SECURED MESSAGE COMMUNICATION FRAMEWORK USING MULTI-LAYERED AUTHENTICATION MECHANISM

T.PRABHU¹, R.SELVARAJ², T.SATHEESH³
ASSISTANT PROFESSOR/ DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING
TAMILNADU COLLEGE OF ENGINEERING

ABSTRACT

Authenticated key exchange (AKE) is one of the most important applications in applied cryptography, where a user interacts with a server to set up a session key where pre-registered information (aka. authentication factor), such as a password or biometrics, of the user is stored. While single-factor AKE is widely used in practice, higher security concerns call for multi-factor AKE schemes, e.g. combining both passwords and biometrics and device simultaneously. However, in some schemes, security is even weakened in the sense that leakage of one authentication factor will defeat the whole authentication process. Furthermore, an inevitable by-product arises that the usability of the protocol often drops greatly. To summarize, the existing multi-factor protocols did not provide enough security and efficiency simultaneously. Here, we make one step ahead by proposing an efficient authentication method. We define the security model and give the according security analysis. To overcome the security issues proposed method implements textual, graphical, bio-metric and device password to access the user accounts and an efficient AES algorithm for data transaction which is more secured algorithm is used.

KEYWORD: Triple Des, Multi-Factor Key Encryption, VPN, E2FA, TOTP, Unclonable

I. INTRODUCTION

At the time of systems are connected through the network, attacks are possible during transmission time. Network security is a process that is designed to detect, prevent and recover from a security attacks. User authentication is a very important part for many information systems. The authentication service is concerned with assuring that a communication is authentic. It helps to prove that the source entity only has involved the transaction. The key exchange protocols allow two or more parties communication over a public network to establish a common secret key called a session key. Due to their significance in building a secure communication channel, a number of key exchange protocols have suggested over the years for a variety settings. In order to avoid mistakes and impersonations during the process we can use various authentication means. It is often done via the following methods:

- **Textual Authentication** is the most popular way, while quite insecure in some cases. The statistics show that most passwords in use are not so hard to guess.
- **Secret Hardware Key Based Authentication** provides higher security than password with storage space for long secret keys and computation power for authentication. But if it is stolen or lost, the authentication fails completely.
- **Genetic Authentication** utilizes the unique and life-long invariant property of the biometrics. But it is not so reliable.

Combining all these processes together is called the Multi Factor Authentication Key Exchange (MFAKE) protocol.

Functions of MFAKE protocol

For a secured data transaction, before transferring the data few authentication steps are followed. The user needs to complete all the authentication steps to send/receive a data. The authentications steps generally involve three steps. They are the above discussed process, password based textual authentication, a hardware device with a serial key and the unclonable biometric password. These steps are used in order to authenticate the user and for a secured data transaction.

To make the transaction more secured another step implemented called the graphical authentication method. Phishing can be combated by protocols that provide strong, easy-to-use server-to-client authentication.
Password-authenticated can make server-to-client authentication easier and resistant to offline dictionary attacks, and additionally provides a secure key for encryption.

Graphical password is more difficult to defend against. If a user’s computer is compromised by passive spyware that records keystrokes and occasionally transmits this information to an attacker’s server, then the use of one-time passwords may be effective, since a previously used one-time password cannot be used again.

In Biometric passwords are users can never lose their biometrics, and the biometric signal is difficult to steal or forge.

With storage space for long secret keys and computation power for authentication, hardware provides higher security than password.

To reduce the damage caused by compromising an authentication factor, many organizations with high security requirements – such as financial institutions, governments, and corporate virtual private networks (VPNs) – are deploying multi-factor authentication, which depends on a variety of attributes or factors. The factors could include: a long-term password, a set of one-time passwords, a private key, or a biometric. To be effective in practice, factors should have different, complementary natures of compromise. For example, one-time passwords cannot all be compromised unless one obtains the sheet of paper listing all the one-time passwords or the device generating the one-time passwords, whereas a biometric read by a trusted device (such as a secure fingerprint reader) should not be able to be reproduced without the presence of the person in question (or at least their finger).

II. RELATED WORK

The present enhanced fine-grained two-factor authentication (E2FA) access control system framework for accessing internet-based cloud services from cloud data. In our proposed system E2FA get to maintain the framework, a client can access the cloud data based on an encrypted device to connect it PC. It was actualized within the help of client secret key, it cannot get the data from cloud whenever the device is off. That encrypted device uniquely works on one machine only. It will not be handling both the component to develop the security of the framework; in these limited situations the clients are going to have the same type of PC for the cloud data. In encrypted device is protected with enhanced hierarchical identity-based encryption. That comparative analysis is done and presented in this paper.

The User authentication has become a fundamental problem of cloud system. The advantage of internet based cloud services, which contains the ease of accessing resources, reduction of cost and expenditures, increases the efficiency, scalability, and flexibility. In addition to the user authentication it needed to show an OTP. The innovative approach of cloud computing provides more features meanwhile to access any kind of data in that cloud, sometimes you may share sensitive data that data privacy should be maintained.

Two factor authentication is a method which allows the user to protect their data using two layer protection mechanisms. This ensures the data security at higher level. Let us consider the case of an ATM in which for any transaction we need 2FA. Another example is the Biometric system or which we need a thumb impression which is not separable with the pin number which the user possesses. Basically it’s a security system which requires two authentication means. These two means should be of different class or category and their combination should be unique to the user. But is this technology the ultimate solution or their chances of user data being compromised, this paper seeks to answer these questions. The TOTP algorithm utilizes a shared secret key and the current Unix time-stamp to generate a pass code. Generally the time-stamp increases in 30 seconds, so passwords generated close together in time from the same secret key will be equal on both the levels i.e. server and client.

Typically, in a 2FA system: the user enters his login credentials into a server; the server generates an OTP using the time-stamp running locally on the client device. The server can now run TOTP to verify the one-time password entered by the user. Synchronization between the client and the server is important and so the one-time passwords are accepted from time-stamp difference of ±1. Later in this paper we will discuss about the Vulnerabilities, Background, Computation and Weakness and finally an Implementation of the TOTP as a 2FA tool. As times have changed so have the ways of communication and business, with the increase in utilization of the technology in these processes emphasis on cyber security has become discernible.

III. PROPOSED WORK

A. USER REGISTRATION

The User Registration has both the sender and receiver registration process. Initially they have to register for their interaction between them. The sender and receiver registered by using the individual textual passwords. The Registration process is common for both the sender and receiver. During the registration phase the user have to register the hardware security key and their fingerprint. These registered values are stored in database for security verification purposes while the login process.

B. AUTHENTICATION

The authentication process undergoes four steps. Authentication is done after user registration. The four steps are,
1. Textual authentication
2. Graphical authentication
3. Hardware authentication
4. Biometric authentication

TEXTUAL AUTHENTICATION

The user first registers with a simple textual security password and with a serial key. After registration the first steps is to verify whether the user is an authentic user or not, by checking the user name, the textual password and the serial key. This is the first step of authentication.
GRAPHICAL AUTHENTICATION

The graphical password is created by using the information about the sender and receiver and with the help of sessions using in it and is sent to the user registered phone number. These passwords are accessed only in the particular location of the secured image. The graphical password is generated based on the users clicking point which is based on the corresponding \( x \) axis and \( y \) axis value. If the values of the clicking point match with the registered value, only then the user can login and process this system [8]. After finding the coordinates a text box will be displayed and the graphical password should be entered.

BIOMETRIC PASSWORD AUTHENTICATION

The biometrics scheme for the authenticated data is generated. Registered finger print value is checked with the current fingerprint of the person who tries to login. This is done by checking pixel by pixel of the registered fingerprint and current user fingerprint. By using this biometrics the data is being prevented. The sender and receiver perform the data transaction by using biometrics scheme. So the system is full secured.

HARDWARE-BASED AUTHENTICATION

It has storage space for long secret keys and computation power for authentication. Hardware provides higher security than password. Here it is authenticated using a USB device.

C. DATA TRANSMISSION

The two phases in the data transmission are,
1. Data transmitting
2. Data receiving

DATA TRANSMITTING

The sender sends the data to the receiver in the encryption format for the security purpose. Encryption is the most effective way to achieve data security. To read an encrypted file, you must have access to a secret key or password that enables you to decrypt it.

The encryption process is done by AES algorithm. The data’s are encrypted so the unknown person can’t access the files which are sent by sender. These encryptions are known only by the authorized sender. AES is considered one of the most efficient algorithms currently available.

DATA RECEIVING

The receiver accesses the sent data using the session password. Decryption is the process of taking encoded or encrypted text or other data and converting it back into text that you or the computer can read and understand.

The receiver can decrypt and view the original format of the data which has sent by the sender. Authorized person can only decrypt the file using the key. So the file is prevented from unauthorized access.

DATATRANSMISSION: AES ALGORITHM

A comparison of two encryption standards, 3DES and AES is presented. It may seem that DES is insecure and no longer of any use, but that is not the case since the DES and 3DES algorithms are still beyond the capability of most attacks in the present day. However, the power of computers is increasing and stronger algorithms are required to face hacker attacks. AES has been designed in software and hardware and it works quickly and efficiently, even on small devices such as smart phones. With a large block size and longer keys, AES will provide more security in the long term.

The features of AES are as follows –

- Symmetric key symmetric block cipher
- 128-bit data, 128/192/256-bit keys
- Stronger and faster than Triple-DES
- Provide full specification and design details
- Software implementable in C and Java

Operation of AES

AES is an iterative rather than Feistel cipher. It is based on ‘substitution–permutation network’. It comprises of a series of linked operations, some of which involve replacing inputs by specific outputs (substitutions) and others involve shuffling bits around (permutations).

Interestingly, AES performs all its computations on bytes rather than bits. Hence, AES treats the 128 bits of a plaintext block as 16 bytes. These 16 bytes are arranged in four columns and four rows for processing as a matrix –

Unlike DES, the number of rounds in AES is variable and depends on the length of the key. AES uses 10 rounds for 128-bit keys, 12 rounds for 192-bit keys and 14 rounds for 256-bit keys. Each of these rounds uses a different 128-bit round key, which is calculated from the original AES key.

The schematic of AES structure is given in the following illustration –
Encryption Process

Here, we restrict to description of a typical round of AES encryption. Each round comprise of four sub-processes. The first round process is depicted below –

Byte Substitution (SubBytes)
The 16 input bytes are substituted by looking up a fixed table (S-box) given in design. The result is in a matrix of four rows and four columns.

Shift rows
Each of the four rows of the matrix is shifted to the left. Any entries that ‘fall off’ are re-inserted on the right side of row. Shift is carried out as follows –

- First row is not shifted.
- Second row is shifted one (byte) position to the left.
- Third row is shifted two positions to the left.
- Fourth row is shifted three positions to the left.
- The result is a new matrix consisting of the same 16 bytes but shifted with respect to each other.

Mix Columns
Each column of four bytes is now transformed using a special mathematical function. This function takes as input the four bytes of one column and outputs four completely new bytes, which replace the original column. The result is another new matrix consisting of 16 new bytes. It should be noted that this step is not performed in the last round.

Add round key
The 16 bytes of the matrix are now considered as 128 bits and are XORed to the 128 bits of the round key. If this is the last round then the output is the ciphertext. Otherwise, the resulting 128 bits are interpreted as 16 bytes and we begin another similar round.

IV. CONCLUSION

There are many authentication schemes in the current state. Some of them are based on user’s physical and behavioral properties, and some other authentication schemes are based on user’s knowledge such as textual and graphical passwords. Secured message communication frameworks provide a flawless and bleach free data transmission. The data transferred are highly protected and are in an encrypted manner. Only the authorized receiver has the key to decrypt. The authentication schemes used here are highly secured and are betterment to the cryptography in network security. Enhancement can be done in a manner that “Steganography” can be used for encrypting and transferring the data. It is a method of hiding secret message in an image, encrypting the image and transferring it to the authentic receiver. Thus the project “SECURED MESSAGE COMMUNICATION FRAMEWORK USING MULTILAYERED AUTHENTICATION MECHANISM” is flexible and can be enhanced at any time with more advanced features.

REFERENCES


AUTHORS

1. T.PRABHU M.E. IS WORKING AS ASSISTANT PROFESSOR IN DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING AT TAMILNADU COLLEGE OF ENGINEERING. HIS AREA OF INTEREST INCLUDES COMPUTER NETWORKS, CYBER FORENSICS.

2. R.SELVARAJ M.E. IS WORKING AS ASSISTANT PROFESSOR IN DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING AT TAMILNADU COLLEGE OF ENGINEERING. HIS AREA OF INTEREST INCLUDES MOBILE ADHOC NETWORKS, NETWORK SECURITY.

3. T.Satheesh M.E. IS WORKING AS ASSISTANT PROFESSOR IN DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING AT TAMILNADU COLLEGE OF ENGINEERING. HIS AREA OF INTEREST INCLUDES DIGITAL SIGNAL PROCESSING, NETWORK SECURITY.