

Implementation of Multilayer Security in Cloud Computing for Secure Authentication

Poonam Kaurav¹, K.K. Joshi², Neelam Joshi³

P. G. Student, Department of Computer Science & Eng., MPCT Gwalior, India¹

Assistant Professor, Department of Computer Science & Eng., MPCT Gwalior, India²

Assistant Professor, Department of Computer Science & Eng., MPCT Gwalior, India³

ABSTRACT: Now a days the cloud computing is rising and resourceful technology. The requirement of IT industry is to repository terabyte data generated by every day. For depot IT requires many of hardware, software and network frameworks. Cloud computing solve this problem in cost effective manner. It also changed the vision completely not only IT Industry but some other sectors like healthcare, education sector, etc. It has potential to provide servers for extensive variety of resources from research to E commerce. Cloud computing is growing very fast because of their features like resource potential, network infrastructure, storage ability, cost effective, quick access of information. On other side all the data is virtual and cloud is as open facilities and public network are using for their application and services, which in turn has question on security disputes like verification data loss. The paperproposed verification model using Multi Authentication System(MAS) technique and threshold cryptography

KEYWORDS: Secure Keyboard, OTP, Knowledge Base Verification System.

I. INTRODUCTION

Cloud computing is one of the healthy and leading technology in present scenario .it offers services in tiniest cost manner. Than traditional tactic user can easily have all services of cloud and share their data. The services provided by cloud computing is like Google drive, cloud storage, i cloud. Cloud provide their best features but everything is on internet so that there are chance of hacking of data. We aware there are many safety issues in cloud computing like system and data safety are the extensive areas .In data security there are many issues like access control, data integrity, data Confidentiality, data, data integrity data location, data availability authentication. All the security issues are delicate but most important and skepticism subject is data confirmation. Authentication contrivance helps to establish proof of identities. The validation mechanism process certifies that the origin of electronic message or document is properlyrecognized. For data validation login and password is compulsory provided by cloud service provider the validation mechanism may be applied in both domain and workgroup. Once password is hacked by the hacker validation is lost and attacks on obtainable data which can be altered, erased. Therefore we try to propose new prototype that can solve issues of validation so that approved user can get all services provided by cloud provider .in this paper we are proposing new security tool based on MAS protocol and threshold cryptography Many real life systems use an validation protocol called MAS.

II. RELATED WORK

Validation process provides password and login. But in the public network the password can be easily hacked by the hacker so that there are many instrument are used like importantstructure where we are commonly used symmetric and asymmetric algorithm .one of the mostprevalent algorithm in asymmetric is RSA. It uses with MASverification protocol. RSA is very strong procedure but there is some drawback of this method generating keys over head of keys. Symmetric procedure is also used for secure authentication. Best algorithm of symmetric scheme is Diffie Hellman algorithm but again there are some drawback of this scheme is key interchange problem. [1]Maximum tasks are

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 3, March 2017

performed by internet with these tasks a threat is occurred i.e. leakage of private data like personal information etc. To manage these types of issues we use MFA, OTP, CRYPTOGRAPHIC, HASHING techniques. [2] Biometrics techniques are mainly centered on face, fingerprint and iris detection verifications and identifications systems. In detection process system only checks all the data exists for reading process or do not match with the existing data. [3] The service provider challenges the user with an image password. To control the suitable click points and their order, the user needs some suggestion information conveyed only to her handheld device. They show that our method can overcome threats such as key-loggers, weak password, and shoulder surfing [4] they present an exploratory comparative study of the usability of 2F technologies. First, they conduct a pre-study interview to identify popular technologies as well as contexts and motivations in which they are used. They present the results of a quantitative study based on aiming to measure the usability of three popular 2F solutions: codes produce by safety tokens, one-time PINs received via email or SMS, and devoted smartphone apps (e.g., Google Authenticator).

[5] This paper emphases on the execution of two-factor authentication technique by using both users friendly old-style Alphanumeric Password and graphical Password as gateway for authentication. [6] The threats of using static passwords to authenticate users show more and more security risks with the development of hacking. They introduce a DCT based stenographic method for data hiding. [7] Cloud Computing is constantly rising and displaying constant growth in the field of computing. The main exciting task in cloud computing is the security and privacy issues caused by the subcontracting of infrastructure, delicate data and perilous applications and its multi-tenancy nature. [8] There have been serious privacy concerns about outsourcing user information to cloud servers. But also due to a large number of cloud data security cases happened in recent years. Proposed research is a privacy preserving system using Attribute based Multifactor Authentication. Proposed system work on privacy to user's data with safe and secure authentication and store them on cloud servers such that servers do not have access to sensitive user information. So public key infrastructure having some drawback. Validation Using Graphical Password in Cloud is also one method it resist to mutual attacks and improve safety in cloud computing. Acquiring user authentication using single sign in on cloud .it is one of the improved solution it decreases number of password and login. But again there isdrawback multiple user cannot be involved protected locking for untrusted clouds mechanism. There is some difficulty of public key structure. So there is another idea called secret sharing scheme. In which secret is alienated in to the parts and distribute among trusted dealer. When someone else wants secret again pool all parts of stealth and rebuildunique one. This secret resolves the trick of key exchange

III. PROPOSED WORK

The validation is the procedure to authenticate client before enter in cloud it is not just putting password and login. Confirmation is most sensible issues in cloud for the same MAS is validation protocol used in cloud. It is the protocol that works with four parties.

1. Client station
2. Authentication server
3. Knowledge Base Verification System
4. Server offers services
5. Security Keyboard

MAS is mainly works on "Voucher" to communicate with other user interconnect over non secure data.

IV. PROBLEM STATEMENT

As safety is sensitive issue in cloud computing the data are coming from cloud using public network (internet) there are probabilities to hack the data. There have been lot of work done on safety issues and tests but still there is not 100% full immuneclarification. There are many physical and some other attack on data that abolish data on server. one result for that is scattered the data on more than one server instead of one server .but this not resolve problem totally because data stored in encrypted mode using encryption key .the assailants attack on key and may be hack the data.

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 3, March 2017

V. PROBLEM SOLUTION

Attackers counter attack on data that is located on same server. So that solution is do numerous copies of same data and data is placed on various servers. But data is encoded by encrypted key. Attackers may be attack on key so that data is exposed to the assailants. The clarification of this problem is instead of putting multiple copies of data on different server we are smearing Shamir's clandestine sharing on key. The encrypted key is alienated into number of parts and stockpiled them on different server. The most well-known faultless secret sharing scheme is the (k, n) -threshold scheme first proposed by Shamir in 1979 and hereafter mentioned to as a Shamir threshold scheme A key can be recreated again with least number of secret that are on dissimilar server there is no problem if attackers attack on one server The remaining server can rebuild key. This Shamir's scheme overwhelmed problem of key interchange. The secret can be recreated only when an adequate amount of shares are combined together; single shares are of no use on their own. More formally, in a secret sharing scheme there are single dealer and n troupes. The dealer gives a stealthy to the players, but only when specific circumstances are fulfilled. The dealer achieves this by giving each player a portion in such a way that any cluster of t (for threshold) or more players can together renovate the secret but no group of less than t players can. Such a structure is called a (k, n) -threshold scheme (sometimes it is written as an $(k-n)$ threshold scheme).

VI. WORKING MODEL

As suggest work is based on various authentication model. It has following steps

1. Authentication server:

Whenever a cloud wants to access a facility from cloud server it entails a "Ticket" before it will decency client request. Only on the foundation of that ticket the cloud server will grant access to all the subscribed service to client. This ticket proves client's confirmation to server. This removes overhead of cloud server for execution verification orders and also protects cloud's dispensation and memory. To get ticket client first request authentication from the Authentication Server (AS). The AS created by "session key" (which is also an encoded key) basing on client's encrypted password and an arbitrary value that signifies the required service. The session key is effectively used a "Knowledge Base Verification System" that will be used by the user to get chief ticket to access facility.

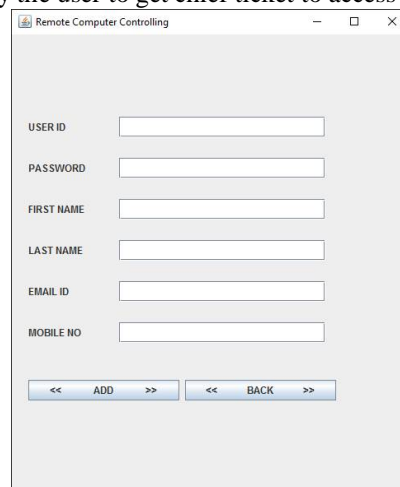


Figure 1: Registration Form for Cloud

2. Knowledge Base Verification System

A knowledge base verification system (Figure 2) is a verification system in which the user is asked to answer at least on "secret" question this is the normal process we always face. But in this project we made it more intricate while asking a

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 3, March 2017

question we used to display a multiple sections of Images and ask the user a question related to these images due to this the probabilities of data leakage is very low and the security of data is robust.

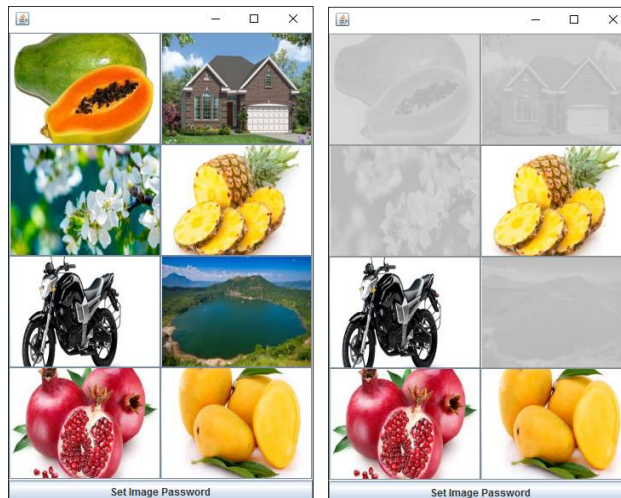


Figure 2: Knowledge Base Password

Secure Keyboard:

A secure keyboard is a device that is specifically designed to enable isolation between connected computers. Computers are typically connected to different networks and isolation between these networks must be assured to prevent data leakages and intrusions. The main persistence using the Secure Keyboard is to input password through it not using system keyboard, user entered the password using secure keyboard and enter into the cloud and when the secure Keyboard is used the system normal keyboard did not work. It makes the system Liable and Secure

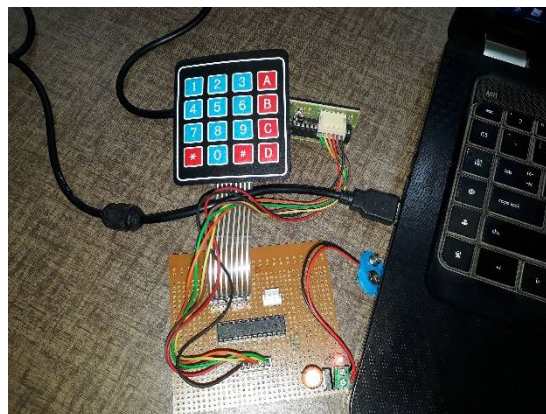


Figure 3: Secure Keyboard

ALGORITHM USED

- Step 1: [Login page from cloud]
Read login id
- Step 2: [Display picture password image read only select image by user]

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 3, March 2017

- Step 3: [Check images password open DB on server and read user image according to login id]
If (read image is equal to selected image)
Then
Display secure login Goto step 4
Else
Goto step 2
- Generate message for mobile (unauthorized login)
[End of if statement]
- Step 4: [Enter password using secure keyword]
1) Open serial post communication to connect with keyboard
2) Read login id from keyword
3) Read password through keyboard
4) Press # to confirm
- Step 5: [Check password]
1) Open DB to check entered password.
2) If(login id & password matched)
Then generate random OTP for user
Go to step 6
Else
Go to step 1
[End of if statement]
- Step 6: [Input OTP to entered into cloud]
If (input OTP is valid)
Then
Open application
Else
Go to step 1
- Step 7: [End]

Random picture password registration

- Step 1: [Prepare picture database
According to various categories on server]
DB=prepare database ()
- Step 2: [Show the user registration from when fetch by server
Read ID.
Read random picture password.
Read password (secure password)
Read mobile no
- Step 3: [Save all information on cloud database]
Save DB registration
- Step 4: [End]

VII. CONCLUSION

In this paper we have deliberated about the necessity of authentication in cloud computing .It is description method of authentication by MAS and threshold cryptography so that encryption technique is more vigorous. There have lot of effort done already on safety issues and encounters but still there are loop holes. This work of literature is irreplaceable approach because suggest structure minimizes the problem of alteration of key that are usually occurs in symmetric and asymmetric key cryptography.

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 3, March 2017

VIII. FUTURE WORK

We have discussed innovative approach for safety of authentication but threshold cryptography distribute secret and store in different server. That means server is reliable entities but some approved user itself changes the key construction that is deposited as part of secret on server then next time some approved user uses that secret to part reconstructed .but that key cannot be shaped because one or more part of secret are not unique secret that are intricate to reconstruct key. We can enhance this work for identification and revealing of cheater among share holder that holds the part of secret.

REFERENCES

- 1] Implementing High Grade Security in Cloud Application using Multifactor Authentication and Cryptography Niharika Gupta and Rama Rani
- 2] Biometric Authentication in Cloud Computing RakhshandaBatoool Ghazal NaveedAbdulhaq Khan 3] Universal Multi-Factor Authentication Using Graphical Passwords AlirezaPirayeshSabzevar, AngelosStavrou Computer Science Department, George Mason University, Fairfax, Virginia, 22030
- 4] A Comparative Usability Study of Two-Factor Authentication Emiliano De Cristofaro† University College London e.decrisofaro@ucl.ac.uk Honglu Du PARC honglu.du@parc.com Julien Freudiger PARC julien.freudiger@parc.com Greg Norcie† Indiana University
- 5] Two factor Authentications for Secured Login in Support of Effective Information Preservation and Network Security S. Vaithyasubramanian, A. Christy and D. Saravanan,Sathyabama University, Chennai, India 2 Faculty of Operations and Systems, IBS Hyderabad, India
- 6] Multi-factor Authentication in Banking Sector TusharBhivgade,MithileshBhusari , Ajay Kuthe , Bhavna Jiddewar, Prof. PoojaDubey Department of Computer Science & Engineering, Rajiv Gandhi College of Engineering & Research, Nagpur ,India.
- 7] Multi-factor Authentication in Cloud Computing for Data Storage Security DeepaPanse Assoc. Prof. CSE Dept. GCET, Keesara JNT University, Hyderabad, India P. Haritha Asst. Prof. CSE Dept. GCET, Keesara JNT University, Hyderabad, India
- 8] Attribute based Multifactor Authentication for Cloud Applications T.LakshmiPraveenaM.Tech Scholar VVIT College of Engineering Nambur,Guntur(Dt),AP V.RamachandranAsst.Professor VVIT College of Engineering Nambur, Guntur (Dt), AP CH. Rupa, Ph.D Associate Professor VVIT College of Engineering Nambur, Guntur (Dt), AP