ISSN: 0975-833X

Available online at http://www.journalcra.com

International Journal of Current Research
Vol. 13, Issue, 06, pp.17856-17862, June, 2021

DOI: https://doi.org/10.24941/ijcr.41553.06.2021

INTERNATIONAL JOURNAL OF CURRENT RESEARCH

RESEARCH ARTICLE OPEN ACCESS

ADAPTIVE MULTI-FACTOR AUTHENTICATION PROTOCOL FOR SENSITIVE REMOTE CONNECTIONS

Amal ALRUWAILI and *Saloua HENDAOUI

Jouf University, College of College of Computer and Information Sciences

ARTICLE INFO

Article History:
Received 27th March, 2021
Received in revised form
15th April, 2021
Accepted 20th May, 2021
Published online 30th June, 2021

Key Words:
Security, Authentication,
Password,
Biometric, Periodic,
Third Factor.

ABSTRACT

National cyberspace that is secure and trusted is required for the growth and prosperity of any country. In this age of big data, public organizations are facing many information security challenges related to the expansion in the use of technology. Additionally, cyber threats are in continuous development which requires proactive enhancement of the national cybersecurity to protect information technology systems. In this paper, we deal with the enhancement of authentication policies in access to national information systems. We propose an adaptive authentication protocol that includes both passwords and biometric factors in the authentication. Two main phases are proposed: initial and periodic authentication. The performance of our protocols is proven by simulation.

Citation: Amal ALRUWAILI and Saloua HENDAOUI. "Adaptive multi-factor authentication protocol for sensitive remote connections", *2021. International Journal of Current Research, 13, (06), 17856-17862.*

INTRODUCTION

Information is always associated with various types of threats and risks which raises the challenge of building different frameworks to face such risks and threats. Software attacks, theft of intellectual property, sabotage, phishing attacks, malware threats, and information extortion are just a few examples. The rise of these risks and threats left organizations no choice but to invest heavily in Information Security Management Systems (ISMS). Information is a significant asset that organizations cannot afford to lose even partially. Information security is guarding information and information systems from unauthorized use or access, modification, destruction, disruption, or disclosure to ensure (CIA triangle) confidentiality, integrity, and availability (Nieles *et al*.,2017). Authentication is the ability to prove that parties logged in the system are trusted (Patel *et al*., 2019). Various authentication techniques can be used to prove that a user is authorized to enter and access system resources (Stamp, 2011). Evidence of the success of authentication mechanisms is the guarantee of confidentiality, integrity, and availability (Alexandra *et al*., 2017). As an instance, we cite smart cards, passwords, digital certificates, biometrics, and Kerberos (Alexandra *et al*., 2017). We can classify authentication techniques into three main classes (Stamp, 2011):

***Corresponding author:** *Saloua HENDAOUI,*
Jouf University, College of College of Computer and Information Sciences.

Something you know where authentication is performed via passwords. Password is a mixture of numbers, letters, and symbols. This authentication technique can use passwords or pin numbers or one-time passwords (used only once for authentication) (TC-STAG, 1996). Passwords can save us a little cost, but in return, they are not ideal for authentication because of attacks and password cracking, in addition, they can fall victim to eavesdropping, keystrokes, guessing, and social engineering to obtain the password (Stamp, 2011). Something you have, e.g., smart card, ATM card. Something you are, e.g., fingerprint, iris scan. A fingerprint is used to verify identity and it is a unique mark in every person as it differs from passwords that may be similar to each other. A photo of a fingerprint is taken and then entered into the improvement phase. The image is enhanced by image processing techniques. It is then that the different points are identified and extracted from the enhanced image. This is how a fingerprint biometric works. In theory, scanning the iris of the eye for identification and verification is considered one of the best biometrics. In iris scanning, there is no or little or no genetic effect on the iris pattern, so that the determination of the measured pattern is stable throughout life and is considered unrelated in the case of identical twins in addition to this even in the eyes of the same individual. The iris scanner methodology determines the location of the iris, then it is performed by taking an image of the eye in black and white, then processing the image using a two-dimensional wavelet transformation. The iris symbol appears as a result. Biometrics can be said about it that it provides high safety, but in return is a high cost because it requires advanced equipment and programs. Also, it is not without problems such as people's fear of health problems such as eye damage. Therefore, in our proposal, we design an adaptive authentication protocol in which we allow the user to choose the appropriate factor to use. The remaining parts of the paper are organized as follows: Section 2 gives the Literature review; Section 3 describes the proposed methodology and the main authentication categories**.** Section 4 discusses the results followed by the conclusion and future work in section 5.

LITERATURE REVIEW

Amin *et al*. (2017) confirmed that a one-time password is vulnerable to fake transactions. To provide a secure context for online transactions, the researchers propose a multi-factor algorithm where the one-time passcode must be obtained by the stored IMEI number of the mobile device on the bank's server. Because of the uniqueness of the IMEI number, one can say that it plays a critical role in this process. The following steps must be taken into account before the activation of the proposed algorithm: The client has a mandatory IMEI application to activate the SIM code. Then, the client will give all the obtained details to the authorized bank to complete the registration process. After that, the client will send the request to the server for data transmission. Finally, the verified data will be added to the IMEI request by the bank. To enhance the quality of authentication, the employed algorithm will make full use of one-time passwords and dedicated hardware. Before starting any online transaction, the proposed framework asks for certain details such as user name and password. Then, a request is sent to activate the IMEI application. After that, the client must give certain biometric information. In case that the given information is correct, the transaction process will be redirected to the dedicated page to complete the transaction.

Bhardwaj *et al*. (2019) have developed a two-factor authentication model (2FA) that is based on a smartphone application to protect data. The researchers agree that the use of smartphones in the authentication process helps solve many critical issues associated with protection challenges, and costs associated with delivery delays. Also, they confirm that the 2FA framework can be employed to improve the authentication process by making full use of two authentication mechanisms for protecting logins from different attacks. The current authenticator application is installed on a mobile device connected to the server. The mobile application will not be worked unless it recognizes the QR code using the installed scanner or additional software. The connection between the mobile and the server will be conducted using the Media Access Control (MAC) of the phone for user identification to ensure security, convenience, and cost-effectiveness. The current model depends on two methods of authentication using asmartphone represented in login verification and application authentication using the JavaScript programming language. Boonkrong (2017) confirm that there are many deficiencies associated with single-factor authentication because of its accuracy-related issues that are subject to many factors. Thus, multi-factor authentication can be used to overcome such deficiency by providing more than one authenticator in validating identities, enhancing safety, protecting users' devices, and hindering opportunities for unauthorized access. The researchers in the current study do their best to propose an improved scheme for managing human resource information by implementing an authentication scheme that is based on a dynamic third factor (DTF) for promoting security. This scheme is regarded as an auto-generated framework upon registration to the information systems. If users sign out, the systems require regeneration of the alphanumeric key to enhance security, integrity, and confidentiality in the networked environment. This approach makes full use of three factors represented in passwords, timestamps, and biometric data to generate the authenticator. Sapuay *et al*. (2019) Implement two authentication methods by making full use of alphanumeric passwords and graphical passcodes using computer-based software to gain authentication to secure the system. Worthy here to mention is the generated OTP shall not be easily guessed, retrieved, or traced. For each client, the International Mobile Subscriber Identity (IMSI) number is required and stored in the server's database. The Timestamp is also used to generate a one-time password that is valid for a short period. There must be synchronization between the phone timestamp and the server timestamp. Ussatova *et al*. (2019) have developed a multi-factor authentication technique that depends on two main steps: a registration system and an actual authentication mechanism. Worthy here to mention is that the authentication process must be conducted in conjunction with the registration process to save the information on the bank's server. To obtain an internet banking service, a login process must be carried out to achieve transaction authentication. The proposed authentication depends on the encrypted key given to the consumer by the bank's server that is regarded as a must for the completion of the authentication protocol. Here, the bank's server renders a digital certificate to the user, and at the same time, it records the IP address to get a symmetric key for the consumer for successful verification. The public key is used by the consumer's machine to compute the hash value of the password, and it is also used by the bank's server to verify the signature to achieve mutual authentication. Khattri *et al*. (2019) performed MFA by adding the calculation of distance and time as additional factor impedes fraud and impedes the activities of the attacker on the account illegally. Even if the attacker obtains (information and details of the card and the PIN, OTP), it is difficult for him to start the step, which is the request from the application that is linked to the phone number registered with the financial institution.

METHODOLOGY

In system security, authentication is crucial since it allows organizations to keep their networks safe by allowing only authenticated users (or processes) to access their protected resources, including computer systems, networks, databases, websites, and other applications or services that are dependent on the network. User authentication occurs for all remote accounts' connections. Generally, to be able to use a system, a user has to select a username or user ID and a valid password. In operating systems and software, as well as wired and wireless networks, user authentication enables human-to-machine interactions.

Authentication categories: In the following, we cite the main types of authentication methods:

Single-factor authentication: Authentication can be done via something the user knows, e.g., secret thing like password, PIN. Password is a mixture of numbers, letters, and symbols, something you know and others do not know. This type of knowledge-based (passwords and PIN) is exposed to many types of attacks and threats which make it less reliable. Obtaining passwords is the goal behind these attacks and threats to gain unauthorized access. Passwords can save us a little cost, but they are not ideal for authentication due to attacks such as brute force attacks, dictionary attacks, and password hacking. In addition, they can fall victim to eavesdropping, shoulder surfing, keystrokes, guesswork, and social engineering to obtain the password.

Also, authentication can be done using something you have, e.g., a smart card, ATM card, or something the user is, e.g., fingerprint, iris scan. A fingerprint is used to verify identity and it is a unique mark in every person as it differs from passwords that may be similar to each other. A photo of a fingerprint is taken and then entered into the improvement phase. The image is enhanced by image processing techniques. It is then that the different points are identified and extracted from the enhanced image. This is how a fingerprint biometric works. In theory, scanning the iris of the eye for identification and verification is considered one of the best biometrics. Genetic effect on the iris pattern, so that the determination of the measured pattern is stable throughout life and is considered unrelated in the case of identical twins in addition to this even in the eyes of the same individual. The iris scanner methodology determines the location of the iris, then it is performed by taking an image of the eye in black and white, then processing the image using a two-dimensional wavelet transformation.

The iris symbol appears as a result. Comparison of iris codes based on the Hamming distance between the symbols. Biometric techniques provide high safety, but with a high cost because it requires advanced equipment and programs. Also, it is not without problems such as people's fear of health problems (e.g., eye damage).

Multi-factor authentication (MFA): Because passwords are considered insufficient to verify a user’s identity, the most common form of MFA is two-factor authentication (2FA). The multifactor is that if the threat was able to impersonate a user from the actor with one piece of evidence, then the threatened would not be able to present two or more shreds of evidence. A powerful multi-factor authentication protocol must use factors from two different classes. Indeed, using factors from the same class does not achieve the goal of the MFA method. One of the improvements to a well-secured online authentication architecture is multi-factor authentication. This improvement was found to solve the user data security problem and consists of several layers of authentication in addition to the password (Lam,2016; Ometov,2018). The combination of two or more authentication methods is the concept of multi-factor authentication (Lam,2016; Ometov,2018). This type of authentication is a combination of any of the three methods of one-factor authentication that were mentioned above. An ATM card is an example of this type. As the user owns the card in addition to knowing the personal identification number. Two-factor authentication is more reliable, stronger, and more difficult than one-factor authentication (Bani-Hani *et al*., 2019). The user can access the system after all authentication factors are successfully bypassed, verified, and in possession of the user (Hasmik,2017; Sabzevar,2008). Multi-factor authentication has attracted much attention from researchers due to issues targeting passwords, classic methods of being a single point of failure, vulnerabilities, and other problems. Multi-factor authentication is being adopted in many services and organizations on the Internet. The multi-factor authentication method is effective and reduces the risks targeting the single-registration process, but studies have shown that the multi-factor authentication method is seen to provide high levels of security, but it has been classified as more difficult, less appropriate, and takes longer compared to passwords (Gunson,2011; Weir,2010).

Users usually have many levels of permission to access their accounts or do their task for an example bank account, so authentication ranges from passwords to fingerprints and faces recognition to verify the identity of a user. The traditional way to access any account by entering your user’s name and password isn’t enough to secure your account so Multi-Factor-Authentication gives more protection. Multi-Factor-Authentication is used basically in the digital environment and it requires more than one piece of evidence to ensure the user’s identity. It is a combination of two or more independent credentials.
” According to SC Media UK, 68 percent of Europeans are willing to use biometric authentication for payments. Consider the daily routine of ATM cash withdrawal (Khan,2015Adeoye,2012)”. The main purpose of MFA is to create an efficient defense against any attack. Most systems use multi-factor authentication, especially two-factor authentication, based on sending a one-time password. This method is correct, easy, and it guarantees us a high level of security and confidentiality for accounts. However, saving passwords is an option available on our devices. One of its advantages is that it facilitates the use of applications, but in return, it has risks and disadvantages. If the mobile is stolen or lost, and the password is saved on the device, this causes a risk that enables others to use the account illegally, even if a one-time password is sent, since the chip still inside the device. As well as spying on the cell phone, stealing the device password, and using the account whenever possible. If the account password is saved, a colleague in the office or a member of the family may overtake in carrying out unauthorized activities and without the consent of the owner of the account. Also, there is a risk of forgetting the mobile phone unlocked anywhere and with saved passwords. Therefore, multi-factor authentication that depends on a one-time password improves the level of security, but this still insufficient because of the beforementioned risks... We cannot fixedly restrict users, as some refuse unusual authentication methods. Such as imposing biometric authentication, not all people carry it because of accidents and distortions that have befallen them, in addition to users' fear of the health problems that may result from them. Also, not all users have biometric-reading devices and it is difficult for them to provide devices, and in cases that will not be recognized due to sensitivity to some substances. The same is the case with the facial recognition camera in some device resolutions that do not recognize the face. Some devices do not support biometric authentication. Therefore, given the difficulty of implementing them in terms of cost and in terms of users' desire to adopt these methods, the solution is an adaptive method of authentication.

PROPOSED METHODOLOGY

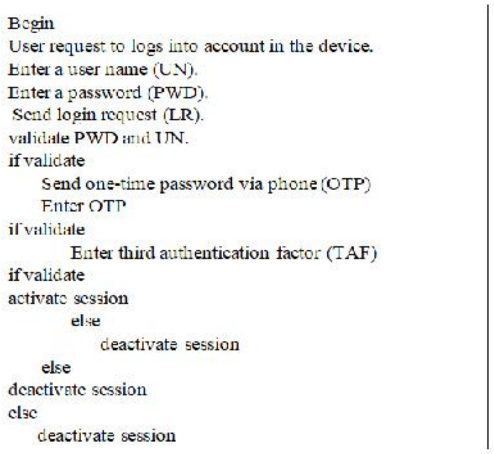
Notation: Table 1 summarizes the notation used in this paper.

Assumption: For our proposal, we assume the following:

- A trusted link is available between the mobile device and the authentication server.
- The user device can capture the adapted biometric factor.
- The AS as well as the database server can check the validity of the exchange biometric factor.

The proposal is summarized by the decision tree shown in fig. 1. We can see that if the username is not directly correct, the session will not be activated, and if it is correct, the password will be entered by the user, and if the password does not match the username, the session will not be activated. And if a password, as well as the username, are correct, the one-time password sent from the server to the device will be entered, then it is tested as well so that if it is incorrect, the session will not be activated and if it is correct then it moves to the next stage, which is the third factor that is chosen by the user, if it is true, the session is activated, and on the contrary, it is not deactivated. We worked on two phases of authentication (fig.2), the first one is initial authentication and the second one is periodic authentication.

Remote authentication: As shown in fig. 3, whenever a user is attempting to log in to the account online, at least two-factor authentication is applied. The first authentication factor is the password, and the second factor is OTP for online authentication. Penetration is reduced by these factors but not stopped. To increase security, in online authentication, there is a necessity for a third authentication factor. In the proposed authentication scheme. The user logs into the account using a password, one-time password, and the third authentication factor that depends on biometrics, and the factor is chosen based on the user's request. If the authentication of all three factors (password, one-time-password, and third factor) is successful, the session is opened and the user gets the ability to view his account and perform various operations. Here, comes the role of the second stage of authentication, which is the periodic authentication while working on the account, the system performs this stage and verify the third authentication factor every specified period to confirm the identity of the user to increase security as well as to ensure that the user is in control of the account.

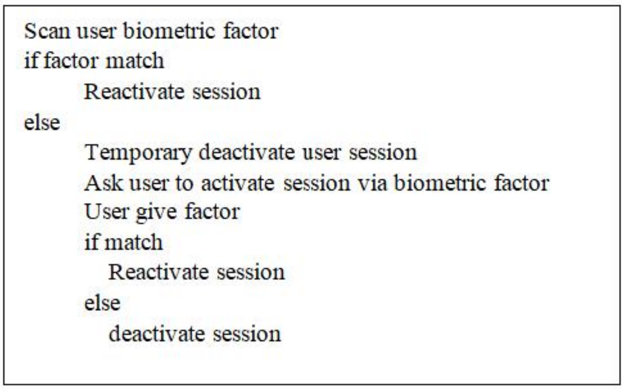


```
Begin
User request to logs into account in the device.
Enter a user name (UN).
Enter a password (PWD).
 Send login request (LR).
validate PWD and UN.
if validate
     Send one-time password via phone (OTP)
     Enter OTP
if validate
          Enter third authentication factor (TAF)
if validate
activate session
          else
               deactivate session
     else
deactivate session
else
     deactivate session
```

Algorithm 1. Initial Authentication procedure (fig. 4 draws the flow chart of this algorithm)

The user starts entering the username and password if they are wrong, the system allows the user to enter the password and the username three times, otherwise, the system moves to send the temporary password. The above steps may be re-executed in case the temporary password is wrong. The system allows the user to enter it only three times and if it was correct, it moves to the next step, which is sending the third factor based on biometrics. If this factor is correct, the user succeeds in entering the session, browse his account and perform operations on it.

Note: for all factors the user must be able to enter three login requests in case of mismatch.



```
Scan user biometric factor
if factor match
        Reactivate session
else
        Temporary deactivate user session
        Ask user to activate session via biometric factor
        User give factor
        if match
           Reactivate session
        else
           deactivate session
```

Algorithm 1: Periodic Authentication procedure fig. 5 draws the flow chart of this algorithm)

At this stage, which is the periodic authentication, which takes place after a specific period, the system scans the user's biometric factor to verify his identity. If the verification is correct, the session is reactivated and if it is wrong, the system allows the scanning three times. If verification fails, the session is suspended temporarily and then the system asks the user to activate the session using biometric scanning to re-activate the session, and then the system performs its turn again in case the user's factor scan is correct or not. Whenever a user session is activated, periodic implicit authentication must be performed. This authentication refers only to the third authentication factor (TAF). The application should perform the periodic comparison between the saved third-factor authentication (TAF) and the used TAF. In our proposal, we recommend as third authentication factor (TAF), face recognition thanks to its advantages.

Biometric factor: Biometrics is the measurement of physiological/behavioral characteristics and is used to verify individual identity such as fingerprint and face recognition (Salama Abd EL minaam *et al*., 2020). These biometric systems are used in many fields such as forensic medicine, safe access, and prison security (Salama AbdELminaam,2020; White,2015; Robertson,2016).

Biometric systems recognize individuals who are using authentication by taking advantage of different biological features (Salama AbdE Lminaam *et al*., 2020). Facial recognition is a computer system application that verifies an individual from a digital image (Saini *et al*., 2014). The face is an important part of the human body, research shows that the face can speak as well as have different words for different feelings, meaning we can say in another way that the face and its interaction play a crucial role in interacting with people in societies (Salama Abd ELminaam *et al*.,2020). The use of the face is considered a key to transmitting a person's identity and provides security solutions in many organizations (Salama Abd ELminaam *et al*.,2020). The use and trend of the facial recognition system are increasing because it is considered a safe, reliable, and secure technology (Salama AbdELminaam,2020; White,2015; Robertson,2016). Facial recognition technology depends on the recognition of the person's face, then the different features of the face are compared with the faces previously recorded (Salama AbdELminaam *et al*., 2020). The facial recognition system has evolved with features and easy-to-use processes that include facial nodules, as there are 80 to 90 unique facial nodes (Salama AbdE Lminaam *et al*., 2020). The facial recognition system measures the shape of the jawbones, the distance between the eyes, the length of the jawline in addition to the depth of the eyes, these nodal points are measured by creating a symbol called a faceprint and this is what represents the person's identity file in the computer database (Salama AbdELminaam *et al*.,2020).

In this proposal, we recommend facial recognition for several features that distinguish it from other measurements. Facial recognition has features that distinguish it from other biometrics, such as fingerprints. The facial recognition system captures vital measurements from a specific distance without interacting with the person (Salama AbdELminaam *et al*., 2020). Also, in the current situation, such as the Covid 19 virus, work systems can use facial recognition without any contact, which leads to reduced infection and the spread of the virus.

Furthermore, the facial recognition system helps organizations to identify a person who has any kind of legal case or criminal record (Salama AbdELminaam *et al*., 2020). It increases security and protecting society from crimes, it's used in public areas like banks and airports. It helps to identify an individual among massive crowed and this kind of authentication can't be performed by other biometrics (Saini *et al*., 2014). Note: facial recognition isn't perfect all the time, because it faces many obstacles like weak lightning or objects covering the face like sunglasses,(Salama AbdELminaam,2020; Saini,2014). Likewise, the identification accuracy may be weak in cases or circumstances in which the photo is not a perfect low-resolution image or in addition to taking pictures of the face with a difference of several years (Salama AbdELminaam, 2020; Saini, 2014).

Transaction verification: In addition to the initial authentication, periodic authentication, we proposed to add another level of authentication, not during normal usage of the application, but during transactions done by an activated session. We recommend that the application perform TAF verification before the execution of the user's requests. To provide a higher level of security and make it difficult for fraud hackers, that is, when the user transfers, for example, a financial transaction in his bank account or authorization, the system verifies the third authentication factor. Transaction verification is known as the process of comparison and then verification of all transactions within a specific group, product type, or region within a specified period.

RESULTS AND DISCUSSION

This section discusses the results and discussion which are obtained from the implementation.

System model: We used scyther simulator

- Scyther is a tool for the automatic verification, falsification, and analysis of security protocols.
- The tool can be used to find problems that arise from the way the protocol is constructed.
- can verify protocols with an unbounded number of sessions and nonces.
- can characterize protocols, yielding a finite representation of all possible protocol behaviors.
- It is efficient: comparison of security protocol analysis tools.
- Analyze security protocols to identify potential attacks and vulnerabilities, able to detect several possible attacks.
- The tool has also been used to find new multi-protocol attacks on many existing protocols.
- Generate a graph for each attack corresponding to the mentioned claim.
- Verify whether the security claims in the protocol description hold or not.

- Automatically generate appropriate security claims for a protocol and verify them.
- Analyze the protocol by performing complete characterization.
- The input language of Scyther allows for the specification of security properties in terms of claim events.
- In a role specification, one can claim that a certain value is confidential (secrecy) or certain properties should hold for the communication partners (authentication).
- Scyther can be used to verify these properties or falsify them.

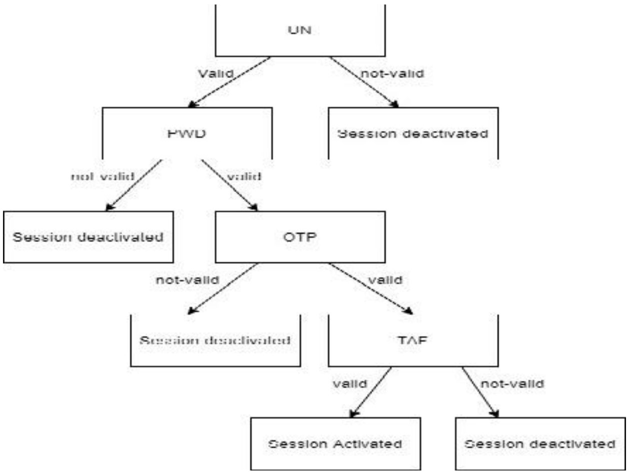


Figure 1. Decision tree of the proposed solution

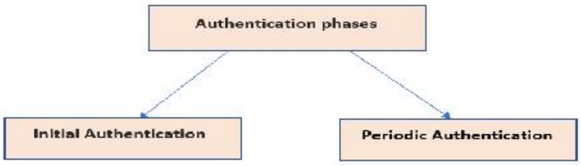


Figure 2. Two authentication phases

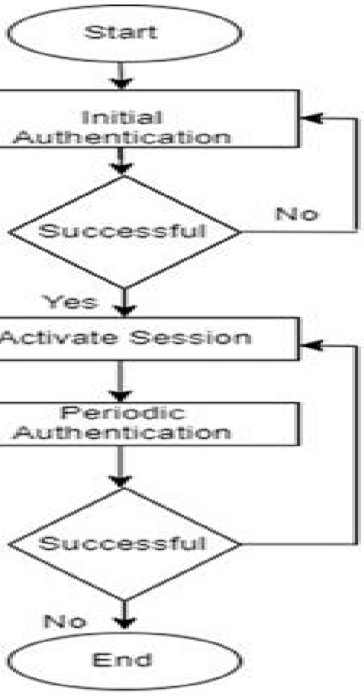


Figure 3. Proposal's flow chart

Implemented protocol: we have two main events in our proposal which are received and send. We have three main agents presented in our protocol which are

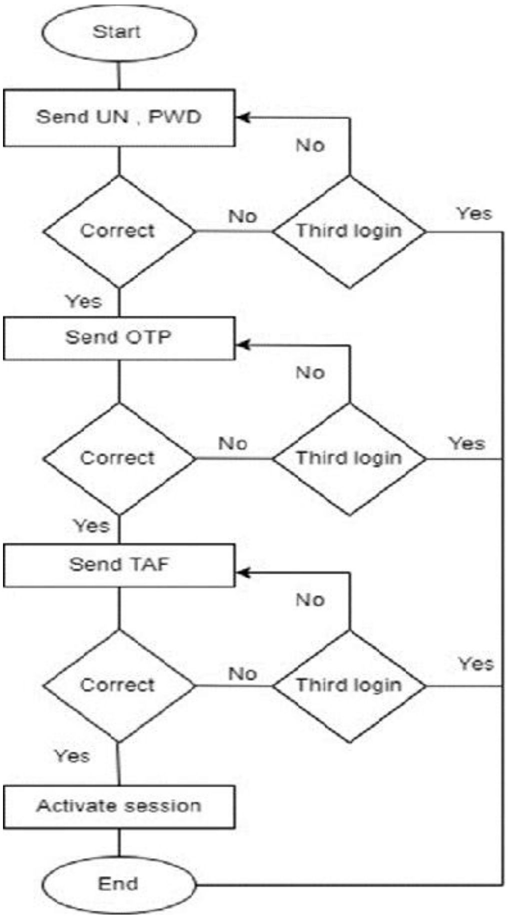


Figure 4. Initial authentication flow chart

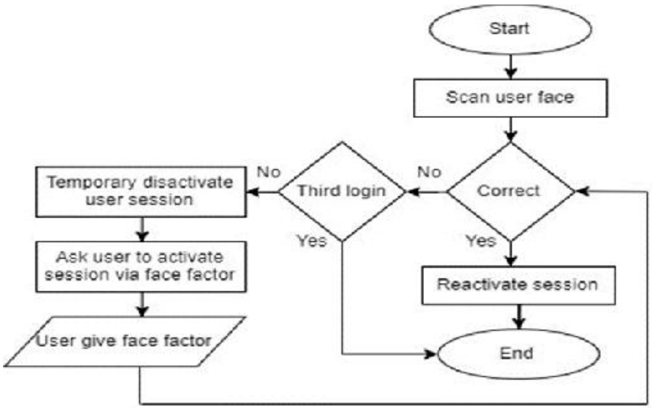
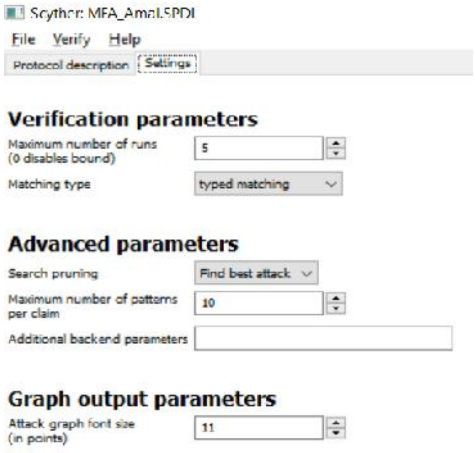


Figure 5. Periodic authentication flow chart



Verification parameters

Maximum number of runs (0 disables bound) 5

Matching type typed matching

Advanced parameters

Search pruning Find best attack

Maximum number of patterns per claim 10

Additional backend parameters

Graph output parameters

Attack graph font size (in points) 11

Figure 6. Simulation parameters

v AS: Authentication Server
v DB: Data base Server
v MD: Mobile Device

Our protocol is executed as follow:

// in this scenario, we assume that data sent by the mobile device is valid

Send-1 (….) : the MD sends its corresponding login and password to the AS.

Recv-1 (….) : the AS receives the data sent by the MD in send-1.

Send-2 (….) : the AS sends a verification request to the DB to verify the login and password.

Recv-2 (….) : the DB server receives data sent by the AS in send-2.

Send-3 (….) : the DB Verify the received data and send the answer to the AS.

Recv-3 (….) : the AS receives the send-event performed by DB.

Send-4 (….) : the AS send OTP to the MD.

Recv-4 (….) : the MD receives the OTP from the AS.

Send-5 (….) : the MD sends the received OTP to the AS.

Recv-5 (….) : the AS
verifies the OTP received from the MD.

Send-6 (….) : the AS sends verification notification to MD.

Recv-6 (….) : the MD receives an answer from the AS.

Send-7 (….) : the MD
sends the biometric factor to the AS (for simplicity reason, we considered this factor as numeric representation).

Recv-7 (….) : the AS receives the biometric factor from the MD.

Send-8 (….) : the AS
sends the biometric factor to the DB.

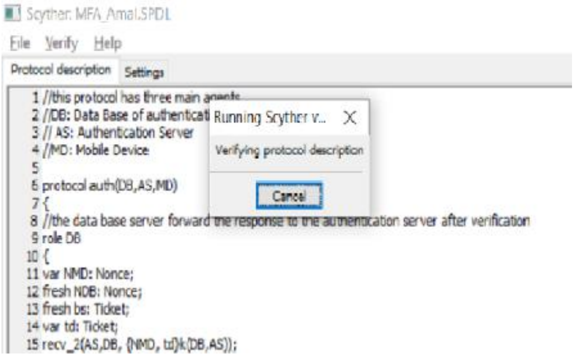
Recv-8 (….) : the DB receives the third factor from the AS.

Send-9 (….) : the DB sends verification notification to the AS.

Recv-9 (….) : the AS receives the verification answer from the DB.

Send-10 (….) : the AS sends the answer to the MD.

Recv-10 (….) : the MD receives the authentication result from the AS.

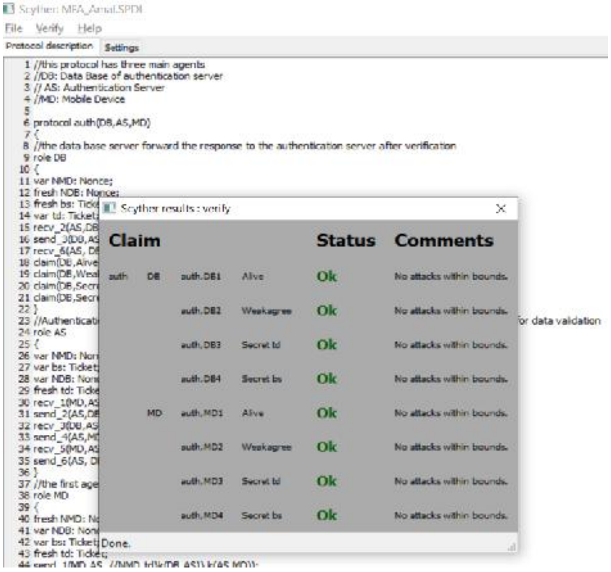


```
//this protocol has three main agents
//DB: Data Base of authenticati
// AS: Authentication Server
//MD: Mobile Device

protocol auth(DB,AS,MD)
{
//the data base server forward the response to the authentication server after verification
role DB
{
var NMD: Nonce;
fresh NDB: Nonce;
fresh bs: Ticket;
var td: Ticket;
recv_2(AS,DB, {NMD, td}k(DB,AS));
```

Verifying protocol description

Figure 7. Protocol verification



```
//this protocol has three main agents
//DB: Data Base of authentication server
// AS: Authentication Server
//MD: Mobile Device

protocol auth(DB,AS,MD)
{
//the data base server forward the response to the authentication server after verification
role DB
{
var NMD: Nonce;
fresh NDB: Nonce;
fresh bs: Ticke
var td: Ticket;
recv_2(AS,DB
send_3(DB,AS
recv_6(AS, D
claim(DB,Alive
claim(DB,Weak
claim(DB,Secr
claim(DB,Secr
}
//Authenticati                                        for data validation
role AS
{
var NMD: Non
var bs: Ticket
var NDB: Non
fresh td: Ticke
recv_1(MD,AS
send_2(AS,DB
recv_3(DB,AS
send_4(AS,M
recv_5(MD,AS
send_6(AS, D
}
//the first age
role MD
{
fresh NMD: N
var NDB: Non
var bs: Ticket
fresh td: Ticket;
send_1(MD,AS, {{NMD, td}k(DB,AS)} k(AS,MD));
```

Claim				Status	Comments
auth	DB	auth.DB1	Alive	Ok	No attacks within bounds.
		auth.DB2	Weakagree	Ok	No attacks within bounds.
		auth.DB3	Secret td	Ok	No attacks within bounds.
		auth.DB4	Secret bs	Ok	No attacks within bounds.
	MD	auth.MD1	Alive	Ok	No attacks within bounds.
		auth.MD2	Weakagree	Ok	No attacks within bounds.
		auth.MD3	Secret td	Ok	No attacks within bounds.
		auth.MD4	Secret bs	Ok	No attacks within bounds.

Done.

Figure 8. Simulation results

Table 1. Notations

Notation	Description
UN	User name.
PWD	Password is a mixture of numbers, letters and symbols, It is selected by the user.
OTP	One time password generated by authentication server and sent to mobile device via chips.
TAF	Third authentication factor.
AS	Authentication server.
LR	Login request.

Fig. 6 shows the configuration of the run to test our protocol against attacks. Fig. 7 shows the verification of the proposed protocol against attacks and as shown by fig. 8, our protocol is safe against attacks. We have conducted a security analysis of the proposed system and this analysis confirms that the proposed scheme is resisting major attacks.

Man in the middle attack: This proposal resists this type of attack, which is a type of hacking where the attacker interferes with a conversation or transmits data so it sends malicious links to both participants. ”Roger Grimes posits that it is perhaps the most common type of hacking to get around multi-factor authentication. It usually requires a man attack in the middle ".In this proposal, the use of biometric factor reduce the risk of this type of attacks.

Denial of service attack: The proposal resists a denial-of-service attack. The attacker renders the resource inaccessible to users as the server pending services, the attacker overwhelms the network by sending excessive messages that cause services to collapse by launching SYN flooding, UDP flooding, and ICMP flooding attacks. maybe able to suspend services to the server by flooding it with requests. The proposed scheme checks the identity and password of the user and if the authentication is successful, the user will be able to access the service. To resist against DoS attacks, we recommend that the application prohibit a device from sending repetitive failed authentication requests.

Malicious user attack: The proposed scheme resists a malicious user attack that imitates the intruder as a real entity and tricks the server into accessing its services due to the periodic authentication as well as the reauthentication required for performing transactions.

Reply attack: The proposed scheme combats a replay attack in which the attacker spies on messages. In fact, this type of attacks will not be able to successfully login the system due to the three authentication phases that have to be successfully achieved.

Server spoofing attack: The proposed scheme counteracts a server spoofing attack in which the attacker impersonates the entity by altering the data to gain illegal access to the stored data since the attacker will not be able to perform neither transactions nor to guarantee a long-activated sessions.

Credential stuffing attack: The proposed scheme combats a credential-stuffing attack that an attacker would take advantage of the fact that users frequently use the same username and password on multiple accounts by trying to access a variety of sites and applications using stolen credential pairs and here comes the importance of the biometric factor that is adaptive to the user choice.

Conclusion and future work

MFA protects sensitive information from being manipulated by hackers, almost always secure. Advanced technologies and device, mainly the fast and easy communication make MFA applicable with low cost in term of time and computations. In this paper, a secure multi-factor user authentication system was proposed and the scheme was simulated using the approved scyther tool which proved to us that the proposal is considered defensive against known attacks.

REFERENCES

Nieles, M., Dempsey, K., & Pillitteri, V. Y. 2017. An introduction to information security. NIST special publication, 800, 12.

Patel, C., & Doshi, N. 2019. Security challenges in IoT cyber world. In Security in Smart Cities: Models, Applications, and Challenges pp. 171-191. Springer, Cham.

Stamp, M. 2011. Information security: principles and practice. John Wiley & Sons.

Alexander, R. D., & Panguluri, S. 2017. Cybersecurity terminology and frameworks. In *Cyber-Physical Security* pp. 19-47. Springer, Cham.

TC-STAG, E. T. S. I. 1996. Security techniques advisory group STAG; definition of user requirements for lawful interception of telecommunications: requirements of the law enforcement agencies.

Amin, A., Haq, I. U., & Nazir, M. 2017. Two Factor Authentication. *International Journal of Computer Science and Mobile Computing, 6*7, 5-8.

Bhardwaj, V. P., Chauhan, P., Nitin. 2019. Mobile Based Multi-Factor Authentication Algorithm for Secure Online Transaction. *International Journal of Innovative Technology and Exploring Engineering IJITEE, 9*1, 376-380.

Boonkrong, S. 2017. Internet Banking Login with Multi-Factor Authentication. *KSII Transactions On Internet And Information Systems, 11*1, 511-535.

Sapuay, S. I., Gerardo, B. D., & Hernandez, A. A. 2019. *Dynamic Third-Factor for Enhanced Authentication in Human Resource Information System*. 2019 IEEE 7th Conference on Systems, Process and Control ICSPC 2019, 13–14 December 2019, Melaka, Malaysia.

Ussatova, O., Nyssanbayeva, S., & Wojcik, W. 2019. Two-factor Authentication Algorithm Implementation with Additional Security Parameter Based on Mobile Application. Advances in Computer Science Research, 89, 84-86.

Khattri, V., & Singh, D. K. 2019. Implementation of an additional factor for secure authentication in online transactions. *Journal of Organizational Computing and Electronic Commerce*, *29*4, 258-273.

https://www.cisco.com/c/en/us/products/security/...

Lam, K. Y., & Chi, C. H. 2016, November. Identity in the Internet-of-Things IoT: New challenges and opportunities. In *International Conference on Information and Communications Security* pp. 18-26. Springer, Cham.

Ometov, A., Bezzateev, S., Mäkitalo, N., Andreev, S., Mikkonen, T., & Koucheryavy, Y. 2018. Multi-factor authentication: A survey. Cryptography, 21, 1.

Bani-Hani, A., Majdalweieh, M., & AlShamsi, A. 2019. Online authentication methods used in banks and attacks against these methods. Procedia Computer Science, 151, 1052-1059.

Hasmik, B. 2017. *Multi-Factor graphical user authentication for web applications* Doctoral dissertation.

Sabzevar, A. P., & Stavrou, A. 2008, November. Universal multi-factor authentication using graphical passwords. In *2008 IEEE international conference on signal image technology and internet based systems* pp. 625-632. IEEE.

Gunson, N., Marshall, D., Morton, H., & Jack, M. 2011. User perceptions of security and usability of single-factor and two-factor authentication in automated telephone banking. *Computers & Security*, *30*4, 208-220.

Weir, C. S., Douglas, G., Richardson, T., & Jack, M. 2010. Usable security: User preferences for authentication methods in eBanking and the effects of experience. *Interacting with Computers*, *22*3, 153-164.

SC Media UK. 68% of Europeans Want to Use Biometric Authentication for Payments. 2016. Available online: https://www.scmagazineuk.com/68-of-europeans-want-to-use-biometric-authentication-forpayments/article/530818/ accessed on 4 January 2018.

Khan, R., Hasan, R., & Xu, J. 2015, March. SEPIA: Secure-PIN-authentication-as-a-service for ATM using mobile and wearable devices. In *2015 3rd IEEE International Conference on Mobile Cloud Computing, Services, and Engineering* pp. 41-50. IEEE.

Adeoye, O. S. 2012. Evaluating the performance of two-factor authentication solution in the banking sector. *International Journal of Computer Science Issues IJCSI*, *9*4, 457.

Salama AbdELminaam, D., Almansori, A. M., Taha, M., & Badr, E. 2020. A deep facial recognition system using computational intelligent algorithms. Plos one, 1512, e0242269.

White, D., Dunn, J. D., Schmid, A. C., & Kemp, R. I. 2015. Error rates in users of automatic face recognition software. PloS one, 1010, e0139827.

Robertson, D. J., Noyes, E., Dowsett, A. J., Jenkins, R., & Burton, A. M. 2016. Face recognition by metropolitan police super-recognisers. PloS one, 112, e0150036.

Saini, R., & Rana, N. 2014. Comparison of various biometric methods. International Journal of Advances in Science and Technology, 21, 2.

https://fsc.org/en/supply-chains/transaction-verification

****