International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 06 Issue: 04 | Apr 2019 www.irjet.net p-ISSN: 2395-0072

Data Security With Multifactor Authentication

Rushikesh Nikam[1], Aishwarya Gawayi[2], Diksha Gaikwad[3], Aishwarya Adam[4]

[1]*Professor, Dept. of Computer Engineering, New Horizon Institute of Technology and Management, Maharashtra, India*

[2,3,4]*New Horizon Institute of Technology and Management, Maharashtra, India*

Abstract - *In the present digital day with remarkable development in Computer sector, Single factor authentication, e.g. passwords, is no more examined as secure in the World Wide Web. It has never been less difficult in Securing the system and remote access. Simple, obviousand easytoguess passwords, such as names and age, are effortlessly found via computerized secret key gathering programs. Expanded access to information increases weakness to hacking, cracking of passwords and online frauds. In this association the conventional login/password authentication is taken into account inadequately secure for several securitycritical applications such as login to Mailing Accounts, Social Networks, Gadgets, Financial accounts, official secured networks, commercial websites onlineetc. Obliging more than one independent factor increases the difficulty of providing false credentials. Multi-factor authentication proposal guarantee a higher protection level by extending the single authentication factor. This paper focuses on the implementation of Multi-factor authentication methods by using both users friendly traditional Alphanumeric Password and in second factor is the user's smart mobile phone device and a pseudo randomly generated alphanumerical QR code which is used as the onetime password token sent to the user via email and in the third factor the data which is uploads is stored in encrypted format and for gate that data we have to decrypt it which provides more security to stored data. And in this paper we describe the Multi- factor Authentication system design and design implementation. Thus affording an additional OTP via QR code And Encryption and Decryption of data provides extra layer of security.*

Key Words: Data Security, CP-ABE, QR Code, Encryption, Decryption

1. INTRODUCTION

Multi-factor authentication (MFA) is a method of confirming a user's claimed identity in which a computer user is granted access only after successfully presenting two or more pieces of evidence (or factors) to an authentication mechanism: knowledge (something the user and only the user knows), possession (something the user and only the user has), and inherence (something the user and only the user is).Multifactor authentication (MFA) is a security system that requires more than one method of authentication from independent categories of credentials to verify the user's identity for a login or other transaction. Multifactor authentication combines two or more independent credentials: what the user knows (password), what the user has (security token) and what the user is (biometric verification). The goal of MFA is to create a layered defense and make it more difficult for an unauthorized person to access a target such as a physical location, computing device, network or database. If one factor is compromised or broken, the attacker still has at least one more barrier to breach before successfully breaking into the target.

1.1 OTP Algorithm

In order to secure the system, the generated OTP must be hard to guess, retrieve, or trace by hackers. Therefore, it is very important to develop a secure OTP generating algorithm. Several factors can be used by the OTP algorithm to generate a difficulttoguess password. Users seem to be willing to use simple factors such as their mobile number and a PIN for services such as authorizing mobile micro payments, so we propose a Secured Cryptographic algorithm. The unique OTP is generated by the mobile application offline, without having to connect to the server. The mobile phone will use some unique information in order to generate the password. The server will use the same unique information and validate the OTP. In order for the system to be secure, the unique

1.2 Security of Data

The security of the data contents has become a rising issue, the proposed system uses the traditional username password combination to login and authenticate along with multiple layers of security so that there is no compromise on security of the data..RSA algorithm is the most widely used public key cryptography algorithm for encryption and decryption by many vendors today. This is the first generation algorithm that was used for providing data security. It basically is used encrypt and decrypt keys. Its security is based on the difficulty of factoring large integers.

2. CP-ABE Algorithm for Encryption and Decryption

Cipher text-policy attribute-based encryption (CP-ABE) is widely used in many cyber physical systems and the Internet of Things for guaranteeing information security. In the ciphertext-policy attribute-based encryption scheme, each user's private key (decryption key) is tied to a set of attributes representing that user's permissions. When a

ciphertext is encrypted, a set of attributes is designated for the encryption, and only users tied to the relevant attributes are able to decrypt the ciphertext..

Types of multifactor:

The use of multiple authentication factors to prove one's identity is based on the premise that an unauthorized actor is unlikely to be able to supply the factors required for access. If, in an authentication attempt, at least one of the components is missing or supplied incorrectly, the user's identity is not established with sufficient certainty and access to the asset (e.g., a building, or data) being protected by multi-factor authentication then remains blocked. The authentication factors of a multi-factor authentication scheme may include:

- some physical object in the possession of the user, such as a USB stick with a secret token, a bank card, a key, etc.

- some secret known to the user, such as a password, PIN, TAN, etc.

- some physical characteristic of the user (biometrics), such as a fingerprint, eye iris, voice, typing speed, pattern in key press intervals, etc

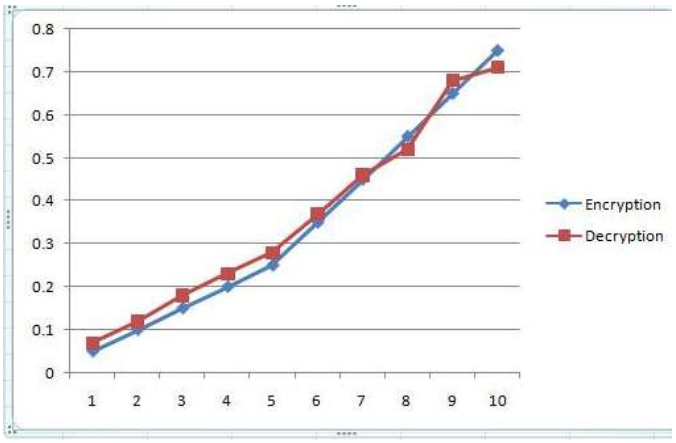

Chart -1: Result

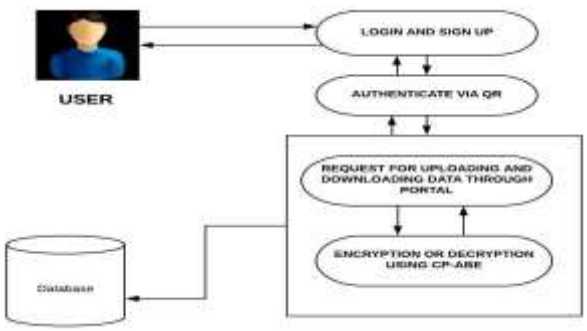

Fig -1 Security Architecture

Procedure for multi-level authentication:

(1)User will login by using its Id and passwords

(2)user have to enter a OTP which is sent on his registered email.

(3)user will perform decryption for downloading data and encryption for uploading the data.

security architecture which consists of three stages of verification process namely normal user personal information encryption and decryption process, encryption process and finally key verification. This three stage encryption process gives more security to user sensitive details also eliminates intermediate attack with efficient manner.

3. CONCLUSION

This System provides a multiple layers of security to the data which is stored on the server. If user want to upload the data or download the data, then user have to go throw for all this security level, and because of this only authorized person can get access to that data. In first stage system provide username and password for login, and in the second stage user gets randomly generated OTP in the form of QR code, which provides more security. in the third stage user can upload data for storing it by using encryption and for downloading a data user have to perform decryption ,and for decryption user must have similar set of key, without valid keys user cannot download data, thus this system provides multiple layers of security to the data stored on the server which minimizes the risk of unauthorized access to the system.

REFERENCES

[1] Ch. Chakradhara Rao and A.V.Ramana DATA SECURITY IN COMPUTING International Journal of Current Trends in Engineering & Research (IJCTER)

[2] Vishal R. Pancholi, Dr. Bhadresh P. Patel Matrushri L.J Gandhi (Bakorvala)and Enhancement of Computing Security with Secure Data Storage using ABE

[3] Sreedhar Acharya B. and Dr. M. Siddappa A Novel Method of Designing and Implementation of Security Challenges in Data Transmission and Storage in Computing International Journal of Applied Engineering Research.