A novel Authentication mechanism for cloud storage based on Manual Substitution Cipher

Drishti Soner
Dept. Of Computer Science and Engineering
Medi-Caps Institute of Technology & Management
Indore, (M.P.)

Dr. Pankaj Dashore
Associate Professor
Dept. Of Computer Science and Engineering
Medi-caps Institute of Technology & Management
Indore, (M.P.)

Abstract - Cloud computing is a popular topic across the IT industry. There are various technologies that have been implemented for increasing the cloud data security but they are not efficient. Various malicious activities from illegal users have threatened in cloud technology such as data misuse, inflexible access control and limited monitoring. The occurrence of these threats may result into damaging or illegal access of critical and confidential data of users. Although there are various authentication schemes have been implemented for the security of these data but either they are too much complex or they require huge network resources. In this paper we introduce a new methodology for providing security in terms to authentication for stored data in clouds by using Manual Substitution Cipher.

Keywords - Authentication, Security, Manual Substitution Cipher.

I. INTRODUCTION

Cloud as defined by NIST: "Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. [1]" This cloud model is composed of five essential characteristics, three service models, and four deployment models. Essential Characteristics are as follows:

- **On-demand self-service:** Consumers are able to use cloud service providers, which does not require human interaction. According to need consumer can change cloud services through online control panel or direct with the provider. Consumer can add or delete users and it can change storage network and software.
- **Broad network access:** All the recourses of cloud computing are accessible over the network. It supports heterogeneous thick or thin client platform such as mobile phones, tablets, laptops and workstations.
- **Resource pooling:** Computing resources provided by cloud providers are pooled to serve multiple clients, customers or tenants with provisional and scalable services. At the same time multiple users can use data within the business management software hosted in the cloud at the same time and from any location. It ensures location transparency.
- **Rapid elasticity:** Elasticity means the ability to scale resources as needed. The cloud is scalable and flexible to suit business needs. It gives flexibility to add or remove users, software features and other resources quickly and easily.
- **Measured service:** Affordable nature of cloud says that consumer only pay for what they use. Consumer and cloud provider can measure bandwidth, processing, storage level and active user accounts. Resource uses can be controlled, monitored and reported from consumer as well as provider's side which provides transparency.

II. PREVIOUS WORK

Chia-Sheng Tsai and Cheng-I Hung [2] had designed a system that uses a "Bluetooth mobile device to unlock doors in a fully automatic process with the possibility to reconfigure the system to work in semi-automatic mode to get the approval of the user if he input a PIN code as additional security procedure."
In this paper [8] authors "Sushma Verma, Saibal Kumar Pal and S.K. Muttoo had developed a new tool for securing the information at rest in Android Platform that uses a lightweight authenticated encryption algorithm, Hummingbird-2, that is believed to be resistant to most of the standard attacks on block ciphers and stream ciphers."
In this paper [11] authors "Nathan L. Gross and Willie K. Harrison had analyzed the utility of one of the most robust attacks against the simple substitution cipher when the cipher text is obtained by the eavesdropper as the output of a symmetric discrete memory-less channel. The utility of the attack algorithm was presented as a function of channel mutual information in the case of noisy cipher text, and the length of the observed ciphertext in the case of noise-free ciphertext. author has also given new technique for the encryption and decryption process."
In this paper [14], a novel group key management scheme is proposed by Susmita Mandal and Sujata Mohanty with perfect forward secrecy. "The goal of this paper was to prevent from compromise of any key exchange among n-parties who shares a common secret over an insecure network. The Authors state that any attacker can not reveal the short term group key even if the long term keys are accidently leaked or compromised."
In this paper [15] author "Nikhil Agrawal, Manoj Kumar and Dr. M.A. Rizvi has explained that some of the existing transposition techniques for creating a cipher text corresponding to the given plain text."
In this paper [16] authors "Faraz Fatemi Moghaddam, Shiva Gerayeli Moghaddam, Sohrab Rouzbeh, Sagheb Kohpayeh Araghi, Nima Morad Alibeigi and Shirin Dabbaghi Varnosfaderani proposed a scheme according to the challenging issues during the user authentication and access control process in cloud-based environments. In the proposed scheme client-based user authentication agent was introduced to confirm identity of the user in client-side. Furthermore, a cloud-based software-as-a service application was used to confirm the process of authentication for un-registered devices.

III. PROPOSED ARCHITECTURE

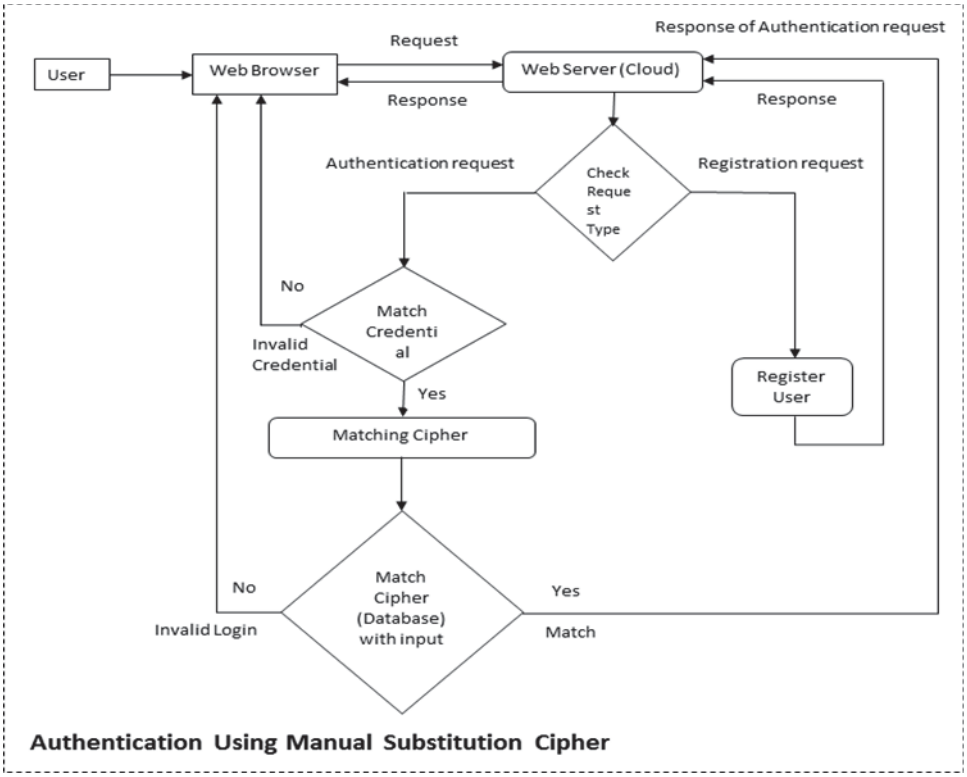

Figure 1: Architecture of proposed algorithm

As shown in figure 1 the proposed architecture first registration is done by the user. Based on this registration details the random pattern for login phase is generated which is offered to the user when he login in the future. These patterns are so random that they are not repeated for three times & when a user enters wrong patterns up to three times then the login is blocked. This authentication approach is completely secure as compared to the previous approaches of authentication.

IV. ALGORITHM

The algorithm can be divided in two sub parts Registration & Login.

1. Registration:-
   - i. User fills required details for registration like User Name, Password and stores it in database.
   - ii. After that user chooses one alphabet from list of A to Z alphabet and inserts numeric value of its choice with respect to the alphabet.
   - iii. To complete the registration step ii is repeated four times, every time alphabets chosen in previous steps are removed from list.
2. Login:-
   - i. User fills user name and Password.
   - ii. Systems checks user name and password in database if match is found then step iii is followed otherwise Step i is followed.
   - iii. List of stored manual cipher patterns is retrieved from the database (8 elements as per registration phase i.e. 4 alphabets & their four numeric values) then a random number is generated and divided by 8. Then a pattern is chosen from list based on the reminder that we got after dividing the random number by 8 i.e. if reminder is 4 then choose fourth element of list.
   - iv. Check the cipher pattern that are not used in last three times, if the current pattern matched any one of last three times then repeat step iii, if no then go to step v.
   - v. User inserts numeric value or alphabet as prompted by system with respect to step iii.
   - vi. If match is found then authentication is successful otherwise user is send back to step i to try again.

V. RESULT ANALYSIS

We had implemented the proposed approach using .NET & SQL server to get results. Refer table 1 & figure 2 for result analysis.

Identity disclosure attack: Identity disclosure, in which the identity is linked to a particular individual.

Replay attack: A replay attack is a network attack in which attacker copies stream of messages between two parties (sender and receiver) and resend it to one or more parties.

Table 1: Prevention from various attacks

Attacks	Status
Identity disclosure attack	**YES**
Replay attack	**YES**
Password based attack	**YES**
Identity Spoofing	**YES**

Outsider attack	**YES**
Man-in the middle attack	**YES**
Eavesdropping	**YES**
Insider attack	**YES**

Insider attack: An "insider attack" is an attack initiated by an entity inside the security perimeter, i.e., a person with authorized system access maliciously attacks on network.

Man in the middle attack: It is type of eavesdropping attack. Attacker secretly relays and possibly alters the communication between two parties who believe they are directly communicating with each other.

Eavesdropping: Eavesdropping is the unauthorized real-time interception of a private communication. The term eavesdrop derives from the practice of actually standing under the eaves of a house, listening to conversations inside.

Password-based attack: An attack in which repetitive attempts are made to duplicate a valid logon or password sequence.

Identity spoofing: It occurs when the attacker determines and uses an IP address of a network, computer, or network component without being authorized to do so.

Outsider attack: An unauthorized entity is trying to steal data or enter into the network for malicious attack.

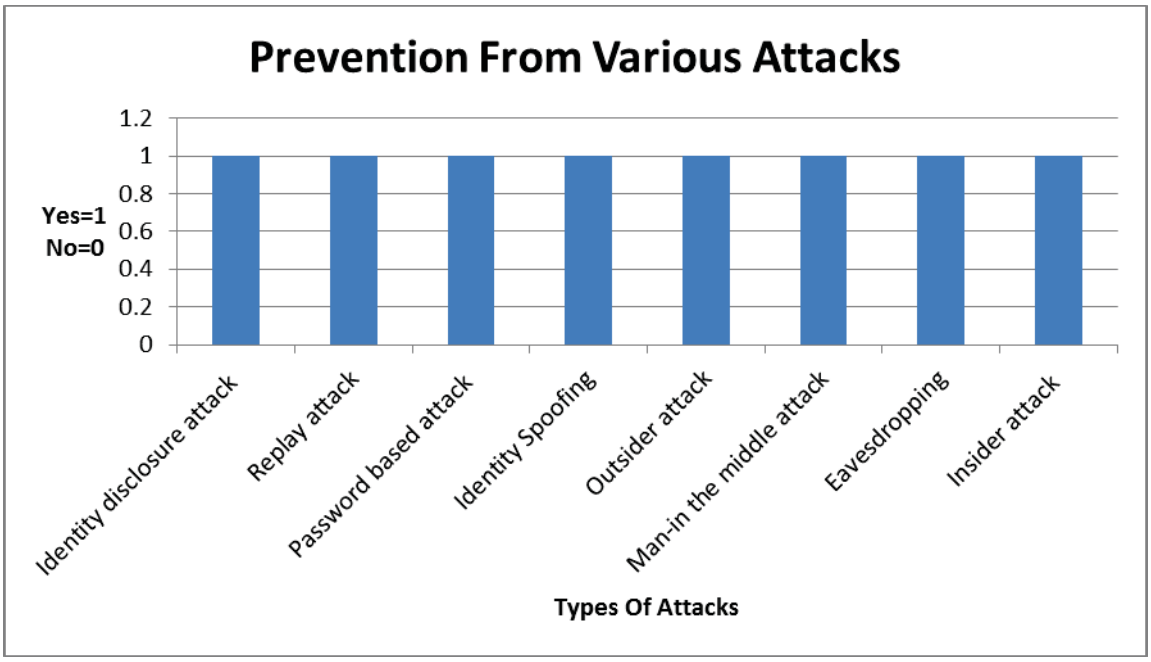

Figure 2: Prevention from various attacks

COMPARISON OF PROPOSED APPROACH WITH OTP, FINGER PRINT

The proposed approach is compared with OTP & Finger Print recognition systems used for authentication. The comparison is based on various dependency parameters as mentioned on Table 2 & figure 3. The value 1 represents 'YES' & value 0 represents 'NO'

Table 2: Comparison of Proposed Approach

Dependency Parameter	OTP	Finger Print	Proposed Approach
Internet	1	1	1
Extra Hardware	1	1	0
Mobile Network	1	0	0
Failure due to third party	1	1	0

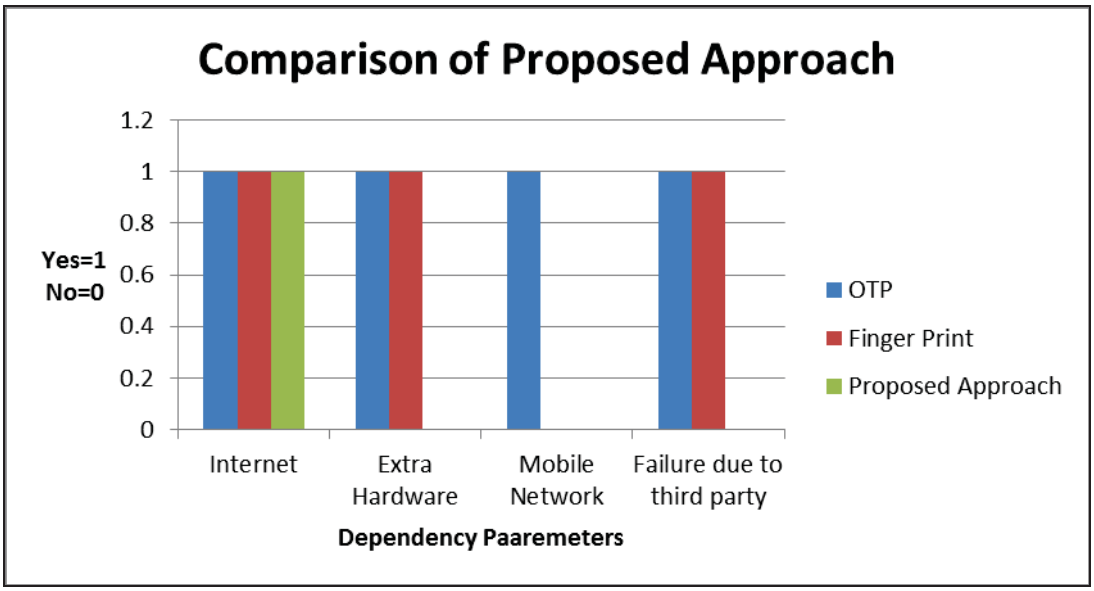

Figure 3: Comparison of Proposed Approach

VI. CONCLUSION

The proposed approach mentioned in the paper demonstrated a new authentication mechanism which uses manual substitution cipher for authentication of users. Thus we presented a new idea for the cloud storage security. Proposed work using the manual substitution cipher for authentication which gives better results as compared to previous work in terms of efficiency and security.

REFERENCES

[1] Peter Mell and Timothy Grance, "The NIST Definition of Cloud Computing", NIST Special Publication 800-145, September 2011.
[2] Chia-Sheng Tsai and Cheng-I Hung presented paper entitled "An Enhanced Secure Mechanism of Access Control" at IEEE in 2010.
[3] Edmond Holohan and Michael Schukat presented paper entitled "Authentication using Virtual Certificate Authorities" at IEEE in 2010 Ninth IEEE International Symposium on Network Computing and Applications.
[4] Sridhar S and Vimala Devi.K presented paper entitled "Nested Mechanism for Mutual Authentication" at IEEE in 2011.
[5] Yanan Sun, Xiaohong Guan, Ting Liu and Yu Qu presented paper entitled "An Identity Authentication Mechanism Based on Timing Covert Channel" at 2012 IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications.
[6] Liu Yang, Rongrong Ni, Yao Zhao presented paper entitled "Segmentation-based Image Authentication and Recovery Scheme Using Reference Sharing Mechanism" at 2012 International Conference on Industrial Control and Electronics Engineering.
[7] Shivraj V L, Rajan M A and Balamuralidhar P presented paper entitled "Secure Personal Authentication through Remote System for E-Transactions (SPARSE)" at IEEE in 2014.
[8] Sushma Verma, Saibal Kumar Pal and S.K. Muttoo presented paper entitled "A New Tool for Lightweight Encryption on Android" at IEEE in 2014.
[9] Vipul Srivastav presented paper entitled "New Approach in Encryption: Magnus Kallus" at IEEE 2014 International Conference on Computing for Sustainable Global Development (INDIACom).
[10] Hadia M. El Hennawy, Alaa E. Omar and Salah M. Kholaif presented paper entitled "NEW PROPOSED STREAM CIPHER Algorithm" at 31st National Radio Science Conference, (NRSC2014), April 28 – 30, 2014, Faculty of Engineering, Ain Shams University, Egypt.
[11] Nathan L. Gross and Willie K. Harrison presented paper entitled "An Analysis of an HMM-Based Attack on the Substitution Cipher with Error-Prone Ciphertext" at IEEE ICC 2014 - Communication and Information Systems Security Symposium.
[12] Khadidiatou Wane Keita and Claude Lishou presented paper entitled "The Impact of Model S-Wane on IPv6" at IEEE in 2014.
[13] Ta Thi Kim Hue, Thang Manh Hoang and Dat Tran presented paper entitled "Chaos-based S-box for Lightweight Block Cipher" at IEEE in 2014.
[14] Susmita Mandal and Sujata Mohanty presented paper entitled "Multi-Party Key-Exchange with Perfect Forward Secrecy" at IEEE 2014 International Conference on Information Technology.
[15] Nikhil Agrawal, Manoj Kumar and Dr. M.A. Rizvi presented paper entitled "Transposition Cryptography Algorithm using Tree Data Structure" at IEEE ICICES2014 - S.A.Engineering College, Chennai, Tamil Nadu, India.
[16] Faraz Fatemi Moghaddam, Shiva Gerayeli Moghaddam, Sohrab Rouzbeh, Sagheb Kohpayeh Araghi, Nima Morad Alibeigi and Shirin Dabbaghi Varnosfaderani presented paper entitled "A Scalable and Efficient User Authentication Scheme for Cloud Computing Environments" at 2014 IEEE Region 10 Symposium.