International Journal of Research
Available at https://edupediapublications.org/journals
e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 05 Issue-01
January 2018

Two Factor Authentication Access Control for Web based Services in Cloud Computing

Anireddy Swathi
M.Tech(Computer Science & Engineering), Bharath Institute of Engg & Tech., Ibrahimpatnam(M).R.R Dist.
G.Manohar Gosul, M.Tech,(Ph.D)
Assistant Professor, Dept of CSE, Bharath Institute of Engg & Tech., Ibrahimpatnam(M).R.R.Dist.

Abstract:*In our proposed machine E2FA get to keep the framework, a user canget right of access to the cloud date primarily based on an encrypted tool to attach it PC. It was actualizedwith the assist of consumer secret key, it cannot get the data from a cloud on every occasion the deviceis off. That encrypted tool uniquely works on one device only. It will no longer be dealing withboth the issue to increase the security of the framework, in these confined situationsthe clients are going to have the identical form of PC for the cloud data.*

Keywords-2FA, cloud computing, Fine grained Access Control, SecurityKey, Hierarchical, Cloud data, Security deviceltering.

I. INTRODUCTION

Cloud computing is a digital host laptop system that allows enterprises to buy, hire, sell, or distributesoftware program and other digital resources over the internet as an on-demand carrier. It now not depends on a server or awide variety of machines that bodily exist, as it's miles a virtual system. There are many programs of cloud computing,together with data sharing data storage[1], huge data management[2] medical data machine and many others. End customers get right to access tocloud-primarily based packages via an internet browser, sensitiveuser or mobile app even as the enterprise software and user'sdata are stored on servers at a remote place. The advantages of Internet-based total cloud computing offerings are large, whichinclude the benefit of accessibility, reduced cost, and capital prices, expanded operational efficiencies,scalability, flexibility and immediately time to the marketplace.Though the new paradigm of cloud computing presents outstanding blessings, there are meanwhile additionally concerns aboutprotection and privateness, particularly for web-based total cloud services. As sensitive data can be protected in the cloud forsharing a reason or convenient get right of entry to; and eligible customers might also access the cloud machine for numerous programsand offerings, user authentication has come to be a vital issue for any cloud device. A user is required to log inearlier than the usage of the cloud offerings or accessing the sensitivedataprotected in the cloud. There are two troubles with theconventional account/password based totally device. First, the conventional account/password based totally authentication is notprivateness-preserving. However, it's miles well acknowledged that privacy is a crucial feature and that must beconsidered here within the cloud computing structures. Second, it is commonplace to the percentage a computer with unique people.

It may be easy for hackers to install a few adware to study the login password from the web-browser. These dayspproposed to get right of entry to manage model referred to as characteristic-primarily based access manage is a good candidate to tackle the primary trouble. Itnot handiest offers anonymous authentication however also further defines get entry to management guidelines based totally on extraordinaryattributes of the requester, surroundings, or the data item. In a characteristic-primarily based get admission to manipulate system1, every userhas a user secret key issued by the authority. In practice, the user secret key is stored inside the personal computer.

When we consider the above mentioned second problem on web-based services, it is common that computers maybe shared by many users especially in some large enterprises or organizations. For example, let us consider thefollowing two scenarios:

• In a hospital ,computers are shared by different staff. Dr. Alice uses the computer in room A when she is on dutyin the daytime, while Dr. Bob uses the same computer in the same room when he is on duty at night.

• In a university, computers in the undergraduate lab are usually shared by different students. In these cases,

usersecret keys could be easily stolen or used by an unauthorized party. Even though the computer may be locked by apassword, it can still be possibly guessed or stolen by undetected malwares.

A more secure way is to use two-factor authentication (2FA). 2FA is very common among web-based e-bankingservices. In addition to a username/password, the user is also required to have a device to display a onetimepassword. Some systems may require the user to have a mobile phone while the one-time password will be sent tothe mobile phone through SMS during the login process.

As sensitive data may be stored in the cloud for sharing purpose or convenient access; and eligible users may alsoaccess the cloud system for various applications and services, user authentication has become a critical component forany cloud system. A user is required to login before using the cloud services or accessing the sensitive data stored inthe cloud. There are two problems for the traditional account/password based existing system. First, the traditionalaccount/password-based authentication is not privacy-preserving. However, it is well acknowledged that privacy is anessential feature that must be considered in cloud computing systems. Second, it is common to share a computer amongdifferent people. It may be easy for hackers to install some spyware to learn the login password from the web-browser.

Therefore such systems are not fully secured.

Disadvantage:

1) The traditional account/password-based authentication is not privacy-preserving.

2) Common to share a computer among different people. It may be easy for hackers to install some spyware tolearn the login password from the web-browser.

3) Existing system is not fully secured.

II. RELATED WORK

Rashmi 1, Dr.G.Sahoo2, Dr.S.Mehfuz3,[3] presented securing software as a service model of cloud which is usedto describe the security challenges in Software as a Service (SaaS) model of cloud computing and also end eavors toprovide future security research directions.From this paper we have referred the solution On Cloud ComputingSecurity.

KashifMunir and Prof Dr. SellapanPalaniappan,[4] presentedframework for secure cloud computing. A cloudsecurity model and security framework that identifies security challenges in cloud computing. From this paper we havereferred the solution for security challenges in cloud computing andproposed a security model and framework forsecure cloud computing environment thatidentifies security requirements, attacks, threats, concerns associated to thedeployment of the clouds.

Mr. AnkushKudale,Dr. Binod Kumar,[5] proposeda study on authentication and access control for cloud computing.The security issues are still in loop of solutions, because of that so many organizations are waiting foradoption of cloud computing services. This is a review paper for authentication and access control for cloud computing.From this Paper, we have referred a good solution authentication and access control for the cloud computing.

Harvinder Singh1, Amandeep Kaur2,[6] presented access control model for cloud platforms using multi-tiergraphical authentication. This proposed scheme has been evaluated under various situations. Both of the graphicalpassword schemes have been evaluated individually with various password combinations. The new multi-levelgraphical password scheme can be considered as a secure scheme for cloud platforms. FromthisPaper, we have referredthe model will be enhanced with more functionality and higher level of authentication security; it would beimplemented by using security questions, image based security for the login protection and at the last level UserIdentification Number (UIN) would be used to access or view the data in cloud platforms on mobile devices andsoftware systems for computers

Joseph K. Liu, Tsz Hon Yuen, Man Ho Au, Xinyi Huang, Willy Susilo, and Jianying Zhou,[7] proposed k-timesattribute-based anonymous access control for cloud computing which is particularly designed for supporting cloudcomputing environment. From this Paper , We have referred an attribute-based access control mechanism

which can beregarded as the interactive form of Attribute Based Signature.

III. PROPOSED WORK

In this paper, we propose enhanced fine grained two factor access control for webbased cloud computing management system, we use simple security device byusing Hierarchical based encryption. The device has some properties: (1) it willreason some light-weight method and (2) it's tamper resistant, i.e., it is acceptedthat nobody will forced the lock it to urge the key info hold on within.

Steps for the working model of our proposed system:
In our proposed system has the following steps to provide security for access cloudresources.
Login Process: In this stage, the client uses username, password, E-mail,etc. details are getting from cloud service provider.
Security Device: The system provides a device like pen drive, USB, etc…
When the device is placed to our PC then the drive will be detected when weaccessed.
Access Authentication: The secured encrypted file is loaded into securitydevice by using hierarchical based encryption and this helps to keep the filesecure.

Figure.1 user key generation process

Figure.2 user authentication process

Hierarchical identity-based encryption: In an identity-based secret writing(IBE) system, there is just one non-public key generator (PKG) to distribute nonpublic key for every user, which is undesirable for a massive network because ofPrivate Key Generation encompasses a heavy job. HIBE operator needs acontinuing length of Cipher text and a continuing range of additive mapoperations throughout secret text.

Our system consists of the following entities:
• **Trustee**: It is responsible for generating all system parameters and initializes the security device.
• **Attribute-issuing Authority**: It is responsible to generate user secret key for each user according to theirattributes.
• **User:** It is the player that makes authentication with the cloud server. Each user has a secret key issued by theattribute-issuing authority and a security device initialized by the trustee.
• **Cloud Service Provider**: It provides services to anonymous authorized users. It interacts with the user during theauthentication process.

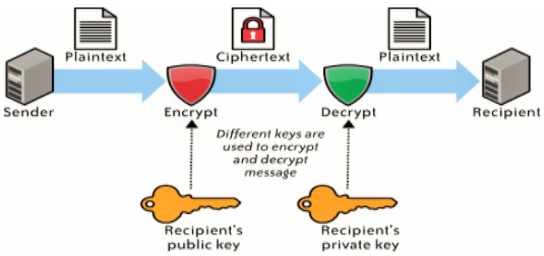

Figure.3 Hierarchical identity-based encryption

We propose a HABE model, that will access the management policies area unitpresented in DNF, and all properties in one conjunctive clause should beadministered by identical DM per the HABE scheme, it contains a multiplenumber of keys with different usages. The outline of the HABE theme, bypresenting randomized polynomial time algorithms as follows:

1. Setup(i)→(parameters, Ni0): The RMK provides highly secured parameter i as input, andoutputs system parameters and RMK Ni0.
2. Create DMK (parameters, Nik, RiK+1) →Nik+1 : Either RMK or DMK creates keys for DMs
parameters and its master key.
3. CreateUsers (parameters, Nik,Riv,Ria)→(Tik,v,Tik,v,a): DMK mainly examine V is eligiblefor a or not, which is created itself. The V is provided with both user identity secret keyand attribute secret key, with the help of parameters and the master key, if not the outputsare "NULL".
4. Encryption (parameters, {Ria|aEA)→(T): User is going to take the file *f* then the DNFaccess control A, and non-private keys of all attributes in A, as inputs, and gives ciphertextT as output.
5. Decryption (parameters, CT,Tik,v{Tik,v,a|aECCg→(*f*): The user having the attributesshould be satisfied by the jthconjunctive clause CCg, takes parameters ,CT, the identitysecret key, and parameter secret keys of user provided on all attributes in CCj, as inputs,to recover the plaintext.

IV. CONCLUSION

In this paper, we've got demonstrated any other 2FA access manipulate framework for online distributed computingadministrations. Based on the function based totally get right of access to control device, the proposed 2FA get access to manipulateframework has been diagnosed to no longer simply provide electricity the cloud server to restriction the manner-in to those customers with thesame association of residences moreover keep customer protection. However in this paper, we've offered E2FA version to comfy get access to internet-primarily based cloudofferings of the Hierarchical characteristic-based totally encryption version for control get right of access to, theenhanced 2FA get to adjust framework goes to be defined as not truly empower greater 2FA to get to adjust framework accomplishes the needed security.

REFERENCES

[1] C. Chu, W. T. Zhu, J. Han, J. K. Liu, J. Xu, and J.zhour Security concerns in popular cloud storage services.IEEE Pervasive Computing, 12(4):50–57, 2013.

[2] J. Baek, Q. H. Vu, J. K. Liu, X. Huang, and Y. Xiang. A Secure cloud computing based framework for big datainformation management of smart grid. IEEE T. Cloud Computing, 3(2):233–244, 2015.

[3] Rashmi 1, Dr.G.Sahoo2, Dr.S.Mehfuz3, "Securing Software as a Service Model of CloudComputing: Issues and Solutions", IJCCSA ,Vol.3, No.4, August 2013.

[4] KashifMunir and Prof Dr. SellapanPalaniappan," FRAMEWORK FOR SECURE CLOUD COMPUTING", IJCCSA,Vol.3, No.2, April 2013.

[5] Mr. AnkushKudale,Dr. Binod Kumar," A STUDY ON AUTHENTICATION AND ACCESS CONTROL FOR CLOUD COMPUTING", Vol.1(2), July 2014 (ISSN: 2321-8088).

[6] Harvinder Singh1, Amandeep Kaur2," Access Control Model for Cloud Platforms Using Multi-Tier Graphical Authentication", Volume 4 Issue11, November 2015.

[7] Joseph K. Liu, Tsz Hon Yuen, Man Ho Au, Xinyi Huang, Willy Susilo, and JianyingZhou,"k-times attribute-based anonymous access controlfor cloud computing", IEEE Transactions on Computers, 64 (9), 2595-2608.