International Journal of Scientific Engineering and Applied Science (IJSEAS) – Volume-2, Issue-7,July 2016
ISSN: 2395-3470
www.ijseas.com

# Multilayer Security in Cloud Computing for Safe Authentication

**Poonam Kaurav[1], Prof. K.K. Joshi & Neelam Joshi[1]**

[1]Deptt. Of Computer Science & Engg., MPCT Gwalior.

## Abstract

As we are familiar with the term cloud computing. It is an Internet based computing whereas multiple resources and services like applications, storage and servers are delivered to the computers and devices through the internet. Cloud computing is continuously growing and covered a vast area of computing.

But with the growth there are some of the problems came like there are a huge amount of data on cloud server what precautions we take for cloud security?

The security and privacy issues caused by the outsourcing of infrastructure, sensitive data and critical applications and its multi-tenancy nature. In this research paper the area for security of cloud computing is very vast for research and many types of authentication methods and multi-factor user authentication.
A major weakness in the security of cloud data is that, the provision of physical security controls is impossible. As a result, strong access control and substantiation becomes very important for providing effective security.

## Introduction

In today's world the improvement and advancement in the technology make the world strong but it also some dark side. There are some of the peoples who are Unsocial with the use of technology and they create harmful effects on our life.

According to survey of a reputed company with the advancement of Information technology there are access in the possibility of cyber-attacks. Cyber-attacks are the attacks in which a person using an information of another person. Information like his online bank details, Transaction details, Transaction passwords etc. and use them for his benefit without notify the account holder it comes in to category of cyber Attacks. Due to this the account holder face a very big loss whether the loss related to their money, his personal details etc.
To overcome these type of disasters we work on a process in which multiple security checks is happened. Due to this we minimize the chances of data lost. For maintaining the good secure access on online transactions we use Secured Keyboard process it offers the best way for this requirement. Based on Multiple Security Checks it can be implemented on secure online transactions.
This software packages should also work with Secure Electronic Transfer, Secure Socket Layer, Public Key Infrastructure and Secure Ecommerce protocol technologies for encryption of data transmissions. Online Transactions operates on Internet or intranet.

## Related Work

1] In today's world the improvement and advancement in the technology make the world strong according to the technology but there is also there is some dark side. There are some of the peoples who are Unsocial with the use of technology who make us stronger.

Now come to the OTP technique it is simple but sophisticated but day by day achievements in the technology of smart phones or data transfer we have to face the OTP Process to secure the our personal data from the unsocial peoples who misuse the information for their benefits.
Let us take an example If we had to do some transactions with our bank whether we use M-Banking, E-Banking and when we initiates the desired transaction we get an OTP on our registered mobile number via SMS and we sends back the OTP within a short period to complete the cycle. To avoid any possible attacks like phishing, man-in-the middle attack, malware Trojans, the OTP must be secured. In order to provide a reliable and secure mode of online transactions without any compromise to convenience, a reliable m-banking authentication scheme that combines the secret PIN with encryption of the one-time password (OTP) has been developed in this paper.
The combination of PIN with OTP provides authentication and security.
The proposed scheme provides security even if any disputes arise due any possible attacks like internet hacking or mobile thefts. The main objective of this paper securing OTP using Fiestal Network Process. By using this method we can easily change the size of the input we provide. The sub-Keys are generated in each round due to this cascading iteration is produced. If we use more round of encryptions it is difficult to crack the OTP.
2] In this research paper different approaches has presented that increases the level of security dimensions using cryptographic techniques. E-commerce portals because day by day e-commerce had created a great impact on the peoples. Most of the peoples buy their goods from E-commerce portals buy online transaction process and due to this it is very risky to maintain the transaction details of the people would be in secure hands. For maintaining the good secure access on E-commerce transaction we use Public Key Infrastructure (PKI) it offers the best way for this requirement. Based on PKI several security services can be implemented for secure E-commerce transaction. E-commerce software packages should also work with Secure Electronic Transfer, Secure Socket Layer, Public Key Infrastructure and Secure Ecommerce protocol technologies for encryption of data transmissions. E-commerce operates on Internet or intranet. Now a days we do lots of transactions whether it is Online Recharge, Fund Transfer, bank transactions and m-commerce etc using smart phones and PDAs which comes handy. Due to this all of the working made easy. Information security has become a very critical aspect of modern communication. When people perform a transaction over Internet, the protection of information against security threats is a major issue. It is an very big issue that how we secure the information of the people they provide. Pretty good privacy can be used to provide authentication and confidentiality to E-commerce security.

3] In this research paper the researchers told about the problem faced by internet banking because it is the thorny issues of trust and security of online Transactions. And we think that a number of majority of customers/Peoples are always worried about the safety of their online Transactions and they are unable to easily trust the web fears that their online transactions might not be safe due to the increasing numbers of online Internet attacks. To overcome this type of Internet attacks now a days a new model for internet banking transactions is represented in this paper. By using this model of

transactions it increases the security and trust over the existing model, by allowing customers and banks have to communicate with each other and sign process transactions online. The main thinking behind the overcome the security issues that it enhances security by use of three-tier, trusted, layered, and secure channel. This model ensures that only liable people have the access to internet bank accounts due to this the information is remain private and unable to modified by third parties and that the transactions made are traceable and verified.4] Now these days all we techies familiar with a term Cloud Computing . It is an internet-based computing, where a set of resources and services such as applications, storage and servers are delivered to computers and devices through the Internet. It incorporates large open distributed system, virtualization, internet delivery of services, dynamic provision of reconfigurable resources and on-demand operations. Cloud Computing is continuously growing and showing consistent growth in the field of computing. But the major challenging task is the security and privacy issues caused by outsourcing of infrastructure. Sensitive data and critical applications and its multi-tenancy nature the explosive growth of cloud computing has made the provision of adequate and effective security challenges. Multi- factor user Authentication is an effective technique for preventing unauthorized access. A major weakness in the security of cloud data is that, the provision of physical security controls is impossible. As a result, strong access control and authentication becomes very important for providing effective security. However, there are still other security issues to be addressed in the future. 5] Today in the present world mostly depends on the exchange of information i.e. the transfer of data in between two or more persons we call it as distributary system. The data is sent to the person is highly confidential so the data distribution is only happened between the distributer and the third party. The data sent by the source must be secured and confidential and must not be reproduced because the data are confidential and highly important. At many points the data is dispatched or copied by unsocial folks who are responsible for the loss of data and other type of damages to the system this type things come under process name data leakage. The term data leakage must be detected in the early stage in order to protect the data from being come in the presence of unsocial individuals. So In this project we deals with the data leakage by using some encryption to the sensitive data and that it cannot be reproduced.

The research deals with the idea of creating a bit pattern on a file at certain location and while the pattern is completed it generates a watermark. Due to this process our data files are safe and protected with unsocial folks. 6] The paper is about the data security of the accidental data leakage it could happened When tenants deploy applications under the control of third-party cloud providers, they must trust the provider’s security mechanisms for inter-tenant isolation, resource sharing and access control. But in some of the cases the accidental data leakage may occur due to misconfiguration or bugs in the cloud platform. To overcome the issues a term CloudSafetyNet (CSN), a lightweight monitoring framework that gives tenants visibility into the propagation of their application data in a cloud environment with low performance overhead. It exploits

the incentive of tenants to co-operate with each other to detect accidental data leakage.

The main purpose of CloudSafetyNet(CSN) that it is an Tag based approach to monitoring data flows is related to information flow control Techniques, encryption and digital watermarking. With the help of this we put a close sense on accidental data leakage and save the data to gone in the wrong hands.7] In this paper researchers research about the cloud security issues in which they talk about the procedure followed by the Austrian government in which the details of the peoples who live there will cross checked and upload on the cloud server. The process is very simple if you are a genuine citizen of the country then u have to apply online for the verification process and when you clear that process you are registered and your eID (Electronic Identification) is generated. The main benefit of this eID system in some situations a centralized deployment approach of MOA-ID may be preferable. We therefore propose a centralized deployment approach of MOA-ID in the public cloud. With the help of this categorized system the loss of data and data leakage is very squat and the trust of the people on this new type of system is good and it always help and create trust while doing online transactions through cloud services. This paper basically an attempt to assimilate private data with privacy leak detection in the context of text mining. There exist a facility to group these documents based on the concept base mining algorithm. The group of documents is always present in the form of hierarchy. When an operator in the role of a subscriber desires to access a document, this request for access will have to go through an authentication procedure based on the Leakage Free Redact able Signature Structure.

All of this information present in the form of cloud user access control list.

A privacy detection leak module which detects privacy leaks depending upon the pattern of previous privacy leaks is also being projected. Due to this the above information is used to update the cloud subscriber access control list and those are responsible for data leakage are prohibited to access the facility. It is an attempt to integrate the privacy preservation with pattern recognition approaches to data drip detection in the context text mining. In the future by integrating pattern recognition as a feature of privacy preservation the cloud service providers will be able to preserve the privacy of the sensitive information being shared.

## Proposed Work

### 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 because it generates a unique Identification code with the help of this only the liable person will have access to the system. And when the secure Keyboard is used the system normal keyboard did not work. It makes the system Liable and Secure

### Knowledge Base Verification System

A knowledge base verification system 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 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.

**Login Process**

When the above two process is completed like, the secure keyboard is connected and you got the access after that the KBVF procedure is occurred. By some of the reason the user unable to authenticate the above process we discuss an auto generated alert message is send to the user registered number that the user would be warned.

And If the User will pass the procedure then an OTP is generated and send to the user registered number. And when the user enter the OTP code and it matched to the system generated code then the user get the Access in the system.

**OTP (One Time Password)**

Now come to the OTP technique it is simple but sophisticated but day by day achievements in the technology of smart phones or data transfer we have to face the OTP Process to secure the our personal data from the unsocial peoples who misuse the information for their benefits.

The main objective of this paper securing OTP using Fiestal Network Process By using this method we can easily change the size of the input we provide. The sub-Keys are generated in each round due to this cascading iteration is produced. If we use more round of encryptions it is difficult to crack the OTP

## Conclusion

Cloud Storage security has become a very serious phase in distributed communication system. Data Privacy, data integrity, data confidentiality are main areas where we need strong security because there are many techniques used by hackers on internet which hack the system and abuse the system resources. The protection of data, system and information against security threats is a major issue. In this research paper we are working on various approaches that increases the level of security dimensions. The main fault in the security of cloud storage is that, the establishment of physical security controls is difficult. Therefore a powerful access control and authentication play a very important role for providing effective security. In this paper, we discover the feasibility of introducing physical, virtual and knowledge based authentication for cloud access control as many factor increase the verge for successful attacks.

**Future Work**

Cloud computing is a fast developing technology that deals an extensive variety of profits to minor and intermediate initiatives. But safety, secrecy and belief are the main anxieties avoiding the mass acceptance of cloud. A cloud environment that delivers various facilities and hosts numerous resources can be protected only by permitting an authentic user to access the resources. Hence strong user authentication mechanisms limiting illegitimate access are the key obligation for obtaining cloud. A user verification device intended for cloud should be solid enough to keep cloud from several conceivable authentication attacks. This work surveys the validation attacks on cloud and the corresponding alleviation measures.

## REFERENCES

1] International Journal of Innovative Research in Computer and Communication Engineering
(An ISO 3297: 2007 Certified Organization)
Vol. 2, Issue 10, October 2014
Copyright to IJIRCCE www.ijircce.com 6192
OTP Encryption Techniques in Mobiles for Authentication and Transaction Security

2] IJCSI International Journal of Computer Science Issues, Vol. 9, Issue 2, No 1, March 2012 ISSN (Online): 1694-0814
Cryptography Based E-Commerce Security: A Review ALP: An Authentication and Leak Prediction Model for Cloud Computing Privacy ,Mohammad Farhatullah Department of CSE Dr.L.Bullayya College of Engineering for Women Visakhapatnam, India calmcview@gmail.com

3] ISBN 978-952-5726-07-7 (Print), 978-952-5726-08-4 (CD-ROM)
Proceedings of the Second Symposium International Computer Science and Computational Technology (ISCSCT '09)
Building Trust and Security for Internet Banking Services
Huangshan, P. R. China,Three-Tier Security Model for E-Business:

4] Deepa Panse Assoc. Prof. CSE, P. Haritha Asst. Prof. CSE
International Journal of Advanced Research in Computer Science and Software Engineering Research Paper Multi-factor Authentication in Cloud Computing for Data Storage Security Dept. GCET, Keesara JNT University, Hyderabad

5] Sandilya Pemmaraju, V. Sushma & Dr. K. V. Daya.Sagar
Global Journal of Computer Science and Technology: BCloud and Distributed Volume 14 Issue 3 Version 1.0 Year 2014
Type: Double Blind Peer Reviewed International Research Journal
Publisher: Global Journals Inc. (USA)
Online ISSN: 0975-4172 & Print ISSN: 0975-4350
Data Leakage Detection using Cloud Computing

6] CloudSafetyNet: Detecting Data Leakage between Cloud Tenants
Christian Priebe,Divya Muthukumaran,Dan O'Keeffe.TU Braunschweig,Imperial College London,Imperial College London

7] Bernd Zwattendorfer and Daniel Slamanig,On Privacy-Preserving Ways to Porting the Austrian eID System to the Public Cloud,Institute for Applied Information Processing and Communications (IAIK), Graz University of Technology (TUG), Inffeldgasse 16a, 8010 Graz, Austria {bernd.zwattendorfer, daniel.slamanig}@iaik.tugraz.at