

Design, Analysis, and Implementation of a Two-factor Authentication Scheme using Graphical Password

Khaja Mizbahuddin Quadry

Research Scholar JNTUK, Andhra Pradesh, India

E-mail: quadry1973@gmail.com

A Govardhan

Professor and Rector, JNTUH, Telangana State, India

E-mail: govardhan_cse@jntuh.ac.in

Mohammed Misbahuddin

Joint Director, C-DAC, Bangalore, Karnataka, India

E-mail: mdmisbahuddin@gmail.com

Received: 19 September 2020; Revised: 08 October 2020; Accepted: 30 October 2020; Published: 08 June 2021

Abstract: With the increase in the number of e-services, there is a sharp increase in online financial transactions these days. These services require a strong authentication scheme to validate the users of these services and allow access to the resources for strong security. Since two-factor authentication ensures the required security strength, various organizations employ biometric-based or Smart Card or Cryptographic Token-based methods to ensure the safety of user accounts. But most of these methods require a verifier table for validating users at a server. This poses a security threat of stolen-verifier attack. To address this issue, there is a strong need for authentication schemes for e-services that do not require a verifier table at the server. Therefore, this paper proposes the design of an authentication scheme for e-services which should be resistant to various attacks including a stolen verifier attack. The paper will also discuss: 1) The proposed scheme analyzed for security provided against the known authentication attacks 2) The concept implementation of the proposed scheme.

Index Terms: Graphical Password, Two-factor Authentication, e-commerce, Smart Card, Stolen-verifier Attack.

1. Introduction

With the expeditious growth of the web technologies (with specific emphasis on the websites that focus on user-friendly nature, and security of the user accounts) along with the other sophisticated technologies, every organization is competing to provide its services in e-mode and as a result, in the last few years, there has been an enormous growth in e-services such as online shopping, online banking, etc. [1, 2]. However, the increased use of these services without adequate knowledge of possible threats and the implementation of proper security mechanisms especially strong authentication has led to an increase in the number of online frauds [3-5]. To protect these services and guarantee the safety of accounts, Two-factor Authentication is employed to improve the security strength [6-16].

Various two-factor authentication methods using Smart cards, Cryptographic tokens, and Biometrics that are available today [17]. Multi modal biometric authentication system also used for the justification of false rejection and false acceptance [18]. There are two factor authentication schemes which were developed to overcome phishing attacks which proved to be an expensive to implement in real time applications [19]. Other than Smart Card based schemes, most of the Biometric or Cryptographic Token-based schemes require a verifier table at the server to validate the user. This verifier table requirement may lead to a stolen verifier attack wherein the attacker, if gets the database access, may steal the verifier table and perform offline guessing to figure out the user's password. There is always a tradeoff between usability and security while providing both the facilities to the user in e-services [20].

Given the simplicity and cost-effectiveness supported with a better security outcome, the authentication methods using Smart Cards have always attracted a majority of the researchers to develop Smart Card based verification schemes, but none of them came up with an effective verification table provided at the server too [9,21]. None of these protocols

were analyzed for security using formal verification. Besides, none of the papers discussed the implementation and realization of the respective proposed schemes for web-based services.

Hence, the objective of the research is to design a two factor graphical password authentication scheme which does not maintain password table at server. Following are characteristics of the proposed scheme [22-28]:

1. A Two factor-based Scheme wherein the second factor can be a USB Token / a Smart Card
2. Graphical Password for Usability
3. Offers Dynamic ID for each login
4. Suitable for Web-based services
5. Offer protection against known authentication attacks such as replay, guessing, stolen verifier attack, etc.
6. A Secure Mutual Authentication Scheme
7. Authenticated Key Generation

This paper is organized into seven sections. Section one gives an introduction. Section 2, deals with the literature survey. Section 3, deals with methodology. Section 4, explains the proposed scheme. Section 5, discusses the analysis of the security projected by the scheme. The details of implementation are given in section 6, and the conclusion and future work is given in section 7.

2. Literature Survey

In 2010, Akram et al [29] proposed a two-factor authentication scheme, which is secure against ID theft, guessing attacks. During the login phase, the user has to choose a file password. This contains the user-created text. This is hashed by the client; in addition, the user enters two upper case letters then the client applies a hash to the hashed pass file plus these two upper case letters. This is the actual password. This is sent to the server. The server does computations and generates parameters and is stored in a smart card. It is sent to the user by the secure channel. During authentication, the user inserts the smart card and selects the pass file, and enters two upper case letters. The server computes the parameters and compares them with the stored parameters if matched gives access.

In 2009 Misbahuddin et al [30] proposed user-friendly two-factor-based authentication. During the registration phase, the user selects images displayed by the server in a grid format and describes the image which is taken as a text password. Also enters image number in the password field. After submitting user details to the server, the server computes secret parameter stores in a file this is sent through a secure channel to the user to save at his PC or a removable device if registering from the public system. During login, the user enters his ID and the system tries to locate the secret smart card file. It checks the validly of the ID if it is valid displays the images in a grid format, then the user enters his password. The password is locally verified by the smart card if it is valid then it goes for the key agreement phase else reject the request. This scheme is secure against many attacks. It works in wired network.

In 2015, Sreeja et al [31] proposed a secure two-way authentication using DNA cryptography and steganography. During registration, the user has to select a text password and has to select an image. The text password is converted into cipher text with a DNA code and is embedded into the image using steganography. The hash value of stego image is calculated and saved by the server. At the time of login, the same stego image value is compared. This scheme is secure against many attacks but is not secure for stolen verifier attacks, as it maintains a password table at the server.

In 2019 Nikita Zujevs [32] proposed a scheme based on the graphical password. At the time of registration, several images are shown in a single picture. There are many pictures of this type. The user has to select one of those pictures as a password. There is an option of deleting or inserting an image in the given picture. During login, the pictures of a different combination of images will be displayed user has to click on his picture password. The drawback of this scheme is storing these passwords in a database, as the hash of the symbols may not match with the hash of the symbols stored during registration.

In 2018 Xian Chu et al [33] proposed a scheme for login into websites. After the registration of user, during login user is challenged with 9 different pages and asked to click on the images he recently visited. If the user selects the correct images, he will be allowed access else denied. Authors claim that this provides usability, security, and efficiency. Prediction of user behavior towards browsing the web pages is not an easy task that needs a more detailed study of the user.

In 2019, Azad et al [34] proposed a hybrid authentication scheme is the combination of two independent authentication schemes pass point and Press touch code. During registration at different pass points, PTC is recorded. During login if the user repeats the same, he will be granted access otherwise an error and retry message will be displayed on the screen.

In 2018, Bilal et al [35] proposed a 2-D graphical password scheme, during registration user asked to draw a graphical password. The graphical password is mapped on a textual password and stored in the database. During sign-in user has to remember the shapes 2-D graphical password and draw it in the same shape as drawn in registration. Authors claim that this is secure against dictionary attack, brute force attack. The time required for login and computational speed is concerned factor which is not discussed.

In 2014, Shraddha, et al [36] proposed an authentication scheme for a cloud application. The password is designed based on the user's name, the server does calculations based on the user's name and provides a set of 100 images in that user has to select 2 images, and the server itself adds two more images. These four images are stored as a password. At the time of login, the user has to enter his username then the server displays a set of 100 images the user has to select pre-defined images. Then the server adds two images accordingly and compares this with the stored password. Then gives access if the password matches else access denied. The main drawback of this scheme is the memory requirements to save all the images. This scheme is not secure against brute force attack and shoulder surfing attack.

In 2009, Misbahuddin et al [37] proposed two factors authentication scheme for multi-server architecture. Users can access all the services under this service provider SP or trusted RC, if he registers once. Initially, the user has to enter his credentials on the RC, and then RC computes sends 9 images in the grid format, these three grids one after another are displayed at the client side. The user selects images and enters the password in the space provided from numbers displayed with images. Then the system concatenates all the passwords and applies hash send it to the registration center RC. The registration center does computations and generates secret parameters and stores it on a java card and issue a smart card through a secure channel to the user. During login, the user has to insert the smart card and open the service providers' website. Users Identity is validated by the smart card than by the server. If credentials are valid service provider gives a challenge-response by displaying images. The user has to enter the corresponding number of his password images; client computes parameters and sends to server if these match with parameters stored at server access will be given. This scheme is secure against shoulder surfing, stolen verifier attacks. This scheme is only applicable to wired networks.

All the above papers are related to graphical passwords, none of them covered the security and usability aspect like the proposed scheme. Drawbacks of the method [29] is vulnerable to shoulder surfing attack, [30], [34] are better techniques works for wired network scenario.[31] is not secure against the stolen verifier attack.[32] has an issue with storing the passwords in the database. [33] Has difficulty in predicting user behavior, needs a detailed study of the user. [34, 35] are having usability issues.

3. Methodology

The motivation behind this scheme is people recognize images easily than text. This scheme aims to make the user an easy log in by providing pre-selected images for remembering his password. At the registration time, either user has to upload his images, or the server provides images for setting the password. For efficient access user is advised to use low-resolution images. Initially, the user sends a registration request for Selecting a User ID, next he has to clarify Whether he is opting i) User selected images or ii) Server provided images. Also has to clarify whether is using his personal computer or public computer. When the user submits a registration request, the server checks the availability of the ID, if it is available; the server sends a set of images and is displayed on the client-side 3X3 image grid. Then the user selects three images at the rate of one image from each grid. Then the client does a hash operation on each image, the hash image values are applied to exclusively OR gate, the result is stored in the hash form at the server is called Pwi. After getting Pwi server do computations and generate parameters also creates a user profile The portfolio images and the parameters are stored in the smart card and are sent to the user by the secure channel. When the user wants login, he inserts the smart card into the system and sends the login request. After verification of digital certificates by both sides, the server sends portfolio images to the user. The user selects the password as per the procedure discussed above. The client does computations and sends the parameter to the server. Then server and client do mutual authentication and generate a key for further whole communication between server and client.

4. Proposed Scheme

The proposed authentication scheme designed for e-services is presented in this section. The proposed scheme can be implemented with Smart Cards or USB tokens. There are three phases in this authentication scheme, namely, Registration Phase, Login Phase, and Mutual Authentication & Session Key Generation Phase

4.1. Preliminary requirements

The scheme uses a graphical password technique as an alternative to a text password. In the process of registration, user is asked to upload 27 images; the system arranges the uploaded images in three frames consisting of 9 images each. It is requested to select low-resolution images to decrease processing time. The logic in giving choice to the user to upload images is that the user can easily recognize the images during the login phase. The user-uploaded images will allow the system to have a larger password space.

When the user starts the registration process, he is asked to select User ID followed by setting the image password which is displayed on three 3X3 frames displayed one after the other. Figure 1 shows a sample frame of 3x3 frames out of the three frames displayed at the time of the registration phase.



Fig.1. 3X3 Image format

The user has to select one image from each frame and also enter its number in the box provided. In Fig..1 there are eight images. Each image is represented by a number called image ID. Here it should be noted that at each login time the image IDs are assigned dynamically to each image in the grid.

After the selection of three images, the client applies a hash to each image and then all hashed values of the three images are XORed; the resultant value is stored at the server in the hash form is called Pw_i . During the login process $h(ID)$ will be verified and then images 3X3 frame will be displayed to select his password which he has set during registration.

4.2. Registration Phase

To execute the registration phase in a secure environment it is recommended through HTTPS. When ' U_i ', a user willing to register with a 'S' server, proceeds as follows:

Step R1: U_i submits ID to the server 'S' for registration.

Step R2: When the user inputs are received, the server checks its records to confirm the input data of $h(ID_i)$, when the server finds the ID availability, it sends the images to the client, and the client displays at the user end as a 3X3 of 3 grids of images one after the other. This allows the user to set his image password.

Step R3: Out of the 27 images U_i selects a total of three images at the rate one image from each of the grid. The password Pw_i is submitted by the client to the server S, in addition to the portfolio images set which has 27 images and this is a combination of the user's secret image plus randomly selected images.

Step R4: When server S receives $h(Pw_i)$, will compute as given below:

$$V_i = Q_i \oplus h(Pw_i || ID_i); \text{ where } Q_i = h(y_i || ID_i)$$

$$H_i = h(Q_i); \text{ and } G_i = h(x \oplus h(ID_i))$$

Where Concatenation of Internet Protocol (IP) address & current time is given by y_i

Step R5: user profile is created by Server S and stores $h(ID_i)$, $h(y_i)$, and the portfolio images. The smart card is personalized by the server and sent to the user by a secure channel that contains the parameters as $\{V_i, G_i, y_i, H_i\}$.

4.3. Login phase

Each time ' U_i ', a registered user, plans to login to the server 'S' for access to the resources, he inserts the smart card into the reader or if he possesses USB token then he attaches it to the system and proceeds with the next step as:

Step L1: Login request from U_i

Step L2: Once the server receives the login request, it sends the login page and its Digital Certificate containing its public key.

Step L3: The client evaluates $H_i^* = h(h(ID_i || y_i))$ immediately after the user enters his ID_i ; compares H_i^* with H_i (which is already stored in smart card); If both values are matched it generates ' P_i ' a random secret.

Step L4: Client also computes $R_i = h(P_i) \oplus h(ID_i)$; and encrypts the parameters P_i , R_i , and $h(y_i)$ as

$S_i = E_{KUs}(R_i, P_i, h(y_i))$, With server's public key and sends encrypted message S_i to Server.

Step L5: With its private key server decrypts the received S_i which is given by $D_{KRs}(P_i, R_i, h(y_i))$.

Step L6: Server checks the validity of $h(y_i)$ and $h(ID_i)$ after computing $h(ID_i) = h(P_i) \oplus R_i$, once it finds valid then computes $h(P_i+1)$;

Step L7: ' P_i ' random secret is generated by the server 'S' as well as the user's portfolio images are retrieved by it.

Step L8: After computing $J_i = E_{h(P_i+1)}(Images, P_j)$ by the server, the same is sent to the user.

Step L9: The client after receiving J_i decrypts as $D_{h(P_i+1)}(Images, P_j)$ and displays images for the user to enter the image password.

P_i is transmitted in the encrypted form, if an attacker gets, he cannot generate $h(P_i+1)$ which is a very important step in resisting the phishing attack.

Step L10: PW_i is the password entered by the user U_i .

Step L11: Hash of V_i^* is compared with H_i after computing $V_i^* = h(P_{wi} \parallel ID_i) \oplus V_i$; If both are equal then computes

Step L12: $C_i = h(h(P_j+1) \oplus G_i)$;

Step L13: User 'U_i' sends C_i to the Server 'S'

4.4. Mutual Authentication & Key Generation Phase

The server does the following computations after receiving C_i from the client:

Step V1: $C'_i = h(h(P_j+1) \oplus G'_i)$ and $G'_i = h(h(ID_i) \oplus x)$; compares C_i with C'_i , if both are not equal, the request for the log in is failed or else both server and client generate the secret key for the present session as given below:

Session key, $Sk = h(P_j+1) \oplus h(h(P_i+1) \oplus G_i)$

From here onwards encryption is done using the above session key to the whole communication between client and server.

4.5. Password Change Phase

Every registered user has the facility of password reset option any time by initiating the password change option; however, he will be able to use the password change request only after a successful login. As all the communication is encrypted with the help of a session key, hence password change phase is also run in a secure environment. Whenever a client opts for resetting the old password, the following steps to be are carried out:

Step C1: As step one, a number P_k is generated randomly, encrypted with the session key given by $E_{Sk}(P_k)$ by the client, and submits to the server.

Step C2: Once the server gets $E_{Sk}(P_k)$ from the client, it carries out the process to decrypt it as $D_{Sk}(P_k)$ and confirm the validity of the nonce by checking its freshness. If the validity is established, creates P_{k+1} selects a random set of images and encrypts with Sk .

Step C3: In this stage, the $E_{Sk}(\text{Image set}, P_{k+1})$ is sent to the client from the server.

Step C4: The client receives the $E_{Sk}(\text{Image set}, P_{k+1})$ from the server and proceeds to decrypt as $D_{Sk}(\text{Image set}, P_{k+1})$ and tests for the freshness of a nonce, based on the validity it displays the images.

Step C5: The user resets his old password by selecting images and submits P_{wi}^* to the client.

Step C6: The Client works out the values for $V_i^* = Q_i \oplus h(P_{wi}^* \parallel ID_i)$; It then restores V_i with V_i^* .

Step C7: The contents of the smart card are then updated by the client as $\{G_i, V_i, H_i, y_i\}$;

Step C8: The set of portfolio images, along with P_{k+2} is then sent to the server by the client.

Step C9: The server receives the data sent by the client and updates the client profile after confirming the validity of the freshness of random numbers.

The reset password phase needs the client to carry on a series of essential steps for executing the password change option and updating the data on the smart card. As the client carries out all the functions, the computational and communication cost is much reduced at the server end. Fig's 2, 3, and 4 given below represent the Registration stage, the Mutual Authentication & Key Generation stage, and the Password reset stages respectively.

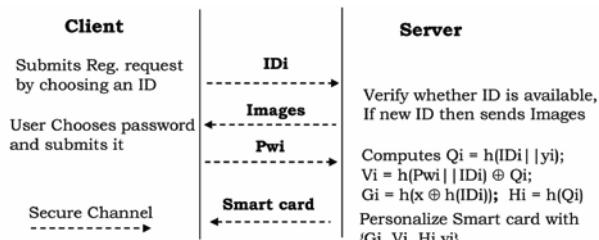


Fig.2. Phase of Registration

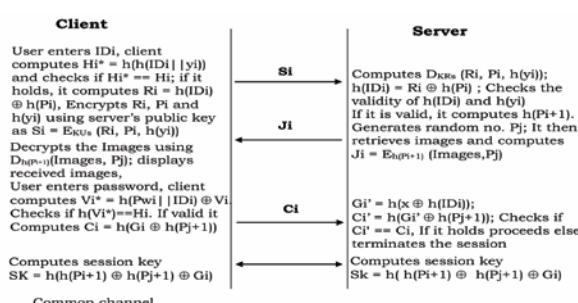


Fig.3. Phase of Authentication & Key Agreement

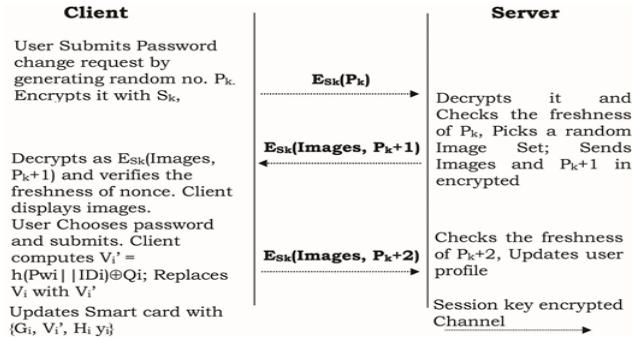


Fig.4. Phase of Password Change

5. Security Analysis

A detailed analysis of the security concerns as proposed by this protocol in terms of the variety of attacks on the scheme along with the possible threats on POC implementation is presented in this section.

5.1. Replay attack

When crucial messages like S_i , J_i , and C_i are intercepted by the adversary during communication and later on replayed to gain access, the attack will not be successful as the user-defined factors are evaluated using random nonce values which are to be cross verified by the receiver for freshness (Server/client). The nonce values are always transmitted in encrypted form so replay attack cannot be performed unless P_i and P_j 's knowledge.

5.2. Insider attack

The insider attack, as the name suggests, is carried out by a raider who happens to be a part of the organization and so has easy access to the user information, which is either used by the raider himself or passed on to others to gain access. The proposed scheme with its unique POC stores all the user credentials in the form of an irreversible message digest on the database at the server. As none of the information is stored in the form of plain text, the raider's attempt to gain access is curtailed successfully.

5.3. Stolen verifier attack

As the name suggests, the verifier information for password verification is stolen by the raider from the server, to use it later on for password verification. But as the proposed scheme doesn't store any verifier table at the server, this attack will not be possible.

5.4. Server spoofing attack

In L9 step, the Server sends J_i to the User, in this way it communicates. The attacker if wants to spoof successfully must create J_i with the help of $h(P_{i+1})$. P_i/P_{i+1} never transmitted, so the attacker never gets $h(P_{i+1})$. If the attacker computes J_i' and sends it by creating $h(P_{i+1})'$ this can be easily detected during the evaluation of L10, step by the client system. In this way, users are protected from masquerader server by the scheme.

5.5. Theft/Loss of Smart Card / USB Token

In case the Smart Card / USB token is lost, which stores the parameters G_i , V_i , H_i and y_i , and a raider gets these, the secret PW_i of the user or the master secret 'x' of the server are unavailable to the raider because of the parameters in the proposed scheme. Because, to get the PW_i , using Q_i which is a message digest value, he has to perform an exhaustive guessing stage offline to get the correct combination of ID / PW_i pair. Such a trial and error procedure requires enough effort and time during which the user may get a new card from the service provider. Also, retrieving the master secret 'x' of the server is rather impossible because G_i requires the computation of $h(x \oplus h(ID_i))$ where all the two are unknown to the attacker.

5.6. Denial of Service Attack

This kind of attack is possible only when the raider holds a high profile in the organization and so is capable of modifying the user credentials stored in the server. Once the raider successfully replaces the user file with a new digest, the user is denied the login with the valid credentials provided by the user. Hence it is named as the denial of the service attack. But the suggested framework is strong enough to foil such attacks because the server doesn't store any kind of secret information. \square

5.7. Implicit Key Authentication:

When a user Authentication scheme provides a secret key with its values known to the server and the client only, it is referred to as the implicit key authentication scheme. The proposed scheme achieves implicit key authentication as the secret session key is created are never transmitted over the channel.

A. Key confirmation

As the name suggests, this authentication scheme involves confirmation of the same secret key by both the client and the server. Hence the proposed scheme assures the same shared secret because both client and server utilize the same validated parameters for the generation of a session key.

B. Known key security

This kind of security scheme comes with the added advantage of the raider failing to derive or guess an access key to a new session from the old keys he had been able to acquire or get their compromised versions. This attribute of this security scheme makes it foolproof as every new session uses keys that are independent of the earlier versions, thus making them computationally inaccessible.

The proposed scheme offers known-key security because each session key is dynamic due to the use of the random numbers in every session. Moreover, the session key is never transmitted during the key generation phase avoiding the interception of the key. In the case, if an adversary gets the earlier session keys somehow, he cannot derive the new session key as firstly the key is a message digest and secondly, it requires a correct guess of the random number p_i using exhaustive search which is practically time-consuming and difficult.

5.8. Storage of registration data

The stored registration data might also be a means to complete an attack. So, the proposed scheme stores all the user data in the form of secret questions and their answers are saved in the form of a digest that makes it irretrievable. So, a raider fails to gain access as he couldn't get the correct answers provided by the user.

5.9. Secure computation

During the registration phase, the client-side computations are implemented with the help of applets which come with a strong protocol in case of the safety of the codes and intermediate values used during the online communication. This curtails the attempts of a raider to access the intermediate values to use them later to succeed with the attack. Moreover, the additional computations like the Authentication and Password Change phases are also carried out using the applets, EJB, and JSP for safety and security concern making it impossible for the raider to gain access. \square

5.10. Security of cookie

It has been discussed earlier that when a user uses a PC at any cyber café or office, and he registers without a smart card or a USB device by simply opting for the 'Public' option, he is allowed access by the server through a cookie type downloadable smart card. Once the user downloads this cookie for registering, it is saved on the system with a validity span of six hours and gets automatically erased for safety concerns.

In such a case, when the registered user leaves the system after some time, without deleting the cookie, an attacker may find it still on the PC as its validity span hasn't finished. Then the attacker gains easy access to all the values like G_i , V_i , H_i , and y_i using it. But as the cookie has all the data stored in the form of a digest, the raider finds those values irretrievable, thus making the cookie safe. In addition to this, the value of G_i can be evaluated only with the master secret known only to the server, with many other secret values used by the server.

5.11. Security against phishing attack

From steps L1 and L4 both client and server get the confirmation that the communication is between the authorized participants. This is done by verifying the freshness of the values transmitted on the network in the form of encrypted values. Afterward, the only client displays the images received from the server. Hence there is no chance of a phishing attack.

5.12. Security against shoulder surfing attack

In the proposed scheme, at the time of registration phase, login phase and password change phase user enter image numbers will appear in the pattern XXXXXX. Even if a camera captures the above process does not reveal the secret. Hence it can be concluded that this scheme is secure against shoulder surfing attack. At the time of each login image numbers as well as the position of images are changing randomly. For the same image user has to enter different number at every login.

6. Proposed Concept Implementation and its Proof

The present section deals with the Proof of Concept Implementation (POC) of the scheme proposed. The Literature Survey carried out as a part of the present study confirms that almost all the Dual Factor Smart Card based User Authentication schemes use a Verifier Table at the Server. So, the present study is unique in its entire framework, as it shows how the Two Factor Authentication process is fulfilled by completely avoiding the use of a verifier table at the server.

This proposed scheme implementation should accomplish by the use of a variety of Java technologies so that high-end security across the communicating channel should be ensured, for both the client and the server. This scheme should use JavaScript and its Applets for all the computations at the client end, and the Servlet, the JSP, and the EJB applications are used to carry out the computations and safer exchange of data or messages between the client and the server, and even within different pages during a transaction. The database used for the proposed scheme should be PostgreSQL 12.0, with JBOSS 4.2.2.GA serving as an application server in the scheme. Though any Operating system can be used to run the POC because of its platform-independent nature, the proposed technique should use MS Windows for all the deployment at the server.

As the proposed scheme aims at providing high-end security across the complete transaction, HTTPS is used to complete the registration process. Further, the second factor in the scheme for authentication is a Smart Card use, the presence of a card reader on the system is mandatory to complete the authentication process successfully. Because all the systems are not provided with a card reader, the implementation of this scheme on a wide range of applications might become restricted due to this additional constraint. To overcome this restriction and improve the applicability of the proposed scheme, the users are provided with two options: 'Public' & 'Personal' at the registration stage. The users use these options while registering, as per the pattern discussed here:

1) In case a client logs in through multiple systems, as and where available to him or he opts to use a USB device instead of a Smart Card, he has to select the option 'PUBLIC' before registering on the network. This selection initiates the server to generate a link to download a 'Virtual Smart Card' file. This Virtual Smart Card file is at the server with the client credentials. The client has to download it and save it on the USB device to proceed with the registration process on different systems at different times.

2) And in case a user wishes to register through his system, the option 'Personal' is to be opted by the user. On this, the server generates a virtual Smart Card when the client registers successfully. This virtual Smart Card should be saved in an unknown location of which the user is unaware of.

3) The third situation is when the public system is used by the client and opts not to use a USB device; a temporary cookie for the client data should be created and is stored on the system by the server. As this cookie will be active for specific time duration of six hours, it gets deleted automatically soon after the period is finished.

This leads to a question that once the cookie gets deleted either by the system or by the user, then what's the way the client can log in later on, as there is no second feature of any kind to support the client login. With this aspect in mind, the proposed POC is equipped with a backup technique to store the saved copies of the smart cards or cookies generated for the clients. Due to this, the client can request for access to his account without a Virtual Smart Card, the POC at the server gets active and shoots specific questions answered by the client during the registration stage. When the answers are given by the client match with the data stored at the server, the system automatically sends the Virtual Smart Card link copy from the POC backup node.

Registration Process: Fig. 5 gives the first stage of registration phase. The user has to select ID, it is checked by the client if it is available then go to next step else ask to select another ID. This is done by the user by clicking on the "Check Availability" option. This aspect, developed from AJAX. If the user ID is available and the user's registration request is accomplished, the graphical password has to be set by the user is discussed in the proceeding stage.

The screenshot shows a web-based registration interface titled 'Registration Page'. It features a text input field labeled 'User ID' and a button labeled 'Check Availability'. Below these are two radio buttons for 'System Type': one selected for 'Personal' and one for 'Public'. A 'Submit' button is also present. The overall design is clean with a light blue header and white body.

Fig.5. Check ID availability



Fig.6. Set image password

Fig. 6, shows the next stage after id selected by the user. This stage takes the client to a page with two options – 'Submit' & 'Next'. It consists of a grid of 3X3 images with image id, with an instruction “enter image number” with three empty boxes. User can enter password in any of the box without following chronological order. Once user enters image number as his password by seeing 9 images set and clicks next button, again one after another two more grids displayed here also user has to see the images and enter text password in the reaming two boxes provided at the bottom of the grid. On the selection of the 'Submit' option by the client, the applet calculates and generates the password hash ready to be sent to the client. When the client clicks the 'Next' option, the server receives the $h(ID_i)$ and $h(PW_i)$ from the client to continue with the registration stage server-based calculations. After user selects Id, graphical password, the server asks the client to fill in the registration form with the details provided by him at the time of registration. This is represented in Fig. 7. This form includes certain client-specific questions that are to be answered correctly only by the client. In case of lost or unavailability of smart card file the same questions will be put as challenge response to the user if he answers correctly, the server recovers the lost Smart Card file or prompts the client to reset the password. This procedure will be discussed in detail later on. As soon as the client completes the above-mentioned registration computations, A Virtual Smart Card is generated by the server. Based on the option selected by the user in case of the second factor, the server either stores it in a secret location not known user or provides a downloadable link as depicted in Fig. 8.

Authentication and Key Generation Process: In Fig. 9, during authentication phase the registered client submits the registration request by selecting the login icon. The server generates the login page at the client end; the client enters his ID after inserting the Smart card or the USB device.

Fig.7. User profile page

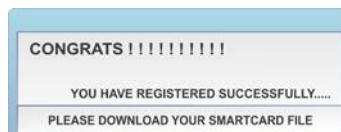


Fig.8. Soft smart card

Fig.9. Locating the second factor

At this stage, the server carries out its routine check to verify whether the system consists of the virtual smart card. When it is found, the client is prompted to identify the second factor. Once the second-factor device is located and ID is submitted by clicking the submit button, the password submission page is generated at the client-side by the server.

Now the user selects his image password and submits it. Here the client generates R_i , P_i , and $h(y_i)$ and sends it to the server after encrypting with the server's public key. When these are received, the server validates the user as per the computations of the proposed scheme. On the successful accomplishment of the client authentication, a dynamic session

key is created by both the user and the client for further communication episodes in the future. Login success and key generation are depicted in Fig. 10.



Fig.10. Generating the session key

Password Change Process: The proposed scheme should be designed in such a way that the password change phase updates can be made by the client himself on his smart card, without any need for connecting the device to the server. This simplifies the password change process thereby enabling the client to change the password whenever and wherever needed by using the external device. To change the old password, the server demands the login be done by the user. On the login being successful, the server and the client gain a session key for the encrypted communication. When a client submits the request for a change password by clicking the 'Change Password' button, an encrypted random number is generated at the client end and is sent to the server. On this communication, the server initiates the decryption phase to confirm the validity of the nonce by checking its newness. At this stage, the client is served with a page for the password resetting, along with an encrypted fresh nonce and images for further authentication. On the receipt of this page, the client goes to the options page, selects the new image password, and sends it to the server. The password change scheme at the server computes the available data and completes the password change process by updating the smart card with the latest parameters.

Forget Password: If the client forgets his password and requests to reset the password, he has to click the 'forget password' link. The server asks the user to enter his ID and then prompts him to answer any three of the five secret questions saved by the user at the time of his first registration on the server. These questions challenge the authenticity of the user and provide necessary security on the channel (Fig. 11).

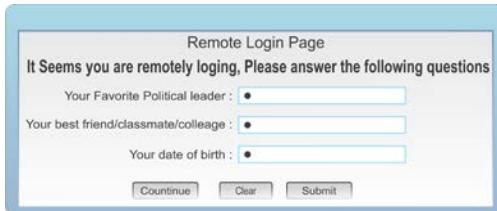


Fig.11. Secret questions page

If the answered are validated, the user is given access to the reset password page. On the successful completion of the new password submission, the server carries out the computations for completing the password change procedure following the proposed scheme. Finally, the smart card should be updated with the newly defined parameters and the message will be sent to the server database.

6.1. Efficiency analysis of the proposed scheme

In the proposed scheme hash functions, XOR operators are used during computations at server and client side. It is assumed that the output of the hash functions, Pw_i and nonce are of 128-bit long. Memory needed to store parameters in smart card is around 512-bits and at server is 256-bits. The communication cost from client to server is 256-bits and during login phase server to client is 540-bits. Sizes of images during login phase is 540kb. Based on the above data it can be concluded that the scheme is efficient. Because most of the calculations are based on hash function, these functions are considered to be efficient.

6.2. Comparison of the proposed scheme with other graphical password schemes

Compared to [29] proposed scheme is better; it is resistant to shoulder surfing attack while [29] is not secure against shoulder surfing attack. The proposed scheme is also better than [31], this scheme does not provide security towards stolen verifier attack whereas our scheme is secure against stolen verifier attack as it does not maintain password table at server.

7. Conclusion and Future Work

A Two-Factor Verification Scheme proposed in this paper using a graphical password for a Web-Based authentication tool, besides it also avoids the use of a verifier table at the server for completing the user verification.

The security analysis, in addition to the POC implementation of the proposed framework, is discussed in this paper. This paper proves the strength of the framework in terms of security against common or automated attacks. The POC (after customizing it as per requirements) can be integrated well with any of the online financial services for secure authentication of a web user. This scheme has been implemented with java technologies. Security is analyzed for the possible attacks. Still needs concrete analysis against common attacks such as Phishing attack, SQL injection, and guessing attack.

References

- [1] Gi-Chul Yang. "PassPositions: A Secure and User-Friendly Graphical Password Scheme" 4th International Conference on Computer Applications and Information Processing Technology (CAIPT) 2017. <https://ieeexplore.ieee.org/xpl/conhome/8308576/proceeding>.
- [2] Mudassar Ali Khan, Muhammad Khurram Khan, Mohsen Guizani, and Kamran Ahmad Awan. "G-RAT | A Novel Graphical Randomized Authentication Technique for Consumer Smart Devices" IEEE Transactions on Consumer Electronics. DOI 10.1109/TCE.2019.2895715, IEEE.
- [3] Yung-Cheng Lee; Geeng-Kwei Chang; Wen-Chung Kuo; Jung-Lu Chu, "Improvement on the dynamic ID-based remote user authentication scheme", International Conference on Machine Learning and Cybernetics, Vol. 6, Issue 12-15, '08, Pg 3283 – 3287.
- [4] Ya-Fen Chang; Chin-Chen Chang; Yu-Wei Su; "A Secure Improvement on the User-friendly Remote Authentication Scheme with no Time Concurrency Mechanism" in the proceedings of 20th International Conference on Advanced Information Networking and Applications, AINA 2006, Volume 2, April 2006, Pg 18-20.
- [5] Bin B. Zhu, Jeff Yan, Guanbo Bao, Maowei Yang, and Ning Xu 'Captcha as Graphical Passwords—A New Security Primitive Based on Hard AI Problems' ieee transactions on information forensics and security, vol. 9, no. 6, june 2014.
- [6] Bruce Schneier, Applied Cryptography, 2nd edition. John Wiley & Sons, 1996
- [7] C.C. Lee, M.S. Hwang, and W.P. Yang, "A flexible remote user authentication scheme using smart cards," ACM Operating systems review, Vol. 36, No. 4, 2002, pg. 23-29.
- [8] Das M. L., Saxena A. and Gulati V. P., "A dynamic ID based remote user authentication scheme", IEEE Trans. Consumer Electronics, May, vol.50, No. 2, 2004, Pg. 629 -631.
- [9] H. M. Sun, "An efficient remote user authentication scheme using smart cards," IEEE Transactions on Consumer Electronics, vol. 46, no. 4, 2000, Pg. 958–961.
- [10] H. Y. Chien, J. K. Jan, and Y. M. Tseng, "An efficient and practical solution to remote authentication: smart card," Computers & Security, vol. 21, no. 4, 2002, pp. 372–375.
- [11] Liao, C. C. Lee and M. S. Hwang "Security Enhancement for a dynamic ID-based remote user authentication scheme" Proceedings of the national conference on Next Generation Web Services Practices (NWeSP'05) 2005.
- [12] Jian Li Lan-Lan Hu, "Improved Dynamic ID-Based Remote User Authentication Scheme Using Smart cards", in the proceedings of 4th IEEE International Conference on Wireless Communications, Networking and Mobile Computing, 2008.
- [13] Misbahuddin M, Ahmed M.A, Rao A.A, Bindu C.S, Khan M.A.M, "A Novel Dynamic ID-Based Remote User Authentication Scheme", in the proceedings of Annual IEEE Indicon Conference, Delhi, 2006.
- [14] Mohammed Misbahuddin; Mohammed Ajaz Ahmed; M.H. Shastri, "A Simple and Efficient Solution to Remote User Authentication Using Smart Cards", in the proceedings of IEEE International Conference on Innovations in IT (IIT '06), Dubai, 2006.
- [15] Omar Cheikrouhou, Manel Boujelben, Anis Koubaa, Mohamed Abid, Attacks and Improvement of "Security Enhancement for a Dynamic ID-based Remote User Authentication Scheme", in the proceedings of IEEE International Conference on Computer Systems and Applications, 2009.
- [16] Shengbao Wang, Zhenfu Cao, and Feng Cao, "Efficient Identity-based Authenticated Key Agreement Protocol with PKG Forward Secrecy", International Journal of Network Security, Vol.7, No.2, Sept. 2008, Pg.181–186.
- [17] Deepak Soni, Nishchol Mishra, "Multilevel Authentication based Data Security and Verification over Cloud Computing", International Journal of Education and Management, Vol.7, No.5, PP.56-68, 2017.
- [18] Safia Mohammed, Michael Hegarty, "Evaluation of Voice & Ear Biometrics Authentication System", International Journal of Education and Management, Vol.7, No.4, pp.29-40, 2017.
- [19] Wang Binjuna,Wei,Yangb,Yang, Yanyanc,Han Jia, "Design and Implementation of Anti-phishing Authentication System", International Journal of Wireless and Microwave Technologies,Vol.1, No.6, PP.38-45, 2011.
- [20] Ugochi Oluwatosin Nwokedi, Beverly Amunga Onyimbo and Babak Bashari Rad, "Usability and Security in User Interface Design:A Systematic Literature Review", International Journal of Information Technology and Computer Science,Vol.8. No.5, pp.72-80, 2016.
- [21] Yan-yan Wang, Jia-yong Liu, Feng-xia Xiao, Jing Dan, "A More Efficient & Secure Dynamic Id-Based Remote User Authentication Scheme", Computer Communications, Vol 32, Issue 4, March 2009, Pg 583-585.
- [22] Reshma, G. Shivaprasad. "Research and Development of User Authentication using Graphical Passwords: A Prospective Methodology" International Journal of Innovative Technology and Exploring Engineering (IJITEE) ISSN: 2278-3075, Volume-8 Issue-9S3, July 2019.
- [23] Gaurav Varshney 1, Manoj Misra, Pradeep Atrey. "A New Secure Authentication Scheme for Web Login Using BLE Smart Devices" International Conference on Engineering, Technology and Innovation (ICE/ITMC) Annual IEEE International Conference on Pervasive Computing and Communications (PerCom) 2017.
- [24] B. Harish Goud, Indurthi Ravindra Kumar. "A Shoulder Surfing Resistant Graphical Authentication System" International Journal of Engineering and Techniques - Volume 4 Issue 1, Jan – Feb 2018.
- [25] Khazima Irfan, Agha Anas, Sidra Malik, Saneeha Amir. "Text based Graphical Password System to Obscure Shoulder Surfing"

- Proceedings of 15th International Bhutan Conference on Applied science and Technology (IBCAST) - January 2018.
- [26] Ian Mackie (B) and Merve Yıldırım. "A Novel Hybrid Password Authentication Scheme Based on Text and Image" IFIP International Federation for Information Processing 2018 Published by Springer International Publishing AG, part of Springer Nature 2018. F. Kerschbaum and S. Paraboschi (Eds.): DBSec 2018, LNCS 10980, pp. 182–197, 2018.
 - [27] Suliman A. Alsuhibany. "Usability and shoulder surfing vulnerability of pattern passwords on mobile devices using camouflage patterns" Journal of Ambient Intelligence and Humanized Computing <https://doi.org/10.1007/s12652-019-01269-March 2019>© Springer-Verlag GmbH Germany, part of Springer Nature 2019.
 - [28] Nida Asma, Hafez Syed Ahmed qasmi, "Conundrum-Pass, A New Graphical Password Approach" 2nd International Conference on Communication, Computing, and Digital systems C-CODE,2019.
 - [29] Syed Akram, Mohammed misbahuddin, and G.Varaprasad "A Usable and Secure Two-Factor Authentication Scheme Information Security Journal: A Global Perspective, volume 21, issue 4, January 2012, pp 169-182.
 - [30] Mohammed Misbahuddin, P. Premchand, A. Govardhan, "A User Friendly Password Authenticated Key Agreement For Web Based Services", IEEE explore, 2009.
 - [31] Sreeja C.S., Mohammed Misbahuddin, "A secure image-based authentication scheme Employing DNS crypto and steganography" wci '15: third international symposium on women in computing and informatics kochi india august, 2015.
 - [32] Nikita Zujevs, "Authentication by Graphical Passwords Method Hope", 978-1-7281-2138-3/19/\$31.00 ©2019 IEEE.
 - [33] Xian Chu" PassPage: Graphical Password Authentication Scheme Based on Web Browsing Records" International Conference on Financial Cryptography and Data Security FC 2020: Financial Cryptography and Data Security pp 166-176.
 - [34] SaifulAzad, "A Secure Hybrid Authentication Scheme Using Passpoints and Press Touch Code", <https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=8879504>.
 - [35] Bilal Eid "A New Password Authentication Mechanism Using 2D Shapes "2018 8th International Conference on Computer Science and Information Technology (CSIT) ISBN: 978-1-5386-4152-1.
 - [36] Shraddah M.Gurav "Graphical Password Authentication Cloud securing scheme"2014 International Conference on Electronic Systems, Signal Processing and Computing Technologies <https://ieeexplore.ieee.org/document/6745426>.
 - [37] Mohammad Misbahuddin, A User Friendly Password Authenticated Key Agreement for Multi Server Environment International Conference on Advances in Computing, Communication and Control (ICAC3'09).

Authors' Profiles



Khaja Mizbahuddin Quadry is a research scholar at Jawaharlal Nehru Technological University, Kakinada. He has completed his M.Tech in 2009 from JNTU Hyderabad. Presently he has one publication in an international journal and one in an international conference. His area of interest is Network security, and Quantum computing.



Dr. A. Govardhan is presently a Professor of Computer Science & Engineering, Rector, Jawaharlal Nehru Technological University Hyderabad (JNTUH). He served and held several Academic and Administrative positions including Registrar I/c., Principal (JNTUH CEH), Director (School of Information Technology, JNTUH), Director of Evaluation (JNTUH), Principal (JNTUH CEJ), Head of the Department, Chairman and Member of Boards of Studies and Students' Advisor. He did B.E.(CSE) from Osmania University College of Engineering, Hyderabad in 1992, M.Tech from Jawaharlal Nehru University(JNU), New Delhi in 1994, and Ph.D. from Jawaharlal Nehru Technological University, Hyderabad in 2003. He is an Editor for 4 Springer Proceedings. He has 3 Monographs and 10 Book Chapters in Springer. He has guided 88 Ph.D theses, 1 M.Phil, and 135 M.Tech projects. He has published 555 research papers at International/National Journals/Conferences including IEEE, ACM, Springer, Elsevier, and InderScience. He has 25 years of Teaching and Research experience. He is a Fellow (CSI and IEI), Life Member/Member in several Professional and Service-Oriented Bodies including the Indian Society for Technical Education (ISTE), Computer Society of India (CSI), The Indian Science Congress Association (ISCA), Association for Computing Machinery (ACM), Institute of Electrical and Electronics Engineers (IEEE), International Association of Engineers (IAENG), World Academy of Science Engineering and Technology (WASET), Free Software Foundation (FSF), Internet Society (ISOC) and International Association of Computer Science and Information Technology (IACSIT).



Dr. Mohammed Misbahuddin did his B.Tech (CSE) from Gulbarga University, M.Tech (S/w Engg.) from JNTU-Anantapur and PhD (CSE) in Network Security from JNTU Hyderabad. He is currently working as Joint Director (Scientist 'E') in Centre for Development of Advanced Computing (C-DAC), E-City, Bangalore. He is the Chief Investigator of the Cyber Security Awareness Project namely Information Security Education and Awareness (ISEA) – Phase II at C-DAC Bangalore. He is a key member of a Nation-wide awareness project on Digital Signatures and PKI namely Next Generation PKI for Smart Applications. He is the Co-Investigator of a National Project named "e-Pramaan – A National e-Authentication Service along with Aadhaar". He has 17+ years of experience in Research,

Training and Project Management. He has applied 3 patents with IPO in the area of Secure and Usable Authentication. He has been in various Programme committees of IEEE /ACM conferences and is a reviewer for two International Journals. His area of interest is Network Security & Cryptography especially Secure and Usable Authentication, Public Key Cryptography and Risk based Engines.

How to cite this paper: Khaja Mizbahuddin Quadry, A Govardhan, Mohammed Misbahuddin, "Design, Analysis, and Implementation of a Two-factor Authentication Scheme using Graphical Password", International Journal of Computer Network and Information Security(IJCNIS), Vol.13, No.3, pp.39-51, 2021. DOI: 10.5815/ijcnis.2021.03.04