ISSN: 2455-6203
International Journal of Science Management & Engineering Research (IJSMER)
Volume : 05 Issue : 02 | July - 2020 www.ejournal.rems.co.in

PAKE Protocol with Image Based Symmetric Key Authentication

Priyanka jain[1+], Rajneesh Pachouri[2]
[1]Research Scholar, [2]Assistant Professor,
Department of Computer Science and Engineering
Adina Institute of Science and Technology, Sagar (M.P.)
[1]ram2004_ahirwal2004@gmail.com,[2]rajneeshrocks92@gmail.com

Abstract: ***Security play important role when information flow over a network. Password authentication key exchange protocol is a technique to exchange symmetric key over a computer network. There are different type of protocol used for exchanging key between the server and users. In this work we use password authentication protocol with image based key generation technique. The concept of making strong secret key is depend on length of the key. Image based key generation method is a a true random number generation method in which we generate a secret key why use of different images. The key length of generated by this method is 128 bit which is too large.***

We present a formal approach to overcome these various problems in password authentication key exchange protocols. We use one time private key (OTPK) in the context of password authentication key exchange (PAKE), which allows for mutual authentication, session key agreement, and resistance to various critical attacks. To enhance more security in our protocol we have used strong session keys which are generated by image based key generation process (True random number generation method). So the proposed protocol is more secure and applicable in various applications.

Keywords— OTPK, TTP, RSA, ECC, DOS, eavesdrop, PASS,

1.Introduction

So long as cozy communication over insecure open networks has been an amazing issue for researchers. For the duration of recent years, cryptographic techniques have been applied to remove those problems. among those approaches, Password

Authenticated Key change (PAKE) protocols have been playing a crucial position in offering comfy communications. PAKE protocols consent a consumer and a server to authenticate each other and form a more potent commonplace consultation key thru a pre-shared human memorable password over an insecure channel.two-birthday celebration password-based authenticated key alternate (two-PAKE) protocol is quite treasured for purchaser-server architectures. but, in massive-scale purchaser-consumer conversation environments wherein a consumer desires to talk with numerous other customers, -PAKE protocol may be very difficult in key management that the quantity of passwords that the user could want to bear in mind.some poorly designed protocols can be vulnerable to partition assaults [18], [19], wherein complete subsets of the password area may be removed in a unmarried attack. We want to put off this type of attack in a comfy manner. Now days typically nobody can agree with to everybody and communique over a community that trouble is unexpectedly growing, so there are want for robust authentication. overcome these authentication troubles on this paper we endorse sturdy 2-thing authentication using one time password scheme.In popular, there are two forms of authentication protocols, the password-primarily based and the public-key primarily based. In a password primarily based protocol, a user registers his account in conjunction with the password to a far off server. Later, he can get right of entry to the far flung server if he can show his data about the password. The server typically keeps a password or verification desk but this can make the system effortlessly subjected to a stolen-verifier attack. To cope with this hassle, recent research propose an method without any password or verification table

within the server. moreover, to decorate password protection, present day studies also introduce a tamper-resistant clever card at the user cease. In a public key-based device, a user should sign up himself to a relied on birthday party, named KGC (Key era middle) to obtain his public key and equivalent private key. Then, they can be diagnosed via a community entity through his public key. To simplify the important thing control, an identification-primarily based public-key cryptosystem is generally adopted, in which KGC problems userID as public key and computes corresponding private key for a consumer.

Thinking about computational efficiency in an authentication protocol, researchers hire low computational strategies encryptions in preference to a lot high priced computation like uneven key encryptions (i.e., RSA, ECC, ElGamal, and bilinear pairings). As thinking about communique performance, it's normally to lessen the number of passes (rounds) of a protocol since the round efficiency is greater critical than the computational efficiency. The most vital measurement of an authentication protocol is its safety, and it must ensure cozy communications for any two criminal entities over an insecure network. Attackers without problems eavesdrop, alter or intercept the conversation messages at the open community. for this reason, an authentication protocol have to resist diverse attacks, which include password guessing assault, replay assault, impersonation assault, insider assault, and man-in-the-center assault.most password-primarily based consumer authentication structures region total self assurance at the authentication server where passwords or easily derived password verification records are stored in a important database. these structures may be easily compromised with the aid of offline dictionary assaults initiated on the server aspect. Conciliation of the authentication server via either outsiders or insiders topics all consumer passwords to exposure and might have severe problems. to overcome those issues within the unmarried server device most of the agencies were proposed which include multiserver systems, public key cryptography and password systems, threshold password authentication systems, server password authentication systems.

1.1 One time private key

Although there are various techniques implemented that are needed for the secure transmission of information from the sender to the receiver. During the transmission of data from the sender to the receiver security plays an important role because the chances of attacks in the network are more. Hence to overcome these limitations there are security techniques implemented for the secure transmission of data. Authentication is also one of the technique through which the data can be sent securely.

One such concept of providing a strong authentication is key generation using one time private key. As we know that key is an important part for the authentication of the data where the sender and receiver uses his own key for the authentication, but if these keys can't be made strong then such techniques is not a secure one [13]. In the concept of key generation using OTPK during the generation of keys by the sender or receiver or by any third party a key is generated for the authentication or for the encryption of the data or for the decryption a key is used and as soon as the sender and the receiver get's authenticated and data is sent securely the key gets destroyed.

2.Background

Password-based authenticated key exchange (PAKE) protocols facilitate two users to generate a common, cryptographically-strong key based on an initial, low-entropy, shared secret (i.e., a password). The complexity in this setting is to prevent off-line dictionary attacks where a rival exhaustively maintains own database, attempting to match the correct password to observed protocol executions. Roughly, a PAKE protocol is secure if off-line attacks are of no use and the best attack is an on-line dictionary attack where an adversary must actively try to impersonate an honest party using each possible password. On-line attacks of this sort are inherent in the model of password-based authentication; more importantly, they can be detected by the server as failed login attempts and defended against.

3.Related Work

In 2011, Maryam Saeed has suggested a new two party authentication protocol without the server's public key in which the limitations of PAKE1 and PAKE2 protocols has been overcome and new authentication protocols have been implemented which can provide several security attributes while it has a remarkable computational efficiency and lower number of rounds [12].

In [12], it is proved that the Hitchcock et al.'s protocol is vulnerable to ephemeral key compromise impersonation, off-line dictionary and Key Compromise Impersonation (KCI) attacks while it does not provide the mutual authentication and forward secrecy attributes. It is also shown that SPAKEI and SPAKE2 protocols are vulnerable to password compromise impersonation and Denial-of-Service (DoS) attacks while they do not provide the mutual authentication property. To remove the above disadvantages, an efficient secure two-party PAKE protocol is designed to provide several securities attributes while the efficiency is also improved.

In 2010 Songs proposed very recently a password-based authentication and key establishment protocol using smart cards which attempts to solve some weaknesses [9] found in a previous scheme suggested by Xu, Zhu, and Feng [7]. In 2009, Lee et al. showed that Juang et al.'s scheme is not secure against stolen-verifier attack. Moreover, Juang's scheme does not satisfy the user anonymity. To solve this problem, Kyung-kug Kim proposed an improved anonymous authentication and key exchange scheme. Then, we show that the proposed scheme is secure against various well-known attacks [11].

In 2011 a password based authentication using Elliptic Curve Cryptography (ECC) for smart card. Since the secret key of the AS is a long-term key, it requires further security. When the secret key of the AS is compromised, the entire operation of the AS will be disrupted. Is it necessary to replace or alter the long term secret key [1].

Password-authenticated secret sharing (PASS) schemes, first introduced by Bagherzandi et al. at CCS 2011, allow users to distribute data among several servers so that the data can be recovered using a single human-memorizable password, but no single server (or even no collusion of servers up to a certain size) can mount an off-line dictionary attack on the password or learn anything about the data. Further in 2012 present a concrete 2PASS protocol and prove that it meets our definition. Given the strong security guarantees, our protocol is surprisingly efficient: in its most efficient instantiation under the DDH assumption in the random oracle model [8].

In 2011 the TW-KEAP is an efficient protocol for sharing a session key to protect communication in an insecure network. It is based on the concept of the Diffie-Hellman key exchange protocol which allows the key exchange without session key appearing in the message. The TW KEAP could support lawful interception because the corresponding server is involved in the key exchange procedure to derive the session key [21].

In 2012 a simple and intuitive model for expressing the semantics of privacy-friendly authentication and accountability technologies such as anonymous credentials systems and verifiable encryption. It allows for expressing the precise relations as well as the authentication and accountability properties between parties. The concepts cover in the model comprises pseudonyms, attribute-based authentication, as well as conditional release of information. As a result, the model can express the relevant primitives for privacy-preserving authentication and accountability at the same time [17].

Many standards exist for authentication, ranging from simple static passwords stored on a single machine to complicated distributed systems. Organizations concerned about protecting their digital assets from sophisticated cyber-attacks have begun relying on two-factor authentication as a defense against unauthorized access [13]. These protocols were proven secure in the random oracle model. Katz, Ostrovsky, and Yung (KOY) [9]

demonstrated the first efficient PAKE protocol with a proof of security in the standard model.

It also achieves mutual authentication in three rounds. In their work [2], Groce and Katz mentioned their framework will significantly improve efficiency when basing the protocol on lattice assumptions. Katz and Vaikuntanathan [10] first instantiated the KOY/GL PAKE protocol under lattice assumptions. The most technically difficult aspect of their work is the construction of a lattice-based CCA-secure encryption scheme with an associated approximate smooth projective hash system. In order to plug into the JG/GK's framework, we use an approximate lattice-based SPH and an error correcting code (ECC) to do the job of an exact lattice-based SPH.

In 2012 by Wang, Y.G. [22] observed that the previous papers in this area present attacks on protocols in previous papers and propose new protocols without proper security justification (or even a security model to fully identify the practical threats), which contributes to the main cause of the above failure. Accordingly, Wang presented three kinds of security models, namely Type I, II and III, and further proposed four concrete schemes, only two of which, i.e. PSCAb and PSCAV, are claimed to be secure under the harshest model, i.e. Type III security model. The type III model will be reviewed later in Section 2. However, PSCAb requires Weil or Tate pairing operations to defend against offline guessing attack and may not be suitable for systems where pairing operations are considered to be too expensive or infeasible to implement. Moreover, PSCAb suffers from the well-known key escrow problem and lacks some desirable features such as local password update, reparability and user anonymity. As for PSCAV, in Appendix B, we will demonstrate that it still cannot achieve the claimed security goals and is vulnerable to an offline password guessing attack and other attacks under the Type III security model [22].

4.Proposed work

The problem in public key cryptography is that if the file size is much longer then it takes more time to encryption or decryption of the message. So we used symmetric key cryptography for sending large file into the insecure network. Again the problem with the symmetric cryptography is that how to share the common session key, because sharing the common session key is causing the various types of attacks. So for reduced these types of problem to share common session key we have produced a very efficient protocol. In our proposed protocol for generating common session key we are using image based key generation which is discussed below.
The proposed protocol works in three Stages:

Stage 1: Registration

During the registration process TTP (trusted third party) generate a registration form for the users, user filled all the required information and send to the TTP. TTP verify all the beneficial information and store in his database. User generate a password as per the instruction given by the trusted third party and send to the TTP, after that TTP store this password in his database for further verification of the user at the time of signing.
Here example of some important information which is needed to registration for the user:

1. user name
2. mobile number
3. email address
4. Address etc.

Stage 2: Signing

The users enter the user name and password for signing to the trusted third party. Here in this stage each of the users needs to generate digital signatures for the authentication. Trusted third party verifies the password if password is valid then goes to the process of key generation, otherwise return the user invalid message.

Stage 3: Key generation

Third stage of our protocol is key generation, in this stage trusted third party generate two times random number (keys), first key generated by the process of pseudo random generator and after verifying that key second key is generated by the process of true random number generator (image based key generation which is discussed below in section 4.1).

ISSN: 2455-6203
International Journal of Science Management & Engineering Research (IJSMER)
Volume : 05 Issue : 02 | July - 2020 www.ejournal.rems.co.in

4.1 **Image based key generation**

Here give the process of generating key by using the image. Figure 1 shows the example of image and figure 2 shows the corresponding binary value of the image. The corresponding M_{key} is the hash value of the image generated key. Steps of generating key by using image are discussed below:

1. Scan pixel values of the image from top to bottom and left to right.
2. Concatenating the value to generate random number consisting of 0's & 1's.
3. Random value can be generated by concatenating columns only or rows only or rows and columns. Here we give an example of concatenating row only.
4. Similarly unique value can be generated for two parties from the same image for authentication.

Figure 1: image of (12×12)

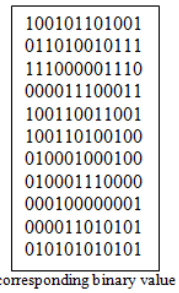


Figure 2: corresponding binary value from image

Generated key is: :
100101101001011010010111111000001110000011100011100111001100110011001101001000100010001000100010000111000000001000000010000011010101010101010101010101
Corresponding M_{key} is:
502a8d2867eaa27ee99b3635c2144909

As we know that if the key length is long then the key is more secure as compare to the short key, so we have been generating a session key by using the true random generation method. Server or trusted third party randomly select the image and generated key by this method. For example if image size is 12× 12 pixels then key size is 144 bits, which is very strong as compare to the pseudo random number. Here give the example of generation of key using image. Trusted third party generated new session key in every session, the previous session key will automatically destroy.

4.2 Proposed Protocol:

In this proposed protocol we have worked on OTPK (one time private key) in the context of password authentication key exchange (PAKE) protocol.

Here some contract signed between the parties and the trusted third party before the establish session key between two parties.

1) Both parties agree for communicating through the online trusted third party.
2) Both parties and trusted third party are agreeing to uses same one way hash function.
3) The trusted third party used secure channel to send OTP (one time password).
4) Both parties are agreeing to communicate with the same time.
5) OTP is sending with time stamp (5 min), and after 5 minutes one time key will be automatically destroy in server side.
6) The parties are sending their information like (email address, mobile number and password) at the time of registration to the server.

Here we are not used PKI (public key infrastructure) so there are needed to the strong authentication for the both parties to the server so we have used concept of OTPK.

NOTATIONS USED

In table 1 show some notations which are used in our proposed protocol.

ISSN: 2455-6203
International Journal of Science Management & Engineering Research (IJSMER)
Volume : 05 Issue : 02 | July - 2020 www.ejournal.rems.co.in

Table 1. Different notations used in algorithm

P_1	Party 1
P_2	Party 2
IDp_1	Identity of p_1
IDp_2	Identity of p_2
K	Common shared key of p_1&p_2
Pw_1	Password of party p_1
Pw_2	Password of party p_2
E_k (M)	Encryption of message m using shared key k
D_k(M)	Decryption of message m using shared key k
r	Random number generated by TTP
S_i	Secret key generated by TTP using TRNG(True random number generation)
H(r)	One way hash function.
M_{key}	Master key which is generated by hash
TTP	Trusted third party
+	Concatenate two values

Our protocol works in three steps which are discussed below. In step 1 we show the communication between party P_1 and trusted third party, in step 2 shows the communication between trusted third party and party P_2 and step 3 shows the communication between party P_1 and party P_2.

Step 1. Communication between party P_1 and trusted third party (TTP) or Server.

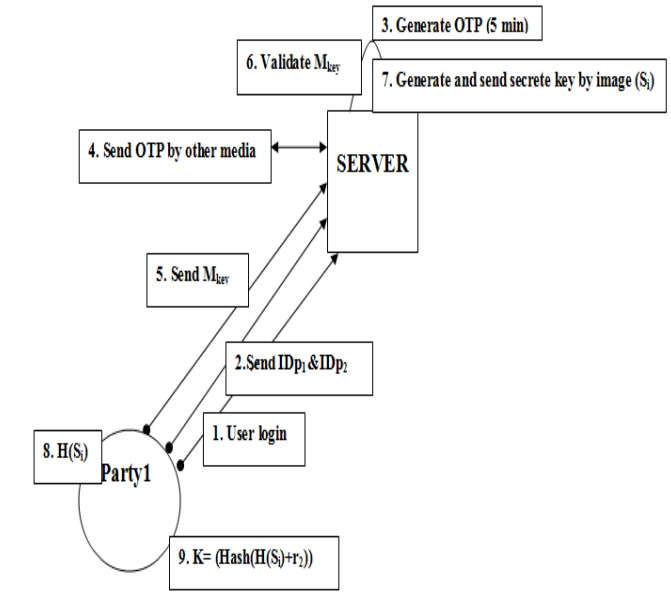
Party P_1 ⟷ TTP

In figure 3 we have shown working module between the party P_1 and trusted third party.

a) User login:

Party P_1 login with Pw_1 and required information to the trusted third party, TTP verify the password and if the password is valid then printing the message user successfully login otherwise print the invalid password message.

ISSN: 2455-6203
International Journal of Science Management & Engineering Research (IJSMER)
Volume : 05 Issue : 02 | July - 2020 www.ejournal.rems.co.in



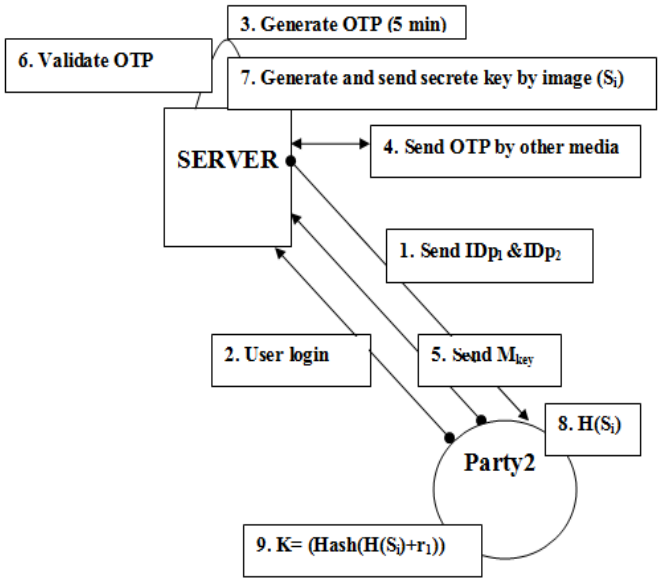


Figure 3: working module between party P_1 and serve

Figure 4: working module between party P_2 and server

b) Send identities:

Party P_1 send the identities (IDp_1 & IDp_2) to the trusted third party, and TTP recognized the identities for further communications.

c) Generate random number r (one time password):

When the above two steps are successfully done the TTP generate random number 'r_1' for the party P_1 with the timestamp (5 minute). That random number r_1 are sent to the party via other media (email).

Note: timestamp (5 minute) means r automatically destroyed in 5 minutes.

d) Party P_1 perform function:

At this stage party P_1 perform some functions like:

i.Generate master key (M_{key})

$M_{key}= H(r_1+Pw_1)$

ii. Keep this random number r_1 in memory.

iii.Send M_{key} to the TTP.

e) Verification:

TTP matched the M_{key} with own calculated M_{key}, if that is valid then server generated images based key (this method describe above in section 4.1 "image based key generation") S_i and calculated hash $H(S_i)$ of this key and send to the party P_1.

f) Session key(K) generation:

$K = Hash(H(S_i) + r_1)$

Party P_1 generated his common session key (K) by the concatenation of $H(S_i)$ and random number r_1.

Step 2. Communication between party P_2 and trusted third party (TTP) or Server.

Party P_2 ⟷ TTP

In figure 4 we have shown working module between server and party P_2.

a) Send identities:

TTP send the identities (IDp_1 & IDp_2) to the party P_2 via other media (mobile or email), party P_2 recognized the identities for further communications and go to process of login.

ISSN: 2455-6203
International Journal of Science Management & Engineering Research (IJSMER)
Volume : 05 Issue : 02 | July - 2020 www.ejournal.rems.co.in

b) User login:

Party P_2 login with Pw_2 and required information to the trusted third party, TTP verify the password and if the password is valid then printing the message user successfully login otherwise print the invalid password message.

c) Generate random number r (one time password):

When the above login process is successfully done the TTP send generated random number 'r_2' for the party P_2 with the timestamp (5 minute). That random number r_2 is sent to the party via other media (email).

Where $r_1 = r_2$;

Note: timestamp (5 minute) means r automatically destroyed in 5 minutes.

d) Party P_2 perform function:

At this stage party P_2 perform some functions like:

i. Generate master key (M_{key})
$M_{key} = H(r_2+Pw_2)$

ii. Keep this random number r_2 in memory.
iii. Send M_{key} to the TTP.

e) Verification:

TTP matched the M_{key} with own calculated M_{key}, if that is valid then server generated image based key (this method describe above in section image based key generation) S_i and calculated hash $H(S_i)$ of this key and send to the party P_2.

f) Session key(K) generation:

$K = Hash(H(S_i) + r_2)$

Party P_2 generated his common session key (K) by the concatenation of $H(S_i)$ and random number r_2.

Here we know $r_1 = r_2$;

So $K = (Hash(H(S_i) + r_1)) = (Hash(H(S_i) + r_2))$

Step 3. Communication between party P_1 and party P_2.

Party P_1 ⟷ party P_2

In figure 5 we have shown working process between two parties party p_1 and p_2 respectively.

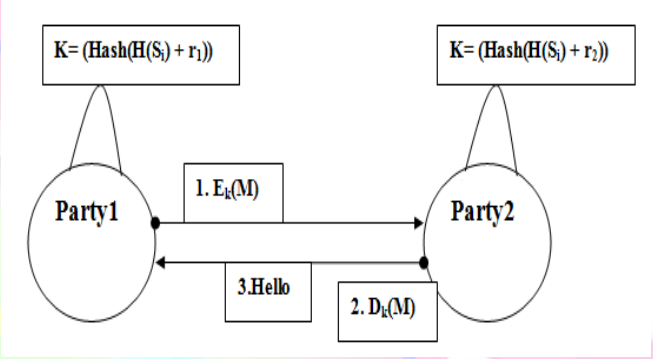


Figure 5: working module between party P_1 and party P_2

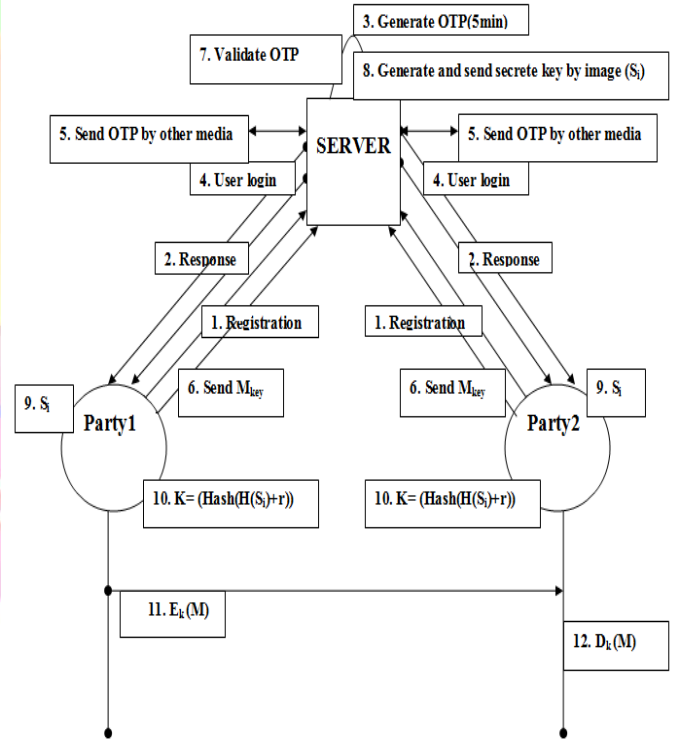


Figure 6. Outline of the proposed technique

ISSN: 2455-6203
International Journal of Science Management & Engineering Research (IJSMER)
Volume : 05 Issue : 02 | July - 2020 www.ejournal.rems.co.in

a) Encryption:
Party P_1 encrypted the message (M) using the common session key K. If party P_2 successfully decrypted the message (M) then confidentiality as well as integrity proof.

b) Decryption:
Party P_2 decrypted the message (M) using the common session key K. if party P_2 successfully decrypted the message then party P_2 confident that the message is coming from party P_1. After that party P_2 sends confirmation message "Hello" to the party P_1. In figure 3, 4 and 5 show the working module of our proposed protocol. In figure 6 shows all the working process of our protocol.

5. RESULT ANALYSIS

Here in this section we have compared our protocol in three parameter basic features and efficiency, security and performance evaluation with the referenced protocols.

5.1 Basic features and efficiency

In the category of basic feature and efficiency, the properties such as transparent TTP or not, offline or online TTP, TTP involvement, fairness, timeliness, additional authentication and storage cost are considered.

Online TTP- A TTP involved during each session of the protocol but not during each message transmission is said to be online.

Offline TTP- A TTP involved in a protocol only in case of an incorrect behavior of a dishonest entity or in case of network problems, is said to be offline.

Timeliness- A protocol provides timeliness if and only if all honest parties always have the ability to reach, in a finite amount of time.

Fairness- The protocol which guarantees the two parties involved to obtain or not obtain the others signature simultaneously is fair.

Parameters	Protocols				
	Verifiable Escrows Based Protocol [16]	Park et. al,'s RSA based protocol [5]	Bao et. al.'s fair contract signing Protocol [3]	DH-BPAKE[15] protocol	Proposed Protocol
Fairness	YES	YES	YES	YES	YES
Timeliness	YES	YES	YES(weak)	YES	YES
Transparent TTP	NO	YES	YES	YES	YES
TTP involvement	Off-line	Off-line	Off-line	On-line	On-line
Additional Authentication	NO	NO	NO	NO	YES
Storage Cost	MORE	MORE	MORE	MORE	LESS
Communication line used	1	1	1	1	2

Table 2: Comparison of basic features and efficiency

ISSN: 2455-6203
International Journal of Science Management & Engineering Research (IJSMER)
Volume : 05 Issue : 02 | July - 2020 www.ejournal.rems.co.in

5.2 Security analysis

In this section, the security of the proposed scheme is examined and it is shown that the proposed protocol has the resilience to several well-known attacks. All security parameters that are necessary for designing the PAKE protocol is taken in the proposed scheme. Such security attributes of the proposed protocol are compared with DH-BPAKE[15] and enhanced DH-BPAKE[12] protocols in table 3. Here, we briefly explain the security properties for proposed protocol.

5.2.1 Forward secrecy: Even if the password of the party P_1 is disclosed, the adversary A cannot still construct the session key since the session key is generated by variable random values r and S_i that modify in every session. The Adversary does not make session key because they do not have the value of S_i, no practical information about the session key will be leaked that is referred to as the forward secrecy property.

5.2.2 Known session key security: The session key is generated from two random numbers r and S_i that are independently selected by the trusted third party. These random numbers will change for every session which is independent of the other sessions. Consequently, the session keys of different session are independent from each other. It is impossible for adversary A to obtain one session key from the disclosed session key of the other sessions. Therefore, the proposed protocol provides the known session key security attribute.

5.2.3 Two factor authentication: When the user is login enters the password pw_1 for party P_1 and first time authenticate to the server, the server sends random number r via other media (mobile or email) user enter the random number and authenticate second time to the server. At this stage two-factor authentication is done.

5.2.4 Resilience to password compromised impersonation attack: Assume that the adversary A reveals party P_1 password and intercepts all the transmitted messages. He/she cannot obtain random value r and random key S_i, so he does not calculate the session key. Consequently, the password compromise impersonation attack cannot take place on the proposed protocol.

5.2.5 Resilience to unknown key share (UKS) attack: The session key is generated by the concatenation of two random values r and S_i which is generated and authenticated by the trusted third party, so any alteration in random numbers corresponding parties will result in a different session key and fail the authentication. Consequently, success probability with UKS attack is negligible.

5.2.6 Resilience to off-line dictionary attack: There is not any obvious password validation information such as a hash function of the password in the entire transmitted message between the parties and server. Thus, the adversary A will not be able to validate the accuracy of his/her guessed password and apply the off-line dictionary attack to the proposed protocol.

5.2.7 Resilience to undetectable on-line dictionary attack: Assume that the adversary A guesses pw_1 as a password of party p_1,but he cannot calculate the M_{key} because it is the combination of password pw and random number r and random value is coming from other secure media (email or mobile), so he/she cannot authenticate to the server because of M_{key} validation failed. Server notice that attack and then stop protocol run with error.

5.2.8 Resilience to replay attack:

The trusted third party independently generates two random numbers r and S_i with the different method, that implicitly and explicitly are used in constructing the session key and other factors. The randomness of such changeable values guarantees the novelty and ensures us that the proposed protocol is secure against replay attack.

Table 3: Comparison of security attributes for the proposed protocol with the DH-BAPKE[15] and enhanced DH-BPAKE[12]

Security attributes	DH-BPAKE protocol[15]	Enhance DH-BPAKE[12]	Our proposed protocol
Forward secrecy	YES	YES	YES
Two factor authentication	NO	NO	YES
Known session key security	YES	YES	YES
Resilience to password compromised impersonation attack	NO	YES	YES
Resilience to unknown key share(UKS) attack	YES	YES	YES
Resilience to off-line dictionary attack	YES	YES	YES
Resilience to undetectable online dictionary attack	YES	YES	YES
Resilience to replay attack	YES	YES	YES
Mutual authentication	YES	YES	YES

5.3 Performance evaluation

This section compares the computational costs of the proposed protocol with DH-BPAKE[15] and enhanced DH-BPAKE[12] protocol. Table 4 shows that the proposed protocol removes the exponential operations, modular multiplication; modular inverse imposed to DH-PAKE[15] and enhanced DH-BPAKE[12] protocols.

Among authentication plays a key role on the protocol rounds. Protocol with mutual strong 2-factor authentication complete in at least three rounds that is considered in our proposed protocol so there is a decrease in the number of protocol rounds from four rounds for the DH-BPAKE[15] protocol to three rounds for our proposed protocol. But it is one round more as compare to the enhanced DH-BPAKE[12] protocol because of it provides 2-factor authentication. The Overall computational cost is less as compare to enhanced DH-BPAKE[12] protocol. The comparison of computational costs of the proposed protocol with DH-BPAKE[15] and enhanced DH-PAKE[12] protocols are summarized in table 4.

ISSN: 2455-6203
International Journal of Science Management & Engineering Research (IJSMER)
Volume : 05 Issue : 02 | July - 2020 www.ejournal.rems.co.in

Protocols	Participants	Exponentiation operation	Random Number Generation	Modular multiplicatio	Modular inverse	Modular addition	Hash Calculation	Number of rounds
DH-BPAKE Protocol[15]	client	2	1	1	1	2	3	4
	server	2	1	1	1	2	3	
Enhanced DH-BPAKE Protocol[12]	client	2	1	0	0	0	3	2
	server	2	1	0	0	0	2	
Our proposed protocol	client	0	0	0	0	0	2	3
	server	0	2	0	0	0	2	

Table 4: Performance comparison of proposed protocol with DH-BPAKE[15] and enhanced DH-BPAKE[12] protocol

6. APPLICATIONS OF PROPOSED PROTOCOL:

In our proposed protocol we have used strong 2-factor authentication PAKE (password authentication key exchange protocol) which can be utilized in various security sensitive areas where needs of very strong authentication.

There are some areas where we can use our protocol significantly:

a) Military:

Our proposed protocol is most suitably used in Defense (military) for sending confidential file or important information one unit to another with strong two-factor authentication.

b) Internet Transactions:

A shopkeeper which operates an internet trading portal requires the user to digitally sign the transaction to signify approval. The User will login to the site using a browser. In such case, the OTPK based authentication works very efficiently, to authenticate an internet based online trusted third party for OTPK certificates.

c) Enterprise eDocuments:

A large enterprise operates an electronic document system to digitize the entire business workflow for processing efficiency. The application requires Microsoft office and PDF documents to be digitally signed during the creation and approval process. For this scenario, the OTPK can be authenticated by the USERID password for the TTP certificate. Some document size is very large and they are very credential, then they need to protocol which sends that document securely one party to another in that place our protocol works very efficiently.

d) Banking Kiosk:

In the banking field, bank server required strong authentication to identify the user identity, so in our protocol we have used strong 2-factor authentication. Banks used smart cards and other physical devices for stronger authentication they are very costly, in our proposed protocol we have used OTPK token for the authentication that is very cheap.

7. CONCLUSION:

In this paper, we have pointed out the previous some password authentication key exchange protocols which have many drawbacks especially failed to provide fully two-factor authentication security. And we have proposed such a secure authentication key protocol that achieves fully two-factor authentication and provide more security of session keys. We have compared our protocol to the some predefined protocols like DH-BPAKE[15] and enhanced DH-BPAKE[12] protocols and analyzed that proposed protocol is much better as compared to these protocols in the areas of basic features and efficiency, security and performance. Our protocol also proposed the security attributes that are necessary for designing the PAKE protocol like forward secrecy, known session key security, password compromise impersonation, Unknown key share (UKS), off-line dictionary, Undetectable on-line dictionary and replay attack. And yet, our scheme is simple and reasonably efficient to the context of share common session key securely.

REFERENCES

[1] Amutha Prabakar Muniyandi, Rajaram Ramasamy, "Password Based Remote Authentication Scheme using ECC for Smart Card", Proceedings of the 2011 International Conference on Communication, Computing & Security, pp. 549-554, 2011.

[2] A. Groce, J. Katz "A New Framework For Efficient Password-based Authenticated Key Exchange", In proceedings of 17th ACM Conference on Computer and Communications Security, pp. 516–525. ACM Press, New York, 2010.

[3] F. Bao, G. Wang, J. Zhou, and H. Zhu, "Analysis and improvement of Micali's fair contract signing protocol," in Proc. ACISP'04, 2004, vol. 3108, LNCS, pp. 176–187, Springer-Verlag.

[4] G. Wang, "An abuse-free fair contract signing protocol based on the RSA signature," IEEE Transactions on Information Forensics and Security, vol. 5, no. 1, pp. 158–168, Mar 2010.

[5] J. M. Park, E. Chong, H. J. Siegel, and I. Ray, "Constructing fair exchange protocols for e-commerce via distributed computation n of RSA signatures," in Proc. PODC'03, 2003, pp. 172–181, ACM Press.

[6] Juan E. Tapiador, Julio C. Hernandez-Castro, "Cryptanalysis of Song's advanced smart card based password authentication protocol", 2010. Online available: http://arxiv.org/pdf/1111.2744.pdf.

[7] J. Xu, W.-T Zhu, and D.-G Feng. “An improved smart card based password authentication scheme with provable security.” Computer Stan- dards & Interfaces 31, pp. 723–728, 2009.

[8] Jan Camenisch, Anna Lysyanskaya, “Practical Yet Universally Composable Two-Server Password Authenticated Secret Sharing”, Proceedings of the 2012 ACM conference on Computer and communications security, pp. 525-536, 2012.

[9] J. Katz, R. Ostrovsky, and M. Yung “Efficient and Secure Authenticated Key Exchange Using Weak Passwords”. Journal of the ACM, Vol. 57, issue 1, pp. 78–116, 2009.

[10] J. Katz and V. Vaikuntanathan “Password-based Authenticated Key Exchange Based on Lattices”, In Advances in Cryptology, volume 5912 of LNCS, pp. 636–652. Springer, 2009.

[11] Kyung-kug Kim, “An Improved Anonymous Authentication and Key Exchange Scheme”, Proceedings of the CUBE International Information Technology Conference, pp. 740-743, 2012.

[12] Maryam Saeed, Hadi Shahriar Shahhoseini, “An Improved two-party Password Authenticated Key Exchange Protocol without Server's Public Key”, IEEE 3rd International Conference on Communication Software and Networks (ICCSN-2011), pp. 90-95, 2011.

[13] Matthew A. Ezell, Gary L. Rogers, “A Framework for Federated Two-Factor Authentication Enabling Cost Effective Secure Access to Distributed Cyberinfrastructure”, Proceedings of the 1st Conference of the Extreme Science and Engineering Discovery Environment: Bridging from the eXtreme to the campus and beyond, article no 7, 2012.

[14] M. Saeed, H.S. Shahhoseini, "APPMA - An Anti-Phishing Protocol with Mutual Authentication", Proceedings of the 15th IEEE Symposium on Computers and Communications (ISCC20 10), pp. 308-313, June. 2010.

[15] M.A. Strangio, “An optimal Round Two-Party password-Authenticated Key Agreement protocol,” proceeding of the first IEEE International Conference on Availability, Reliability, and Security (ARES’06), pp.216-223, April. 2006.

[16] N. Asokan, V. Shoup, and M. Waidner, “Optimistic fair exchange of digital signatures,” IEEE J. Sel. Areas Commun., vol. 18, no. 4, pp. 591–606, Apr. 2000.

[17] Patrik Bichsel, Jan Camenisch, “A Calculus for Privacy friendly Authentication”, Proceedings of the 17th ACM symposium on Access Control Models and Technologies, pp. 157-166, 2012.

[18] S. Patel. Information leakage in encrypted key exchange. In Proceedings of the DIMACS Workshop on Network Threats, 1997.

[19] S. Patel. Number theoretic attacks on secure password schemes. In Proceedings IEEE Symposium on Security and Privacy, pages 236–247, 1997.

[20] W B Horng and Cheng p Lee, 2010 “Security weaknesses of song’s advanced smart card based Password authentication Protocol”, IEEE International Conference on Informatics and Computing (PIC), pp. 477-480, 2010 .

[21] Wei-Kuo Chiang and Jian-Hao Chen, “TW-KEAP: An Efficient Four-Party Key Exchange Protocol for End-to-End Communications”, Proceedings of the 4th international conference on Security of information and networks, pp. 167-174, 2011.

[22] Wang, Y.G.: “Password protected smart card and memory stick authentication against off-line dictionary attacks”. Information Security and Privacy Research IFIP Advances in Information and Communication Technology, vol. 376, pp. 489–500. Springer Boston, 2012. Available at http://coitweb.uncc.edu/ yonwang/papers/smartcard.pdf.