IOSR Journal of Engineering (IOSRJEN) **www.iosrjen.org**
ISSN (e): 2250-3021, ISSN (p): 2278-8719
Volume 12, PP 64-68

Two Way Authentication Protection for Cloud Storage System

Amit Choudhary, Akshay Mohite, Ravindra Chavan, Sejal D'Mello
(Department of Information Technology, Atharva College of Engineering/Mumbai University, India)

Abstract: *To design a protected authentication protocol while considering the various kinds of aspects in system to observe user's behaviour and to make convenient as well as user friendly protocol is difficult. Involving human in authentication protocols, while promising, is not easy because of their limited capability of computation and memorization. Therefore, relying on users to enhance security necessarily degrades the usability. We demonstrate new technique of authentication using visualization which can enhance not only the security but also the usability of authentication. To that end, we propose two visual authentication protocols: one is a login id-password protocol, and the other is a QR code-based authentication protocol*
Keywords – *Authentication, computation, protocols, security, visualization.*

I. Introduction

1.1 Need

The ever-increasing amount of personal or sensitive data stored in a cloud data storage needs to be protected, since losing it is a very serious problem. As their popularity increases, cloud storage is becoming an option for user in keeping their data online, it poses a lot of security threats and the challenges of protecting their data from being hacked. Human user's involvement in the security protocol is sometimes necessary to prevent this type of attacks but humans are not good at complicated calculations and do not have a sufficient memory to remember cryptographically strong keys and signatures. Thus, usability is an important factor in designing a human-involving protocol.

1.2 Problem Statement

Existing Authentication Systems take more than enough amounts of details from user. Also, user has to remember considerable amount of login details and large passwords which are difficult to remember. The usability of the system gets deteriorated as provision for high security is made available. The User Experience has to be efficient and understandable. No overhead should be caused at user's side. Remembering of long passwords every time should be avoided. Also not much of user's time should be taken for authentication. High Security has to be provided without compromising with the usability.

1.3 Aims and Objectives

Our approach to solving the problem is to introduce an intermediate device that bridges a human user and a terminal. Every interaction between the user and an intermediate helping device is visualized using a Quick Response (QR) code. The goal is to keep user-experience the same as in legacy authentication methods as much as possible, while preventing key logging attacks. More specifically, our approach visualizes the security process of authentication using a Smartphone aided augmented reality.

The visual involvement of users in a security protocol boosts both the security of the protocol and is re-assuring to the user because she feels that she plays a role in the process. To securely implement visual security protocols, a Smartphone with a camera is used. Instead of executing the entire security protocol on the personal computer, part of security protocol is moved to the Smartphone. This visualization of some part of security protocols enhances security greatly and offers protection against hard-to-defend against attacks such as malware and key logging attack, while not degrading the usability. Other objectives are to provide an easy interface and reducing user overhead for remembering many passwords. It will also avoid key logging &not rely entirely on single entity and introduce another entity to enhance security.

1.4 Application &Scope

Besides the security of an authentication protocol, both usability and deployability are equally important and critical for the acceptance of any protocol in modern computing settings. Bonneau et al. have developed 25 different metrics for evaluating such aspects in an authentication scheme to compete with the existing password-based authentication that is well-accepted in practice. Furthermore, while those metrics are ideal, and the best authentication scheme in the literature does not address many of them, they are fairly generic to benchmark different designs and to compare them based on their merits. For that, the authors provided an extensive comparison and study of 38 schemes based on those metrics. Here, we benefit from this study in understanding our protocols in the context of the related works.

We outline some of the merits based on the common features our schemes share with other works, and some others based on the prior user studies and security analyse. The reader is referred to for further details on

the definitions those metrics, and how they apply to the various authentication mechanisms in the literature. We summarize how our protocols perform on those metrics, and thus how they compare to other protocols in the literature. We limit our attention to the baseline, the password-based authentication, and a few phone based authentication protocols. Our design is security-rich, and its security features are discussed earlier to support the marked merits. Finally, for deployability, our system relies on an intensive user study that provides an obvious merit of its use against those metrics.

Our protocols are generic and can be applied to many contexts of authentication. Some of the Applications:

i) Banking System
ii) E-Commerce System
iii) E-Governance System
iv) Login Security
v) Securing Transactions
vi) 2. Review of Literatures

II. Review of Literatures

2.1 Two-Factor Data Security Protection Mechanism for Cloud Storage System

This work was carried out in 2016 by Joseph K. Liu, Kaitai Liang, Willy Susilo, Jianghua Liu, and Yang Xiang with an aim to Two-Factor Data Security Protection Mechanism for Cloud Storage System. The study shows that they used cryptography for double encryption techniques. In this paper, they proposed that two-factor data security protection mechanism with factor revocability for cloud storage system. this system allows a sender to send an encrypted message to a receiver through a cloud storage server. The sender only needs to know the identity of the receiver but no other information (such as its public key or its certificate). The receiver needs to possess two things in order to decrypt the cipher text. The first thing is his/her secret key stored in the computer. The second thing is a unique personal security device which connects to the computer. It is impossible to decrypt the cipher text without either piece. More importantly, once the security device is stolen or lost, this device is revoked. It cannot be used to decrypt any cipher text. This can be done by the cloud server which will immediately execute some algorithms to change the existing cipher text to be un-decrypt able by this device. This process is completely transparent to the sender. Furthermore, the cloud server cannot decrypt any cipher text at any time. This security and efficiency analysis show that our system is not only secure but also practical [1].

2.2 A Secure Authentication Protocol using HOTP on USB Storage Devices

This work was carried out in 2014 by Suratose Tritilanunt, Napat Thanyamanorot, and Nattawut Ritdecha with an aim to A Secure Authentication Protocol using HOTP on USB Storage Devices. The external storage using a universal serial bus (USB) communication becomes the most popular use for storing digital data. Application such as evidence acquisition in digital forensic area needs external storage devices that are portable, high speed of data transfer, and easy to use for collecting digital data from suspect computers. Apart from these advantages of USB storage devices, they do not have a built-in function to authenticate users. If unauthorized users obtain this device with some utilities installed in it, they might use it as a weapon to attack or steal valuable information from anyone. To avoid this situation, this paper proposes a two-factor authentication technique to solve such problem, as well as to limit the software usage in which users can run it inside that assigned device only. That means no unauthorized users can make a copy version and distribute it to other devices and run the software. The result from the experiment shows that the proposed authentication protocol is able to achieve all goals of this paper [2]

2.3 Enhanced Security for Multi-Cloud Storage using Cryptographic Data Splitting With Dynamic Approach

This work was carried out in 2014 by Balasaraswati V.R.,Manikandan.S with an aim to Enhanced Security for Multi-Cloud Storage using Cryptographic Data Splitting with Dynamic Approach. The study shows that the use of cloud computing has increased rapidly in many organizations. Security is considered to be the most critical aspects in a cloud computing environment due to the sensitive information stored in the cloud for users. The goal of cloud security is mainly focused on the issues related to the data security and privacy aspects in cloud computing. This multi cloud model which is based on partitioning of application system into distinct clouds instead of using single cloud service such as in Amazon cloud service .It will discuss and present the cryptographic data splitting with dynamic approach for securing information. The metadata information is stored in private cloud. This approach prevents the unauthorized data retrieval by hackers and intruders. The results and implementation for the new proposed model is analyzed, in relation to addressing the security factors in cloud computing [3].

III. System Design

3.1 System Block Diagram

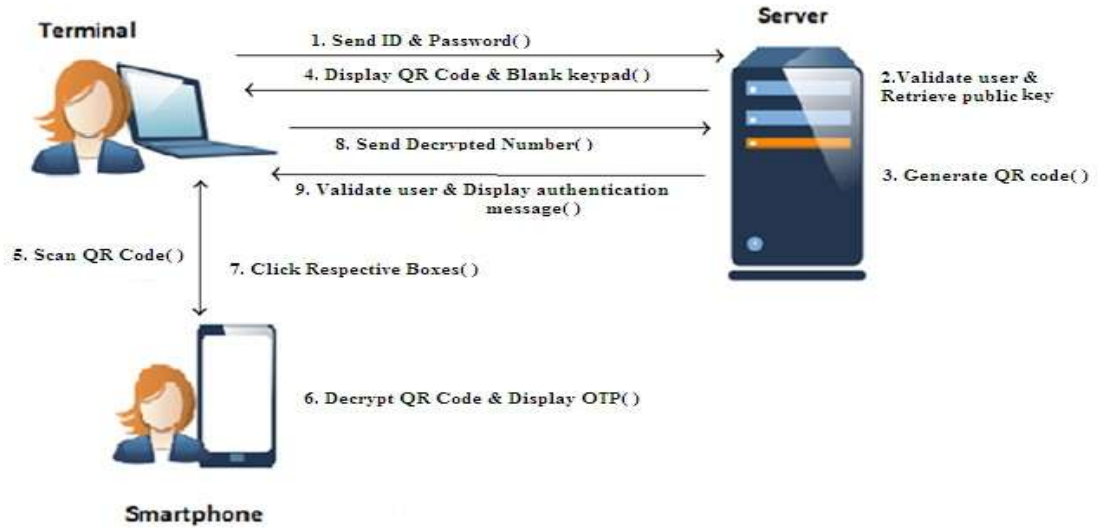

Figure 3.1 System Block Diagram

3.1.1 Terminal:

A user's terminal such as a desktop computer or a laptop, by using the user can log in to the server. When server generates QR code, then the QR code and blank keypad is displayed on terminal prompting the user to click on respective blank boxes. We assume that Keylogger is installed on terminal. We also assume that, the channel between the server and the user's terminal is secured with an SSL connection.

3.1.2 Server:

Server is the system entity, which performs back-end operations by interacting with the user (terminal). Using encryption, Server generates QR code and blank keypad when valid user tries to connect it and display them on the terminal. We assume that the server is secured by every means and is immune to every attack by the attacker.

3.1.3 Smartphone:

The user has a Smartphone, which is equipped with a camera. Smartphone acts like a bridge between the server and the terminal. Smartphone captures QR code displayed on terminal and decrypts randomized OTP. It also stores a public key certificate of the server for digital signature verification. Verification is performed by the Smartphone to avoid any man-in-the-middle attack by the terminal. Smartphone actually in our system, we assume that there is no direct channel between the server and the Smartphone.

3.2 Control Flow Diagram

This Figure 3.2 shows the sequence of control flow for authentication purpose. This shows proper steps in diagram which help to understand the process easily.

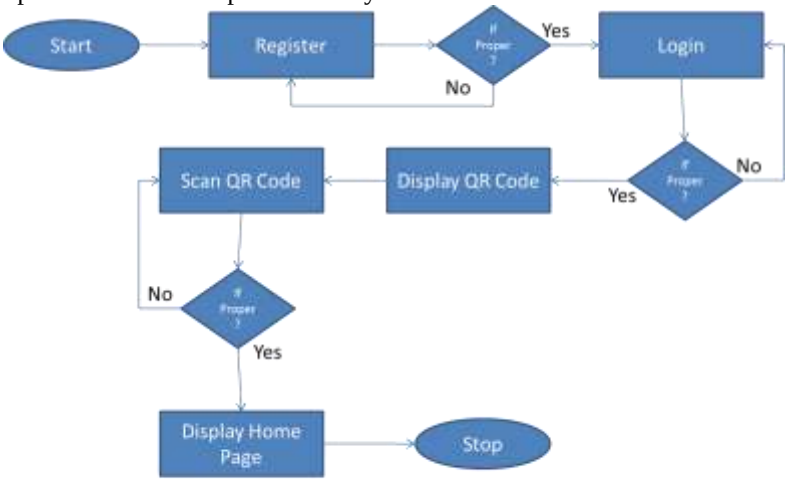

Fig. 3.2 : Control Flow Diagram

3.3 Use Case Diagram

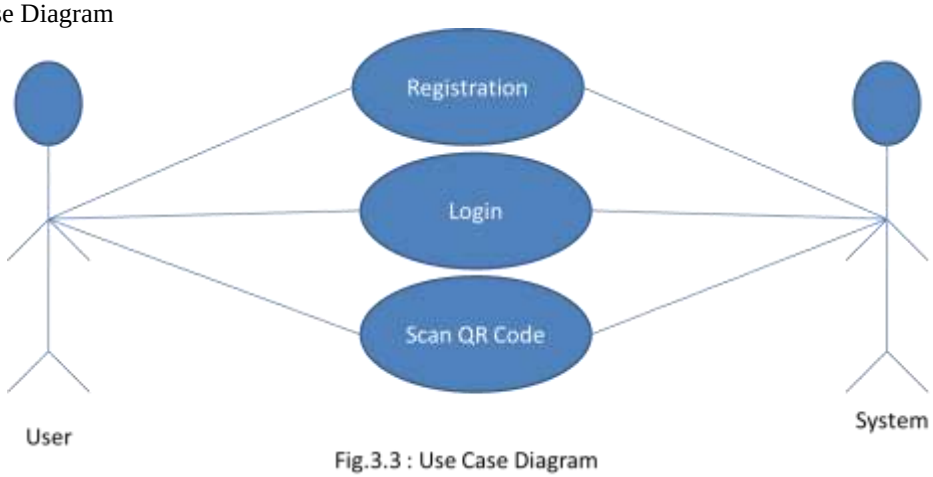

Fig.3.3 : Use Case Diagram

This Figure 3.3 shows the user & system relation accordingly the step wise manner. Initial step is registration process the the login authentication by admin to give authorisation.Terminal step is verification of QR code automatically generate on screen in step 2 authentication by user registered mobile.

3.4 Sequence Diagram

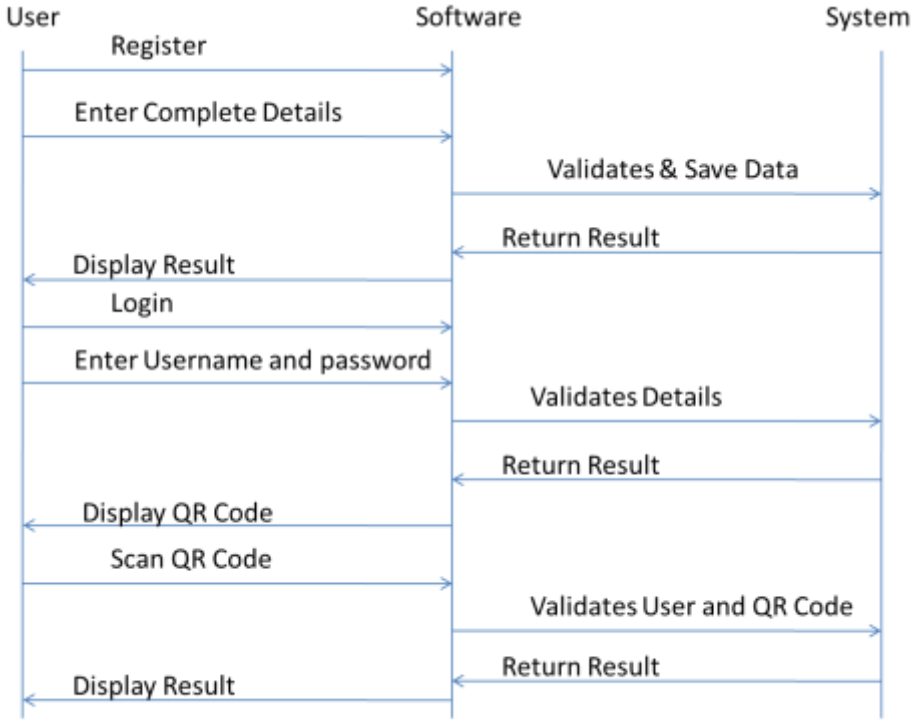

Fig.3.4 : Sequence Diagram

IV. Expected Output

This approach will give new technique of protection to authentication protocol. This two-step authentication provide security form intruders & also from any threats. This will provide protection to large database & cloud storage. This will enhance the use of cloud storage on a large scale.

Along with all these features, the overall results which are expected from the system are as follows:

This will prevent storage from data leakage or any passive attacks. A user-friendly application for owner to prevent large database by strong authentication protocol.

V. Conclusion

Thus, we proposed two visual authentication protocols: One is a login protocol, and the other is a QR-based authentication protocol. Through rigorous analysis, we verify that our protocols are immune to many of the challenging authentication attacks applicable in the literature. Furthermore, using an extensive case study on a prototype of our protocols, we highlight the potential of our approach for real-world deployment: we are able to achieve a high level of usability while satisfying stringent security requirements. In future, this authentication protocol can be used in many system to give efficient protection. Due to this efficient authentication protection, it give enhancement to use of cloud storage as much as possible.

VI. Future Scope

This authentication protocol is can be implement in various technique & also in various field. In future, it can be implement in personal database as well as in large database or big data. New technique may implement or enhance the authentication protocol which will prevent database from hackers by all possible ways. This authentication protocol can be implement by different algorithm which will improve efficiency & reduced the implementation cost.

Acknowledgement

It gives us great pleasure in presenting this paper titled: "Two Way Authentication Protection for Cloud Storage System".

We express our gratitude to our project guide Prof. Sejal Demello, who provided us with all the guidance and encouragement and helped us in finding our mistakes and improving it. We also would like to deeply express our sincere gratitude to Project coordinators.

We are eager and glad to express our gratitude to the Head of the Information Technology Dept. Prof. Neelima Pathak, for her approval of this project. We are also thankful to her for providing us the needed assistance, detailed suggestions and also encouragement to do the project.

We would like to deeply express our sincere gratitude to our respected principal Prof. Dr. Shrikant Kallurkar and the management of Atharva College of Engineering for providing such an ideal atmosphere to build up this project with well-equipped library with all the utmost necessary reference materials and up to date IT Laboratories. We are extremely thankful to all staff and the management of the college for providing us all the facilities and resources required.

References

[1] Joseph K. Liu, Kaitai Liang, Willy Susilo, Jianghua Liu, and Yang Xiang, "Two-Factor Data Security Protection Mechanism for Cloud Storage System," IEEE Transactions on Computers, Vol. 65, pp. 1992-2004, June 2016.

[2] Suratose Tritilanunt, Napat Thanyamanorot & Nattawut Ritdecha, "A secure authentication protocol using HOTP on USB storage devices," International Conference on Information Science, Electronics and Electrical Engineering , Vol. 3, pp. 1908-1912, November 2014.

[3] Balasaraswati V.R., Manikandan.S , "Enhanced Security for Multi-Cloud Storage using Cryptographic Data Splitting with Dynamic Approach," International Conference on Advanced Communications, Control and Computing Technologies , Vol. 14, pp. 1190-1194 January 2015.

[4] C.-K. Chu, S. S. M. Chow, W.-G. Tzeng, J. Zhou, and R. H. Deng,"Key-aggregate cryptosystem for scalable data sharing in cloud storage," IEEE Trans. Parallel Distrib. Syst., Vol. 25, pp. 468–477, Feb. 2014..

[5] H. C. H. Chen, Y. Hu, P. P. C. Lee, and Y. Tang, "NCCloud: A net-work-coding-based storage system in a cloud-of-clouds," IEEE Trans. Comput., Vol. 63, pp. 31–44, Jan. 2014.

[6] L. Ferretti, M. Colajanni, and M. Marchetti, "Distributed, concurrent, and independent access to encrypted cloud databases," IEEE Trans. Parallel Distrib. Syst., Vol. 25, pp. 437–446, Feb. 2014.

[7] Y. H. Hwang, J. K. Liu, and S. S. M. Chow, "Certificate less public key encryption secure against malicious key attacks in the standard model," in J. UCS, Vol. 14, pp. 463–480, June 2008.

[8] J. K. Liuand D. S. Wong, "Solutions to key exposure problem in ring signature," in Int. J. Netw. Security, Vol. 6, pp. 170–180, Jan 2008.

[9] Y. Zhu, G.-J. Ahn, H. Hu, S. S. Yau, H. G. An, and C. Hu, "Dynamic audit services for outsourced storages in clouds," IEEE Trans. Services Comput., vol. 6, pp. 227–238, Apr.–Jun. 2013.

[10] B. Libert and D. Vergnaud, "Unidirectional chosen-cipher text secure proxy re-encryption," IEEE Trans. Inf. Theory, Vol. 57, pp. 1786–1802, Mar. 2011.