Chapter 4

ACCESS CONTROL USING MOBILE VERIFICATION SYSTEM FOR CLOUD

4.1. Introduction

Due to the large number of threats that occur in the cyber world, a unique password is not sufficiently protected from these threats. Several examples are available for such threats and attacks on passwords in the literature. Therefore, researchers focused their researchers on strong authentication or multifactor authentication mechanisms against various threats in the cyber world. Recently, the SMS based OTP has become very popular and is commonly used to authenticate and authorize multiple applications over the Internet. To stop fraud and several bouts alongside validation and authorization of business services was introduced based on SMS (OTP). OTP provides a second authentication coefficient when entering any online resource [117], [118], [119]. Out-of-band OTP (OOB) delivery is one of the fastest and easiest ways to provide reliable authentication for any user, anytime and anywhere.

The basic idea of OTP based on SMS is that each account in the system is connected to a mobile phone, and this mobile phone is at the disposal of the owner of this account [120]. Therefore, the owner of the account is the only person who can receive SMS messages sent to the phone number associated with the account. Adding physical ownership to a particular device (mobile phone) associated with a specific online system account makes OTP an important part of a multifactor authentication / authorization system [121].

4.2. SMS Based OTP Password

A unique password / one time password (OTP) is used as an additional factor in authentication applications. OTP are only valid for one authorization or authentication request. To avoid password lists, a convenient way to provide an OTP user is to send it via SMS. The user's telephone number must be registered for the service provided by OTP for authentication or authorization [122]. Figure 4.1 summarizes this basic principle:

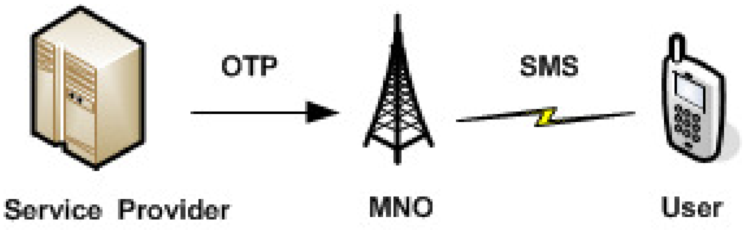


Figure 4.1: SMS OTP example in form of a Mobile TAN

4.2.1. Parties in SMS OTP

- Service provider.
- The second part is the mobile network operator.
- The end user and his mobile phone as a third party. These three parts are shown in figure 4.1
- In some cases, a quarter is involved. The fourth part is an SMS provider that connects a real service provider to mobile networks, offering a simple interface for delivering a text message to a mobile phone [122].

4.3. Architecture of Access Control Mechanism Using Mobile Verification

This research proposed a verification system that uses a mobile device to authenticate a user to a cloud server through a possibly untrusted personal computer (i.e., a client).

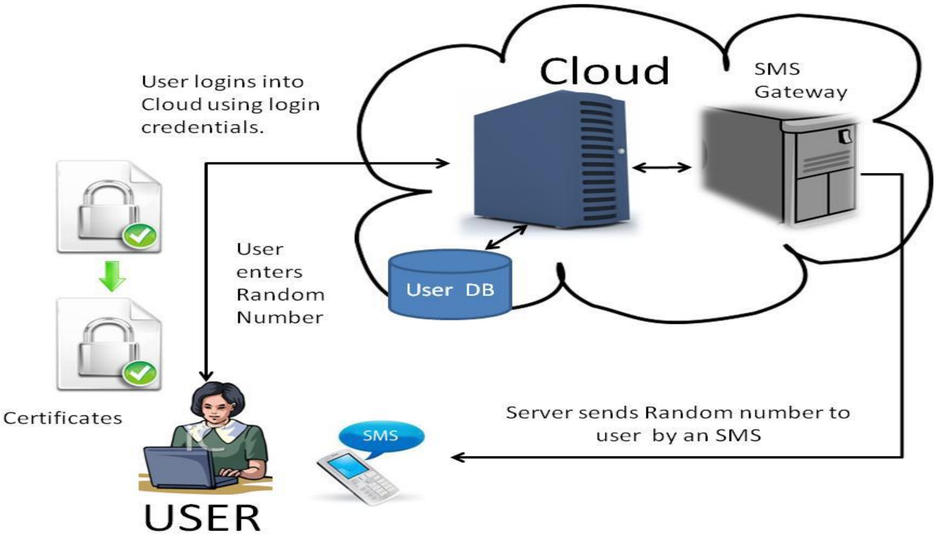

User logins into Cloud using login credentials.
Cloud
SMS Gateway
User enters Random Number
User DB
Certificates
SMS
Server sends Random number to user by an SMS
USER

Figure 4.2: User Authentication Architecture Using Mobile SMS

The first factor is the combination of username and password that are normally required by cloud servers. The second factor is a one-time password that is entered into the client's browser, which is not trusted and is sent to the web server. Our authentication protocol includes the following steps, as shown in figure 4.3:

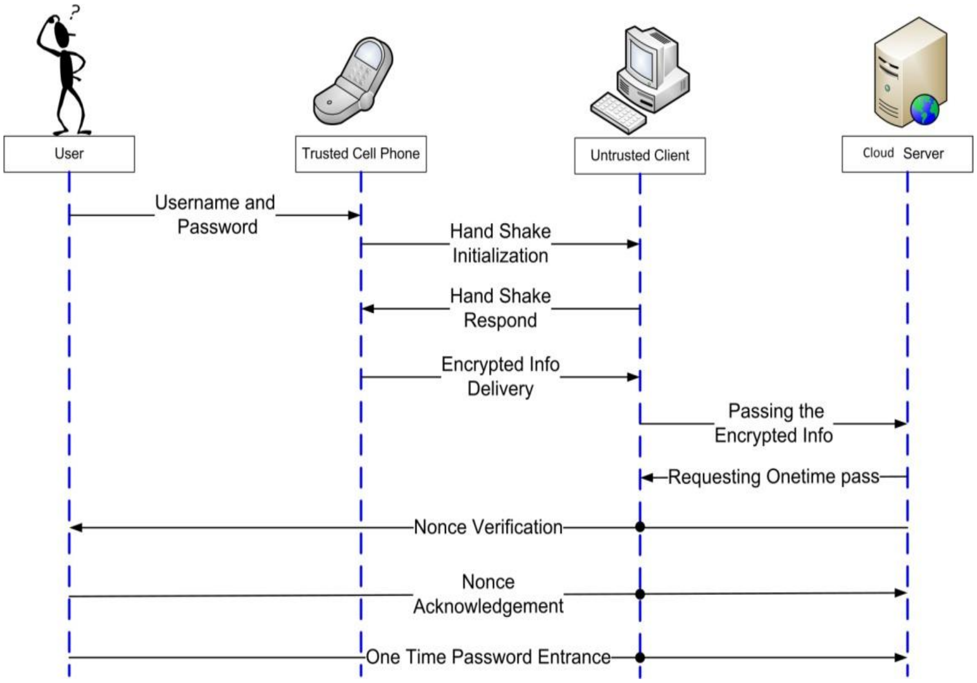


Figure 4.3: Working of OTP Mobile Authentication Mechanism

Step1- the user wishes to login into a secure website.

Step-2 the user sends an encrypted SMS to server.

Step-3 the server received the encrypted SMS.

Step-4 the server decrypts and breaks the SMS into certain parts: Sender's Mobile Number, Username, PIN and IMEI number.

Step-5 Server checks the information against the database to ensure that user is genuine, if user is not genuine then server ignore the SMS.

Step-6 If the user is genuine then server generates an OTP and this OTP is encrypted by a unique symmetric key shared between server and user.

Step-7 server sends the encrypted OTP to user via SMS.

4.4. Access Control of Data and Application

The users are divided into groups and permissions are assigned to those groups, not to the individual users, as shown below:

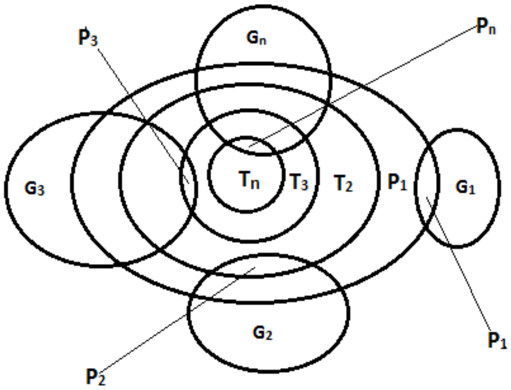


Figure 4.4: Group and Permission Based Access Control

G_1, G_2, G_3………G_n are groups of users, T_1, T_2,T_3……T_n are Tasks and P_1, P_2,…… P_n are the permissions that are given to particular group that has a role assigned to access a particular task e.g. G_1 T_1 with permission P_1, which we can write as $G_1 \rightarrow [(T_1),P_1]$ and $G_2 \rightarrow [(T_1, T_2),P_2]$ means group G_2 has the right to access the tasks T_1 and T_2 with permission P_2 and so on.

There are three entities within this model as is understood from the name:

A. **User** -Users in cloud are identified by a unique key which may be username/password tokens or certificates like Kerberos [124] or X.509 [125] during implementation.

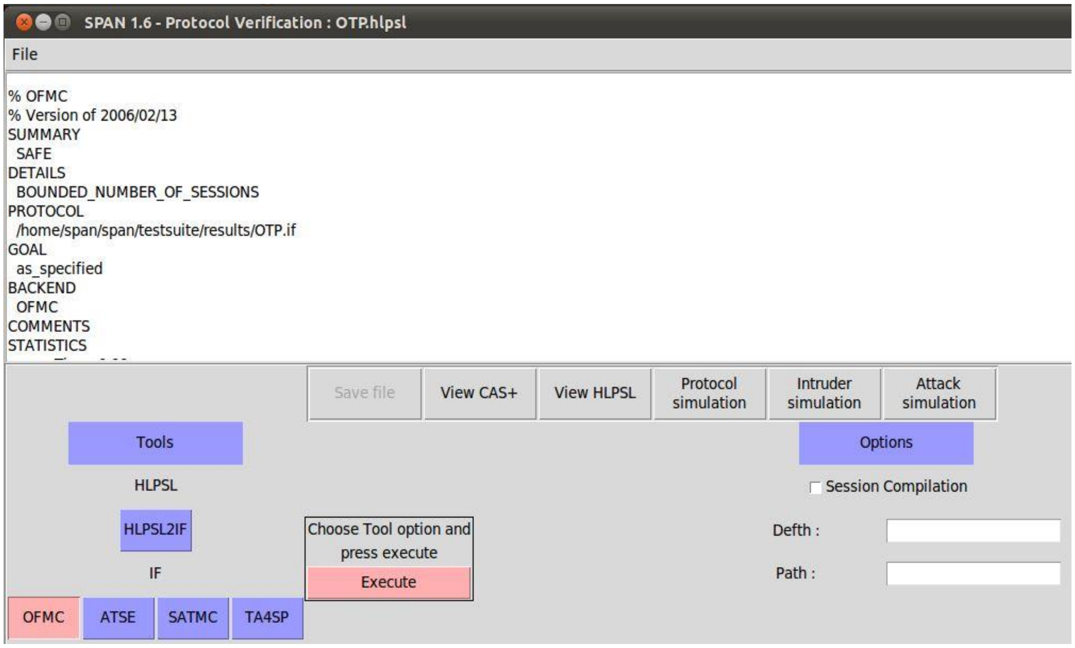
B. **Resource/Task** -Resources within a cloud are identified by the following attributes:

- ***Master key*** is the key of the owner to control over the resource.
- ***Protected operations list*** a list of operation names that must be authorized for execution over the resource.
- ***Max access level*** the maximum levels into the web hierarchy to look while authorization for protected operations over the resource.

C. **Relationship** -Relationships among user and tasks are identified by access rights (Permissions).

4.5. Simulation and Experimental Analysis

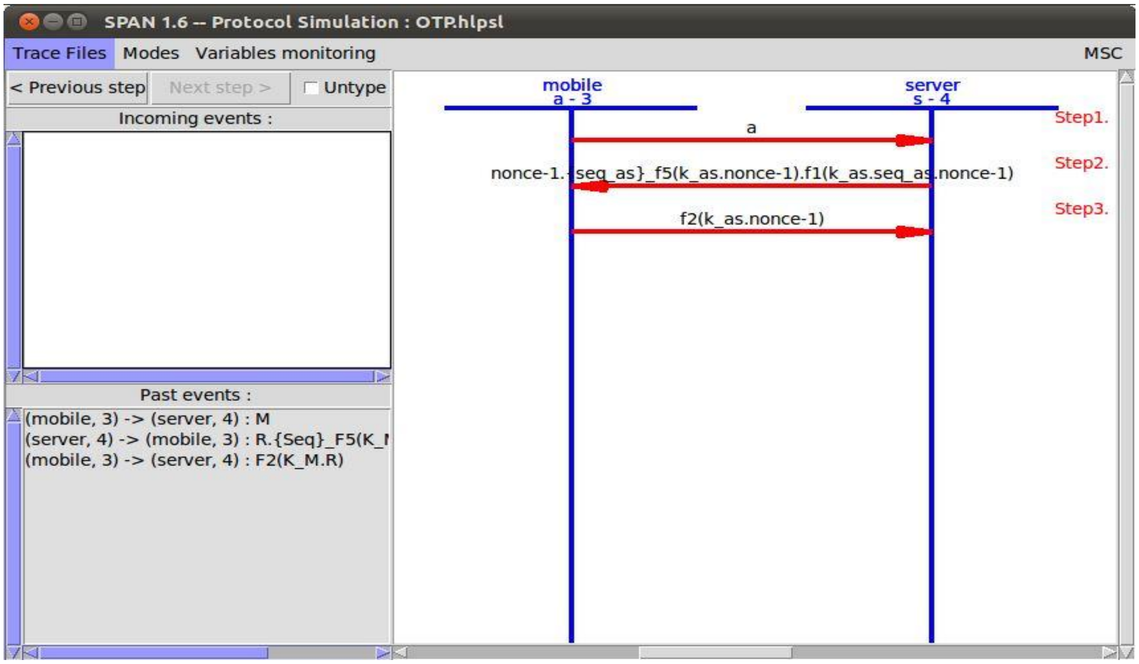
This section focuses on the proposed simulated model with AVISPA and analyses the results as shown in figure 4.5. After executing the HLPSL specification for otp over OFMC model we got the result as safe, means out proposed protocol is free from threat or attack.



```
% OFMC
% Version of 2006/02/13
SUMMARY
  SAFE
DETAILS
  BOUNDED_NUMBER_OF_SESSIONS
PROTOCOL
  /home/span/span/testsuite/results/OTP.if
GOAL
  as_specified
BACKEND
  OFMC
COMMENTS
STATISTICS
```

Figure 4.5: OFMC Result of OTP Protocol

According to our proposed mechanism, the user initiates an OTP request for the server, and the server sends OTP to the mobile device. After receiving the mobile OTP, enter and check the server for successful authentication, we can see the steps in the figure 4.6.



```
(mobile, 3) -> (server, 4) : M
(server, 4) -> (mobile, 3) : R.{Seq}_F5(K_M
(mobile, 3) -> (server, 4) : F2(K_M.R)
```

Figure 4.6: MSC for OTP Protocol Simulation

4.6. Security Evaluation of the Mobile Authentication Mechanism

In this section, we analysed the main known attacks on the confidentiality and integrity of the user's credentials when using the mobile authentication protocol.

4.6.1. Key Logging Attacks

The password *p* is hashed on the mobile device. Also, the cipher text $\{\{u_j||h(p)\}K_s ||N||T\}K_s$, is difficult to decrypt because of the reserved key K_p is strongly kept by the service provider. Hence, it is safe against any key logging program of any type.

4.6.2. Lost or Stolen List of OTPs

If an attacker can somehow obtain a mobile device, the attacker must also initiate the logon process. Because users save the OTP list separately from their mobile device. Thus, an attacker cannot obtain both combined assets.

4.6.3. Shoulder Surfing

In proposed mechanism, OTP is valid for a certain period of time. Thus, an attacker cannot determine the next OTP that the server will require. This, in turn, stops attacks that can occur as a result of shoulder navigation.

4.6.4. Lost or Stolen Mobile Device

Although a stolen mobile device can cause possible brute force attempts to find a user name and password on the cell phone, an attacker also needs to have an OTP to access the account. This gives the user enough time to act or cancel and update credentials to prevent any attack that may occur later.

The figure 4.7 depicts the comparative analysis of the proposed work and existing work in the literature as below.

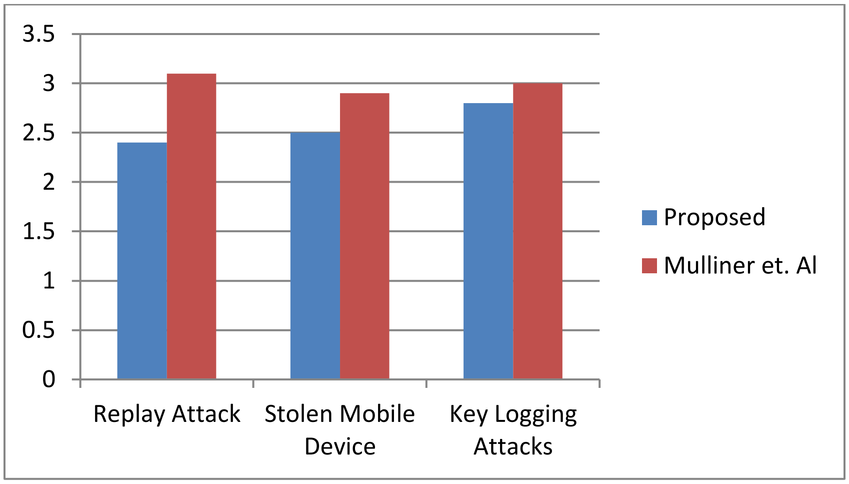


Figure 4.7: Security Risk Against Various Attack

4.7. Important Observations

- We offer a new way to provide an OTP user and send it via SMS. Instead of saving the OTP list on the mobile device.
- Our model uses a complex password using a one-way hash function. In addition, this scheme uses OTP at a time in the next step, which provides more value for the circuit. Then, without knowing the secret user number, the server's secret and OTP, it's impossible to guess the password.
- The SMS gateway in our model generates encrypted text that is once sent to a mobile phone, cannot be decrypted, and the private Kp key is protected by the service provider. Then our model avoids registering keys.
- If a mobile device is lost or stolen, the TNA in it will be useless for the attacker. For authentication, an attacker must initiate the logon process and requires an accurate

identification and a password for which the mobile phone number is already registered. Then, in that case, you can only tackle the shoulder.

- An 8-digit PIN must be used as an input for the phone to create the correct OTP, which is very difficult to guess or brute force if a mobile phone is used.
- For attack from the shoulder, attackers require a secret user number x and OTP. Only the current user can have x and OTP. In addition, we recommend that users dynamically change IDs / passwords, while mobile devices are lost or stolen.
- OTP can operate for a limited time, which prevents the session from being captured.
- The activity of changing the password must be executed in the entry phase. The user's power of attorney is checked before communicating with the cloud in the local system, thus avoiding the DOS attack.

4.8. Conclusion

Our solution is compatible and does not require any changes on the part of the mobile phone. It is easy to implement at the end of the service provider and in the format of OTP messages without changes. OTP based SMS is one of the most user-friendly multifactor authentication mechanisms. We believe that our solution provides OTP security solutions against SMS messages from attacks and helps prevent theft and fraud in an online account. But network availability and sim-cloning can be a barrier in the generation and protection of otp. We analysed the use of AVISPA to test protocol security. Authentication of OTP factor results in stronger authentication.