher block chaining mode therefore no trespasser can attack the system off-line.

T_4: Cost-effective authentic and anonymous data sharing with forward security [5]- This technique is the enhanced version of ID-based ring security by introducing forward security. The proposed system offers absolute anonymity and has been proved to be forward-secure in the random oracle model. With this technique, all the signatures that were created earlier still stay valid, even if the private key of any user gets hacked. This feature is particularly beneficial for significant data sharing system, since it is impractical to re-authenticate all the users when the private key of only a single user has been corrupted. The proposed technique is quite efficient and does not involve any pairing operations. This system is very practical in case of applications related to authentication and user privacy like e-commerce, ad-hoc network etc.

T_5: Trusted framework for online banking in public cloud using multi-factor authentication and privacy protection gateway [6]- This is a multifactor authentication technique based on biometric fingerprints. This scheme offers a highly protected identity confirmation process for legitimating the remote users. The framework is specially designed for online banking. In this approach, the authentication details of the users have not been exposed to the bank and the cloud servers. The framework has been extended to build up a privacy protection gateway using tokenization and methods of data anonymization. The experimental results show that the proposed method is highly effective and practical and the performance has been improved.

T_6: Two-channel user authentication by using USB on Cloud [7] – It is a new USB authentication for vulnerable cloud environment. In this approach, the users are authenticated using passwords with USB. An individual generic multifactor authentication has been developed which can correctly authenticate the clients even when the remote server is down. The authors assert that the proposed scheme provides both availability as well as security**.**

T_7: SUAS: Scalable User Authentication Scheme for Secure Accessing to Cloud-Based Environments [8] - It is a new method of authentication by which the performance of user authentication is enhanced and the rate of scalability in cloud environments is improved. Cryptography, agents and key exchange schemes have been used in the proposed method. The authors have used three agents, first user authentication agent, second user authentication agent and the key manager agent [8]. These three agents enhance the efficiency by dividing user authentication and key management into various components. The end results state that the proposed model is highly advantageous to be used in cloud environments as it enhance the reliability, efficiency and scalability of cloud computing.

T_8: Data Security in Cloud Architecture Based on Diffie Hellman and Elliptical Curve Cryptography [9] - This is a new framework which is based upon exponential cryptography, that encrypts the data and linear cryptography, that builds up a secure connection. In order to guarantee user authenticity, the authors have come forward with four-step methods. In the first step connection is established, in the second step account is created, in the third step authentication is checked and in the final step data exchange is done. It has been claimed that the technique presented in this paper has lower computational cost and the time complexity is exponential due to which it cannot be cracked easily.

T_9: A Multi-Token Authorization Strategy for Secure Mobile Cloud Computing [10]- The authors have studied a version of identity management system (IDM) called OAuth and have identified many flaws in this model. Two major shortcomings have been recognized. The first weakness is that the hackers can easily authorize themselves as this model has malicious code. Secondly in this model, the authorization token travels across the communication links between the users, clouds and identity management systems. The authors have carried out experiments to provide solution for these problems. The proposed technique laid emphasis on the distribution of authorization token between IDMs and the cloud. The authors claim that their method lowers the chances of hacking a token leading to increased security of resources in cloud environment.

T_{10}: Biometric Authentication in Cloud Computing [11]- This paper analyze various biometric authentication techniques and have come up with the conclusion that all of the studied techniques have a lot of flaws. The authors have suggested that the solution to these weaknesses is to follow multi model authentication in which two or more biometric techniques can be clubbed.

T_{11}: Secure Storage and Access of Data in Cloud Computing [12]- This is a new approach by which users can securely save and access their data from the cloud. The ECC technique has been used for protecting the data. The cloud server is divided into two parts, the shared regions and the private regions which lead in the improvement of performance. The authors ensure that with the proposed model the problem of sharing data among groups would be solved using shared section.

T_{12}: Trust Management Approach for Secure and Privacy Data Access in Cloud Computing [13] - It is a new framework which offers trust to the cloud users. It is based on enhanced version of CIA framework. The mechanism for auditing has been presented and logs have been maintained and sent sporadically to the data owner in order to grant trust for cloud users [13]. The jar files of the data have been encoded using base64 encoding algorithm to prevent attacks on data.

4. Comparative Analysis of various authentication techniques

In this section the various authentication techniques which have been discussed in the previous section are analyzed on the basis of type of authentication scheme used by it and what are the contributions of the technique in enhancing the security of the cloud environment. Further the weaker sides these techniques have also been highlighted. Table 1 depicts the type of authentication used in these techniques and Table 2 highlights the strengths and weaknesses of these techniques.

Table (1) Types of authentication scheme used

Technique	Type of Authentication Used					
	Username & Password Authentication	Multifactor Authentication	Mobile Trusted Module	Public key infrastructure	Single-sign On	Biometric Authentication
T_1	×	✓	✓	×	✓	✓
T_2	×	×	×	✓	×	×
T_3	×	×	×	×	✓	×
T_4	×	×	×	✓	×	×
T_5	×	✓	×	×	✓	✓
T_6	×	✓	×	✓	✓	×
T_7	×	×	×	✓	×	×
T_8	×	×	×	✓	×	×
T_9	×	×	×	✓	×	×
T_{10}	×	×	×	×	×	✓
T_{11}	×	×	×	✓	×	×
T_{12}	×	×	✓	×	×	×

Table (2) Pros and cons of various authentication techniques

Technique	Publication	Advantages	Disadvantages
T_1	Anakath et al. (2017)	• Privacy Preservation • Optimum False Positive rate	• Average resource utilization
T_2	Bingol et al.(2015)	• Provides anonymous and mutual authentication • Active RFID tags are used to reader without revealing their identity • Ability to identify and track malicious users.	• No Support for tag removal
T_3	Dubai et al. (2014)	• Provides Role based access control • Authenticate users to access applications on the server • Prevents DDOS attacks	• Works only for single owner scenarios
T_4	Huang et al. (2015)	• Provides Forward Security • Offers anonymity • Provides Mutual Authentication	• Can only be Proved in random Oracle model and not in standard model
T_5	Nagaraju et al. (2015)	• Provides an effective privacy protection gateway • Offers highly secure Identity verification	• Non-generic framework

T_6	Hong (2015)	• Low Computation Overheads • Lower communication costs • Provides security and availability	• Low efficiency as compared to other algorithms
T_7	Moghaddam et al. (2014)	• offers scalability • increased efficiency and reliability • Multiple intermediates decrease the dependency on the main cloud	• Needs manger's keys • if the server goes down , keys used for authentication cannot be accessed.
T_8	Tirthani et al (2013)	• Provides secure connection • Difficult to crack • Lower computational Cost	• Greater time delays due to complexity
T_9	Ahmad et al. (2014)	• Lowered chances of token getting hacked • Greater Security	• One of the links carry complete distributed token and therefore is vulnerable to hacking
T_{10}	Batool et al. (2015)	• Validates if the user is the one which he claims to be • Non-repudiation • Identification	• Difficult to implement on large scale • Higher cost requirements
T_{11}	Kumar et al. (2012)	• Enhanced security by implementing proper access controls. • Greater efficiency than other ECC based techniques	• One to many and many to one communication is not supported.
T_{12}	Mythili et al. (2013)	• Provides greater security	• High processing overheads.

5. CONCLUSIONS

The User's data is the most precious asset in cloud computing. Therefore protecting user's data is very critical aspect of data security as the cloud will almost lose its significance if data security is not assured by it. Authentication is one of the major security hurdles which is being faced by cloud environments nowadays. In this paper various techniques of user authentication in cloud environment have been discussed and analyzed. Authenticating cloud users is gaining more attention. There are numerous techniques that have been proposed in literature, we have explained some of those techniques in our paper. After conducting this review we have come to the conclusions that the all these techniques are prone to some or the other flaws. So lots of work is still required to be done in this field. Therefore, the findings of this paper can be used to develop a new authentication scheme which can overcome the shortcomings of the existing techniques.

REFERENCE

[1] Huma Farooq, "A Review on Cloud Computing Security Using Authentication Techniques", International Journal on Advanced Research in Computer Science, Vol. 8, No.8, pp. 19-22, March, 2017.

[2] A.S. Anakath, S. Rajkumar, S. Ambika, "Privacy preserving multi factor authentication using trust management", Cluster Computing, pp. 1-7, September 2017.

[3] Muhammed Ali Bingol, Fatih Birinci, S uleyman Kardas, Mehmet Sabir Kiraz, "Anonymous RFID authentication for cloud services", International journal of information security science, Vol.1, No.2, pp. 32-42, 2012.

[4] Yaser Fuad, Al-Dubai, "Kerberos: secure single sign-on authentication protocol framework for cloud access control", Global Journal of Computer Science and Technology, Vol.14, No.1, 2014.

[5] Xinyi Huang, Joseph K. Liu, Shaohua Tang, Yang Xiang, Kaitai Liang, Li Xu, Jianying Zhou, "Cost-effective authentic and anonymous data sharing with forward security", IEEE Transactions on computers, Vol.64, No.4, pp. 971-983, April 2014.

[6] Sabout Nagaraju, Latha Parthiban, "Trusted framework for online banking in public cloud using multi-factor authentication and privacy protection gateway", Journal of Cloud Computing, Vol.4, No.22, December 2015.

[7] Sunghyuck Hong, "Two-channel user authentication by using USB on Cloud", Journal of Computer Virology and Hacking Techniques, Vol.12, No.3, pp. 137- 143, November 2015.

[8] Faraz Fatemi Moghaddam, Rama Roshan Ravan, Touraj Khodadadi, Yashar Javadianasl, Abbasali Halalzadeh, "SUAS: Scalable user authentication scheme for secure accessing to cloud-based environments", In: IEEE Symposium on Computer Applications and Industrial Electronics, Vol. pp. 33-38, January 2015.

[9] Neha Tirthani, Ganesan R, "Data Security in Cloud Architecture Based on Diffie Hellman and Elliptical

Curve Cryptography", IACR Cryptology ePrint Archive, 2014.
[10] Azeem Ahmad, Muhammad Mustafa Hassan, Abdul Aziz, "A multi-token authorization strategy for secure mobile cloud computing.", In: 2nd IEEE International Conference Mobile Cloud Computing, Services, and Engineering (MobileCloud), pp. 136-141, June 2014.
[11] Rakhshanda Batool, Ghazal Naveed, Abdulhaq Khan, "Biometric Authentication in Cloud Computing", International Journal of Computer Applications, Vol.129, No.11, pp. 6-9, November 2015.
[12] Arjun Kumar, Byung Gook Lee, HoonJae Lee, Anu Kumari, "Secure storage and access of data in cloud computing",In: IEEE International Conference on ICT Convergence (ICTC), pp. 336 – 339, December 2012.
[13] K. Mythili, H. Anandakumar, "Trust management approach for secure and privacy data access in cloud computing", In: IEEE International Conference on Green Computing, Communication and Conservation of Energy (ICGCE), pp. 923-927, June 2014.

AUTHOR'S PROFILE

Manreet Sohal (born June 10, 1992) is research scholar pursuing PhD at Department of Computer Engineering & Technology, Guru Nanak Dev University Amritsar. She has passed out her M.Tech (CSE) and B.Tech (CSE) from Guru Nanak Dev University. Her main area of interest is Cloud Computing.

Sandeep Sharma graduated with B.E (Computer) degree from the University of Pune, received the M.E(Computer) from Thapar University Patiala and received his PhD degree from Guru Nanak Dev University Amritsar. He is a Professor and The Head of Department of Computer Engineering and Technology at Guru Nanak Dev University, Amritsar. He is a Chief Security Information Officer as well as Nodal Officer of Digital India Week. He is the Network as well as mail Administrator of the Guru Nanak Dev University .He has many research publications in the areas of parallel processing, wireless sensor networks and Cloud computing.