JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue

JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)

An International Scholarly Open Access, Peer-reviewed, Refereed Journal

Multi-Level Key Authentication for information on cloud

Prashant Srivastava
Computer Science Department
Chandigarh University
Gharuan, Punjab
19bcs1731@cuchd.in

Amit Kunar Singh
Computer Science Department
Chandigarh University
Gharuan, Punjab
19bcs3000@cuchd.in

Shiv Gurjar
Computer Science Department
Chandigarh University
Gharuan, Punjab
19bcs3021@cuchd.in

Hardeep Singh
Computer Science Department
Chandigarh University
Gharuan, Punjab
19bvs1725@cuchd.in

Harsh Sharma
Computer Science Department
Chandigarh University
Gharuan, Punjab
19bcs1636@cuchd.in

Er. Gagandeep Kaur
Computer Science Department
Chandigarh University
Gharuan, Punjab
Gagandeep.e12963@cuchd.in

Abstract

Cloud computing has fundamentally altered the ways in which we access, exchange, and store data. Abstract. However, this does bring up some new security concerns that need to be addressed. One of the most challenging aspects of cloud security is making sure that the data that is kept in the cloud maintains both its secrecy and its integrity. Based on this study, we propose a Multi-Level Key Authentication (MLKA) protocol for use with cloud data. The level of security afforded to cloud-based data by our technology is increased by virtue of the fact that it utilizes a variety of authentication procedures. Multi-factor authentication, insider threats, authentication methods, and cloud computing are some of the keywords associated with this topic.

I. Introduction

A significant number of businesses, universities, and other institutions, as well as individual users, have begun to make use of cloud in recent years. These systems make use of a substantial number of shared resources, which may include networks, servers, and storage space. In addition to that, they provide virtual services on demand. Every day, the current level of computer technology advances farther. In addition, in order for computer technology to continue to advance, Improvements to the system in order to attain the high processing power and enormous virtual capacity of the decades. These days, people utilize the internet for a wide range of purposes, including communicating, doing financial transactions, playing video games, and gathering information. It is necessary to do some kind of verification in order to ascertain whether or not the individual who is participating in all of this online activity is the same person they have. In order to complete financial transactions, more secure information, including personal data and other information connected to accounts, is required. Authentication systems may use a variety of authentication procedures, such as username and password authentication, biometric facial recognition authentication, and Kerberos authentication, among others. Authentication of textual and visual content using a hybrid public key infrastructure. Authentication using symmetric key technology. The authentication procedure is a method for determining whether or not the users who are participating in the connection are genuine.

The approach of logging in using a user name and password is by far the most used form of authentication. When using this strategy, there is a greater risk of confidential user information being made public in the event that the server's security is breached. Because of this, the user does not always put their whole reliance in this server that is provided by a third party. Additionally, password authentication is susceptible to a variety of security flaws, such as dictionary attacks and man-in-the-middle assaults, both of which may compromise the security of the system. In cloud computing systems, it is the obligation of other parties to provide the space for data storage

The term "cloud computing" refers to a relatively recent development in information technology that shifts the focus of computing away from personal desktop computers and onto remote servers accessed over the internet [1]. The provision of software, computer infrastructures, and platform services by means of the cloud computing model. This technique reduces the cost of computing while also allowing enterprises to concentrate on their core operations. Cloud companies often deliver one of these three categories of services to its customers. The acronyms for these categories are "Software as a Service," "Platform as a Service," and "Infrastructure as a Service," respectively. Cloud service providers provide their customers software applications in the form of a service known as Software as a Service (SaaS). Platform as a Service, often known as PaaS, is a model of cloud computing in which cloud providers make available to their customers various platforms on which those customers may build their own applications. In Infrastructure as a Service, also known as IaaS, cloud customers make service requests for various pieces of computer hardware, including processing units, storage devices, and network components [2]. Cloud computing customers are relieved of the burden of worrying about the specifics of data processing and the management of their data, which is one of the most significant advantages of cloud computing. Moving to the cloud does, however, provide brand new difficulties and worries in terms of security and privacy.. The authentication of cloud users is a crucial concern when it comes to the safety of cloud computing. A number of cloud service providers offer a single level authentication mechanism, such as a basic text password for customers to use while accessing cloud services; this is seen in Figure 1. [3] [4] [5].

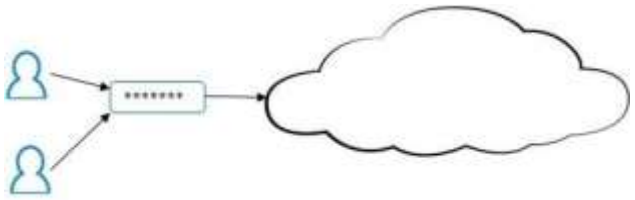

Figure 1. Single Level of Authentication for Cloud

2.Literature Review

Authentication in the vast majority of apps is accomplished only via the use of a username and password. Hackers just need a few minutes, thanks to password-cracking tools that are readily accessible for free internet, to determine a user's password. [6]. The National Institute of Standards and Technology (NIST) and the Federal Financial Institutions Examination Council (FFIEC) provide users with specific instructions on how to complete financial transactions. This is done with the intention of protecting users from the danger described above. argues that techniques requiring two levels of authentication, often known as two- factor authentication (2FA), should be used. It is not sufficient to just have one login password for each tier. and Specify a variety of different models for authentication and authorisation. The authentication process for the application has to make advantage of many tiers. Because of this, users are required to input a secret code that has been sent to their mobile device [7] [8][9].

There are specific recommendations that center on the risk management procedures that are required to verify the identity of retail and commercial clients that utilize internet-based financial services. These recommendations may be found in particular guidelines. In the field of computers, both the law and technology have seen substantial changes since the year 2001.

The standards place a greater premium on the protection of the information that pertains to the customers. The growing number of instances of fraud and identity theft are the primary emphasis of these rules. These guidelines also provide recommendations for ways to enhance existing authentication methods. states that Financial Institutions (FI) should perform periodic checks to ensure the following information: FI should identify risk mitigation actions, including

the appropriate authentication strength. FI should adjust, as necessary, their information security program in light of any relevant changes in technology. FI should conduct these checks at least once every three months. The information of FI's customers need to be protected from any internal or external hazards, including potentialthreats [10].

OTP, ASPE, RSA digital signature are the three components that make up the novel strategy for cloud authentication that was created by Yassin, A. A., and H. Jin. The system requires two different elements for authentication [11]. The model that is suggested in is based on a stringent authentication system. This is accomplished by introducing a multi-level authentication mechanism, which creates and authenticates the password in various stages in order to get access to cloud services. The fact that these techniques employ the same password for several levels of verification is one of their major drawbacks [12].

Using a tenants identification model, the researchers in deploy a novel framework for safe cloud authentication. To protect against a denial-of-service attack and to make the password more safe, update it. Jaidhar C. D. presented an improved approach for mutual authentication to be used with cloud architecture [13] [14].

3. Limitation

Clients or tenants may make use of the cloud provider's on-demand internet-based data storage services offered by cloud providers. In this configuration, the databases belonging to the client are kept in the data centers belonging to the cloud provider. The security procedures that cloud providers use are what determine the level of safety afforded to their customers' databases. Clients may safely access their data stored in the cloud thanks to single-level authentication used by cloud providers. Simple text passwords, biometric authentication, authentication via a third party, and graphical passwords are the primary forms of single-level authentication that are used in cloud computing[15] [16].

4. The Proposed Multilevel Scheme

The purpose of this study is to develop a fresh strategy with the intention of enhancing the degree of safety enjoyed by cloud service users. The multilevel authentication and multilevel security (MLS) concepts have been combined to provide the basis for the proposed approach. The system that has been designed has three distinct tiers of protection, starting with the most basic and working its way up to the most advanced.

Users who are on the lowest level only have access to a single password, which is a textual password. Users who are on the second level, however, have access to two passwords: a textual password and a biometrics password. When there is a rise in the level of sensitivity of the data, there is a corresponding increase in the need for protection. As shown in Figure 2, the most sensitive information is kept at the third level of this structure, and users have access to three different passwords in order to log in and retrieve their data.

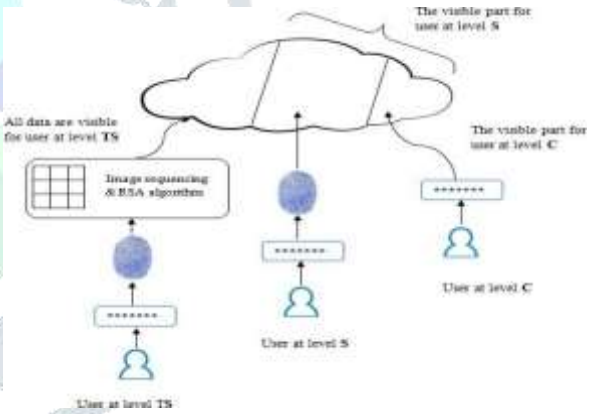

Figure 2. The Proposed Scheme

The concept of multilayer security refers to the practice of storing data at multiple levels of confidentiality within the context of the proposed system. The data may be housed inside the same organization, but they will have varying degrees of confidentiality depending on how important they are. Within the framework being proposed, there is a multilevel security hierarchy that is comprised of three levels of increasing levels of sensitivity. As illustrated in Figure 3, the three levels are confidential (C), secret (S), and top secret (TS), and they increase in level from lowest to highest. Users who need access to the data should have the appropriate degree of security access, which should match to the categorization level.

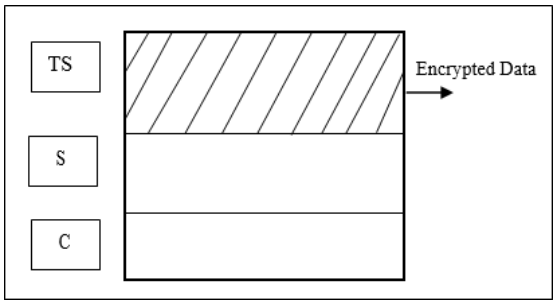

Figure 3. Multilevel Authentication Scheme

The data are separated into three layers according to the confidentiality of the data as follows: The data at the confidential level have the least amount of protection; each authorized user in this level has just one password to access his data. data. After entering the correct password, the user will have access to read and write the data contained inside this level, as shown in Figure 4.

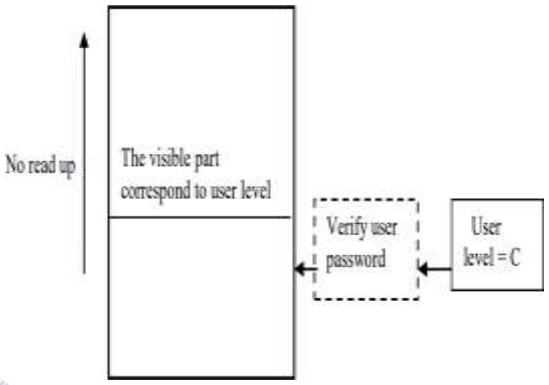

Figure 4. User at Level C

Users who have access to the S (secret) level may read data that has been encrypted to level C as well as material that is encrypted to their own level, but they are not permitted to write data encrypted to a lower level. As can be seen in Figure 5, every user at this level has access to not one, but two different passwords.

The data at the TS (top secret) level contain the maximum degree of secrecy, and in order for users to demonstrate that they are trustworthy, they are required to attempt accessing it with three different passwords. Before being uploaded to the cloud, the data at this level will first be encrypted. The third password, which is based on picture sequencing and uses the RSA method, will be used to increase the security of private data stored in the cloud.

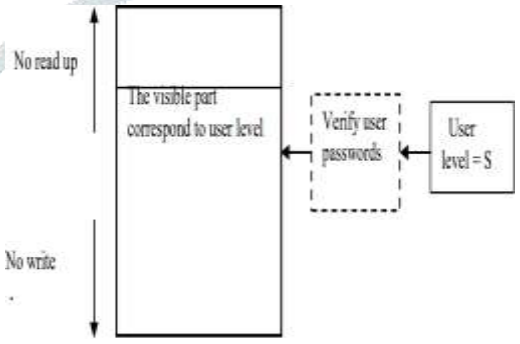

Figure 5. User at Level S

Let's say a password consisting of four photos has been established and used. In this particular instance, the sequence number will be something like (for example, 2468). Therefore, once we enter the sequence number, we will be granted access to go into our cloud. It would seem that this sequence will constantly be updated anytime the system is logged in, doing so to ensure that the password sequence will

remain the same, but that the position will change, as well as the numbers. The next time, the order in which the photos appear will be jumbled, and as a result, the password will also be modified. The new password is generated (for example, 4865) based on the order in which the user selects the photographs at the beginning of the process. Therefore, this process is repeated in order, which ultimately results in an unbreakable password.

Figure 6 illustrates how the use of RSA for data encryption, which will boost data security and was previously mentioned, will take place.

When a user inputs his name and the initial password (represented as a textual password in Figure 7), the suggested model is activated. If the user's level is equivalent to C, the system will show the data at this level once it has

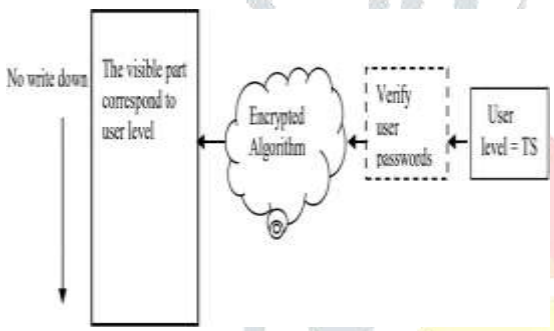

Figure 6. At Level TS

verified the user's password. When a user's level is more than level C, the user is required to input a biometric password. The user on level S goes through the identical procedure, which involves inputting two different passwords (one textual and one biometric). After that, the scheme checks the user passwords and, if the user level is equivalent to S, it displays the information in both this level and the level below it.

On the other hand, if the user's level is greater than the S level, the user will be given a third password. If the user level is equivalent to TS, the suggested technique would check the passwords of the individual users. Decrypt and display the information at this level, as well as the information at the lower levels.

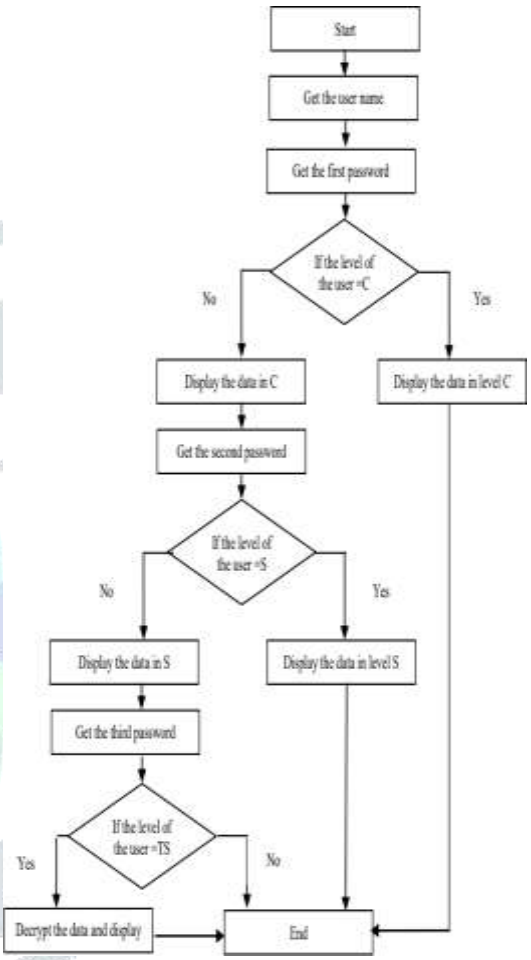

Figure 7. The steps for Proposed Scheme

6. Result and Discussion

The approach that has been presented is based on three layers of authentication, each of which is based on a different degree of user data. Textual, biometric, and graphical passwords, in addition to an encryption layer, are used in the proposed system to protect sensitive

information. Since there is more than one layer of data protection, the strategy uses the defense in depth discipline to ensure that data is secure. In addition, the system that has been presented makes use of more than one sort of password, including textual, biometric, and graphical passwords, in an effort to circumvent the constraints that are associated with the various password systems. Data that requires a greater level of security might have an additional layerof protection added in the form of encryption.

7. Conclusion

One of the most significant obstacles that must be overcome to ensure the safety of cloud computing is authentication. Because passwords are so simple to crack, single-level authentication presents many challenges, particularly when dealing with sensitive data. The answer for improving an authentication system that is based on multilayer authentication is represented by the scheme that was offered, which gave an extra layer of protection. The plan calls for three different degrees of authentication to be carried out, and the data is separated into these levels according to its level of sensitivity, which might be confidential (C), secret (S), or top secret (TS). The level C data are the least sensitive of the available options. To access the data on this level, the user at this level just has to remember a single textual password. The user who is now logged in at level (S) has access to both this level and the level below them using two different passwords: a textual password and a biometrics password. A user with the TS privilege level has access to three different passwords: a text password, a biometrics password, and an image sequencing password. Before being saved in a cloud database, the data at this level, which is the most sensitive data, is encrypted using the RSA method. The currently planned design, along with two additional state- of-the-art plans, were subjected to a comparative study and comparison. The first findings of the planned plan revealed some extremely encouraging outcomes.

References

[1] J. Rittinghouse, "Cloud computing: implementation, management, and security:," *CRC press ,* 2016.

[2] M. a. M. B. A. Yousif, "A Cloud Based framework for Plateform as a Service in Cloud Computing (ICCC)," in *International conference*, 2015.

[3] Z. X. a. Y. Xiao, "Security and Privacy in cloud computing," *IEEE,* vol. 15, pp. 843-859, 2013.

[4] N. Kshetri, "Privacy and Security issue in cloud Computing," *IEEE,* vol. 37, pp. 372-386, 2013.

[5] W. J. a. T. Grance, "Guideline on security and privacy in public cloud computing," *NIST special publication ,* vol. 800, pp. 10-11, 2011.

[6] A. K. a. Marcinsobota, "Distributed Authentication Systems enhanced by quantam protocal," *IEEE,* pp. 928-931, 2008.

[7] K. a. H. L. Mohammed RazaKanjee, "A Physiological Authentication Scheme in Secure Healthcare Sensor," *IEEE,* 2010.

[8] X. W. Z. Fengyu Zhao, "Multi-Tier Security Feature Modeling for Service-Oriented Application Integration," *IEEE,* pp. 1178-83, 2009.

[9] S. Singh and S. Bawa, ""“Design of a Framework for Handling Security Issues in Grids”," *IEEE,* 2006.

[10] S. S. a. S. Bawa, "A Privacy Policy Framework for Grid and web services," *IEEE,* pp. 809-817, 2007.

[11] H. J. A. I. W. Q. a. D. Z. A. A. Yassin, "Cloud authentication based on anonymous one time password," *IEEE,* 2013.

[12] H. D. a. V. Agrawal, "Multi-level authentication technique for accessing cloud services," *IEEE,* pp. 1-4, 2012.

[13] B. Z. a. A. Tauber, "Secure cloud authentication using eIDs," *IEEE,* pp. 397-401, 2012.

[14] C. Jaidhar, ""Enhanced mutual authentication scheme for cloud architecture," in Advance Computing conference (IACC)," *IEEE,* 2013.

[15] S. S. a. V. M. Viswanatham, "Addressing security and privacy issues in cloud computing," *IEEE,* vol. 48, pp. 708-719, 2013.

[16] Y. P. a. N. Sethi, "Enhancing Security in Cloud Computing Using Multilevel Authentication," *IEEE,* vol. 1, 2014.