International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 09 Issue: 05 | May 2022 www.irjet.net p-ISSN: 2395-0072

MULTI-FACTOR AUTHENTICATION SECURITY FRAMEWORK USING BlOCKCHAIN IN CLOUD COMPUTING

Aparna Thakare[1], Rinkal Gohil[2], Sakshi Gaikwad[3], Puja Dhavle[4]

[1]*Professor, Department of Computer Engineering, SCOE, Pune, India*
[2,3,4] *Student, Department of Computer Engineering, SCOE, Pune, India*

Abstract - *Authorizing access to the public cloud has evolved over the last few years, from simple user authentication and password authentication to two-factor authentication (TOTP), with the addition of an additional field for entering a unique code. Today it is used by almost all major websites such as Facebook, Microsoft, Apple and is a frequently used solution for banking websites. On the other side, the private cloud solutions like OpenStack, CloudStack or Eucalyptus doesn't offer this security improvement. This article is presenting the advantages of this new type of authentication and synthetizes the TOTP authentication forms used by major cloud providers. For this purpose, the web authentication form has been modified and a new authentication module has been developed. The present document covers as well the entire process of adding a TOTP user, generating and sending the secret code in QR form to the user. Also add the Blockchain technology for uploading data in proposed model which secure our uploaded data on cloud.*

Key Words: Cloud Computing, Multi-Factor authentication, OTP.

1. INTRODUCTION

We present Secured Access Control Using Multifactor Authentication for Cloud Computing Services to achieving security in distributed cloud storage. It becomes increasingly susceptible to use cloud services to share data in a friend circle in the cloud computing environment. Since it is not feasible to implement full lifecycle privacy security, access control becomes a challenging task, especially when we share sensitive data on cloud servers. This project is presenting the advantages of this new type of authentication and synthetizes the TOTP authentication forms used by major cloud providers. For this purpose, the web authentication form has been modified and a new authentication module has been developed With the help of our system we can achieve maximum security of data in distributed cloud. Cloud computing its a software platform used to control large pools of compute, storage, and networking resources of one or more datacenters. By using this environment, users can benefit of shared computing resources from anywhere, at any time using an Internet connection. Their personal data that a couple of years ago used to be stored on personal hard drives, DVDs or CDs is now stored on cloud. Nowadays many companies are offering cloud data storage services such as Google Cloud Storage, AWS S3 and Microsoft Azure Storage, etc. The company that offers cloud services is usually called Cloud Service Provider (CSP). The high demand of computing resources has pushed organizations to outsource their storages and computing needs. Cloud computing can help organizations on accomplishing more by separating the physical bound between IT infrastructure and its users. Nevertheless, both normal users and companies cannot afford to put their sensitive information in a platform that they cannot control without being assured that their data is safe and secure. In order to have a secure cloud environment each of its components must be secured. Any cloud computing client must authenticate before being able to use cloud resources. The authentication component is a must on any type of cloud therefore there is no coincidence that most of the attacks are performed at this level.

1.1 Motivation

In the existing system no more security for storing data on cloud so we propose a Secured Access Control Using MultiFactor Authentication and Blockchain technology for Cloud Computing Services to achieving security in distributed cloud storage. The mechanism can enhance the security of the system, especially in those scenarios where many users share the same computer for web-based cloud services.

1.2 Goals And Objective

- To Improve The security.
- Secure our cloud data.
- Securely share online data.

1.3. Scope

Methodology achieving security in distributed cloud storage. In particular, in our proposed access control framework, a property based access control system is executed with the need of blockchain technology. As a client can't access the data on the off chance that they don't hold OTP. With the help of our system we can achieve maximum security of data in distributed cloud.

2. LITERATURE REVIEW

- **Security Assessment of OpenStack cloud using outside and inside software tools**

Authors: Ionel Gordin, Adrian Graur, Alin Potorac, Doru Balan.

Description:

In this Paper, the security assessments performed , analyzed the OpenStack cloud Pike version from both outside and inside the cloud network environment. Tests were performed using 3 vulnerability scanners: Nessus, Metasploit and OpenVAS. An outside scan has been performed as well using web app Tenable .IO. we can conclude that Metasploit provided the most results. Although, Metasploit could be considered from this perspective the absolute winner, Nessus provided the most details about each opened port found and offered suggestions on how to mitigate the problem found. OpenVAS is a free of charge application despite Nessus and Metasploit, the results were surprisingly well organized and detailed. To secure the OpenStack services, first should be considered what ports must be accessible from Internet and what ports to be opened from inside the cloud. At the end of this incursion we will have one list of opened ports for inside and another list for outside ports. Some ports should be accessible only to some inside or outside hosts. When the entire list of ports and their limitations is completed then it can be applied the necessary firewall rules. OpenStack comes with an embedded firewall that can be configured easily through dashboard web interface. Future work will analyze further the security of cloud containers and will provide a more detailed approach about isolating VMs from their neighbors and as well from outside threats.

- **Survey on Usable and Secure Two-Factor Authentication**

Authors: Archana B.S.,Ashika Chandrashekar, Anusha Govind Bangi,B.M. Sanjana,Syed Akram,

Description:

In todays Internet environment, each ones identity and secret information are easily copied and forged. Hence its necessary to validate the user by means of password basedauthentication. Single factor based passwords are not considered secure anymore on the Internet and in the banking world. Passwords that are easily guessed are easily intercepted by password cracking tools. Two Factor authentication provide an additional layer of security assurance by utilizing two different factors. Several protocols have been put forth to make authentication secure. Das.et.al scheme introduced remote user authentication which is uses a Dynamic ID where the stolen verifier attack cannot take place because there is no verifier table. This was followed by Misbah.et.al scheme which involved the use of timeserver and achieved mutual authentication. Syed.et.al scheme is an extension of Misbah.et.al scheme where the random number is generated by taking the time stamp on the client machine as the seed value and thereby avoids the need to synchronize the timeservers. These schemes are secure against various attacks.

- **An Enhanced SMS-based OTP Scheme**

Authors: Yonghe Zhou, Liang Hu, Jianfeng Chu

Description:

In this paper, we proposed a scheme to enhance the security of SMS-based OTP. In this scheme, we take SMS as transport layer. Message are encrypted in this layer. Other applications can get the message of transport layer but they cant decrypt it. The decrypt work proceeded in application layer This scheme can prevent outside threats like MITM attack and replay attack. It also can prevent threats from applications on smartphone like eavesdropping and forgery attack. In the course of this work, we realize that the user might change his smartphone, the counter stored in smartphone might get lost. In our future work, TOTP will be introduced to calculate the request code. Thus, the counter will be replaced by a time parameter which do not need to store on smartphone.

- **OTP-Based Two-Factor Authentication Using Mobile Phones**

Authors: Mohamed Hamdy Eldefrawy, Khaled Alghathbar, Muhammad Khurram Khan,

Description:A new two-factor OTP-based authentication scheme has been proposed using mobile phones as they are becoming more and more powerful devices. This new algorithm provides forward and infinite OTP generation using two nested hash functions. We have illustrated our approach to an online authentication process. This scheme achieves better characteristics than the other schemes discussed above. Our proposal is not limited to a certain number of authentications, unlike the previously-mentioned OTP hashing-based schemes, and does not involve computationally expensive techniques to provide the infiniteness like. Our algorithm doesnt require a token embedded server synchronized clock like. Our approach eliminates the problems with utilizing OTPs with an SMS, consisting of the SMS cost and delay, along with international roaming restrictions like. A detailed security analysis was also performed that covered many of the common types of attacks. The two factor authentication property has been achieved without restrictions.

3. ADVANCED SYSTEM

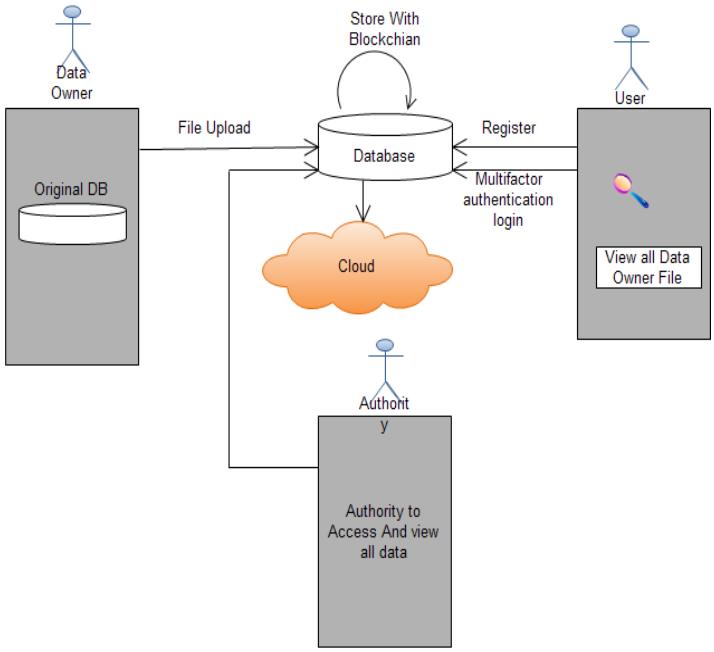

Fig -1: Advanced System Architecture

In this system we there are three modules:

1. Data Owner.
2. User
3. Authority

In this Data owner is the owner of file uploaded on cloud. Data owner can upload file seurely using blockchain technology in our web application. User can view and download all file uploaded by data owner. Authority have access and view all data owner and user registered on our application. In our application there is only one authority user is present and number of data owner and user can registered.

3. CONCLUSION

We developed a web application under cloud computing for uploading and store document on cloud with the help of mutifactor authentication and blockchain technology. In multifactor authentication system we use OTP, Unique code for login and we use Blockchian technology for seurely store our document on cloud.

REFERENCES

[1] Ionel Gordin, Adrian Graur, Alin Potorac, Doru Balan,"Security Assessment of OpenStack cloud using outside and inside software tools",14th International Conference on DEVELOPMENT AND APPLICATION SYSTEMS, Suceava, Romania, May 24-26, 2018.

[2] Archana B.S.,Ashika Chandrashekar, Anusha Govind Bangi,B.M. Sanjana,Syed Akram,"Survey on Usable and Secure Two-Factor Authentication",2017 2 nd IEEE International Conference On Recent Trends in Electronics Information Communication Technology (RTEICT), May 19-20, 2017, India.

[3] Yonghe Zhou, Liang Hu, Jianfeng Chu,"An Enhanced SMS-based OTP Scheme",2nd International Conference on Automation, Mechanical Control and Computational Engineering (AMCCE 2017).

[4] M. Kimura and K. Saito, "Tractable models for information diffusion in social networks," in PKDD, 2006, pp. 259–271.

[5] Mohamed Hamdy Eldefrawy, Khaled Alghathbar, Muhammad Khurram Khan,"OTPBased Two-Factor Authentication Using Mobile Phones",2011 Eighth International Conference on Information Technology: New Generations.