An Efficient multiparty Group Key Transfer Protocol using OTPK

Pratiksha Nadhe, Vinay Sahu, Anurag Jain

Abstract— Security is an important concern during the transmission of data whether in wired or in wireless communication. Since various techniques are implemented for the secure communication but various attacks are possible in these techniques. Here in this paper a more secure authentication using two factors is proposed. The techniques uses one time private key and image based authentication to provide security from various attacks. A secure Group key transfer between client and server which is based on secrete sharing secure channel is also proposed. The technique provides better authentication and security from DDOS attack, replay attack, password impersonation, and guessing attack**.**

Index Terms— OTPK, KGC, TTP, DOD, DDOS, SPAKE1, SPAKE2.

.

1 INTRODUCTION

Security in computers is information protection from unauthorized or accidental confession while the information is in transmission and storage. Authentication protocols provide two entities to make certain that the counteract social gathering is the intended one whom he challenges to communicate within excess of an insecure network. These protocols can be think about from three dimensions: category, competence and safety measures. In general, there are two types of authentication protocols, the password-based and the public-key based. In a password based protocol, a user registers his account and password to a remote server. Afterward, he can right of entry the remote server if he can prove his knowledge of the password. The server usually maintains a password or verification table but this will make the arrangement easily subjected to a stolen-verifier attack. To attend to this problem, latest studies suggest an approach without any password or verification table in the server. Moreover, to improve password protection, recent studies also introduce a tamper-resistant on (OTPK) in the user end.

As far as protected message communication is concern message authentication and confidentiality is essential. Message confidentiality makes sure the sender that the message can be read only by an intended receiver. Message authentication makes sure that the receiver that the message was sent by a specified sender and the message was not altered route. Due to these two functions, one-time session keys need to be combined among communication entities to encrypt and confirm messages. As a consequence, before exchanging communication messages, a key establishment protocol could do with distribute one-time secret session keys to all take a part of entities. The key establishment protocol also could do with to provide confidentiality and authentication for session keys [1].

Many group-oriented applications require communication confidentiality, meaning that the communication data among a group of authorized members are secure and inaccessible to group outsiders. Examples of these applications include secure chat-rooms, business conferencing systems, file sharing tools, programmable router communication and network games in strategy planning. To offer data privacy, an effective approach is to require all group members to establish a common secret group key, which is held only by group members, but not outsiders, for encrypting the transmitted data. There are two kinds of key establishment protocols: key transfer protocols and key agreement protocols. Key transfer protocols are mutually trusted key generation center (KGC) to select session keys and then transport session keys to all communication thing behind somebody's back. A large amount frequently, KGC encrypts session keys under another secret key shared with each person during listing. In key agreement protocols, all communication entities are occupied to agree on session keys [1].

In particular, rekeying, or renewing the group key, is necessary whenever there is any change in the group membership (e.g., a new member joins the group or an existing member leaves the group) in order to guarantee both backward confidentiality (i.e., no joining member can read the previous data) and forward confidentiality(i.e., no leaving member can access the future data).One simple way for a communication group to perform rekeying is to set up a centralized key server that is responsible for renewing the group key and distributing it to all group members.

When a secure communication occupies more than two units, a set of key is needed for all group members. A large amount distinguished group key management protocols can be classified into two categories. (a) Centralized group key management protocols: a group key production center is engaged in managing the entire group. (b) Distributed group key management protocols: there is no unambiguous group key distribution center, and each group associate can contribute to the key generation and distribution. The class of centralized group key management protocols is the large amount extensively used group key management protocols [1].

2 ONE TIME PRIVATE KEY

Although there are various techniques implemented that are needed for the secure transmission of data 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 send securely.

One such concept of providing a strong authentication is using key generation using one time private key. As we know that key is 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 [2]. In the concept of key generation using OTPK during the generation of key 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 send securely the key gets destroyed.

3 LITERATURE SURVEY

In year 2013, Bhagyashree Bodkhe, Ms. Pallavi Jain here they proposed a new contract signing protocol is proposed based on the OTPK (one time private key) method. This protocol will allow two parties to switches their digital signature between them by signing contract. The proposed protocol make certain equality such that either both parties receive each other's signatures or neither of them. The proposed protocol employs offline Trusted Third Party (TTP) that will be brought into play only if one party is take advantage of in other case, the TTP continues inactive. The design is to use a better authentication between two parties in which a token is send to the TTP in reply to that one private key is produced that is make use of for the authentication between two parties and after a convinced amount of time that key has be destroyed. Consequently with OTPK method that the key is not stored at any place so the storage cost will be reduced. This protocol not only solve the problem of single point of failure by using multiple TTP's but allocate the key to until the end of time continues in client possession all the way through the short life span, and not at all stored on a permanent basis so it help in reducing the storage cost and thus providing security against various attacks [3].

In year of 2012, Vijaya lakshmi Pandranki and N. Krishna proposed Secure Group Key Transfer Protocol Based on Secret Sharing. They propose a solution based on Group key transfer protocol move toward and make available confidentiality and authentication for allocating group keys. According to this move toward, each user could do with to schedule at KGC to promise the group key transfer service and to launch a secret with KGC. Consequently, a secure channel is necessitating to begin with distributing this secret with each user. Afterward, KGC can convey the group key and interact with all group members in a broadcast channel. The confidentiality of group key allocation is information hypothetically secure; that is the security of this transfer of assembling key to each group member does not depend on any computational statement. The confirmation of the group key is accomplished by broadcasting single authentication significance to all group members [4].

This confirmation of group key transfer protocol consists of three methods: initialization of KGC, user registration, and set of key generation and distribution. In initialization procedure they decide two protected prime numbers p and q. Subsequently each user is required to register at KGC for promise the key distribution service. The KGC maintains way all scheduled users and do away with any.

unsubscribed users. Upon receiving a collection key making apply for from any user, KGC necessitates to indiscriminately decide on a group key and admittance all contribute to secrets with group members. KGC could do with to allocate this collected key to all group members in a secure and authenticated manner. All messaging between KGC and group members are in a broadcast channel. Every user needs to register at a trusted KGC to begin with and pre-share a alternative with KGC. KGC broadcasts group key information to all group members at one time. The confidentiality of this group key distribution is information tentatively make safe [4].

In year 2012, Vinod Moreshwar Vaze, has give emphasis to OTPK here they suggest on the requirement of advanced protection has moved the order for improved the safety measures solutions. One Time Private Key (OTPK) permits the users to create their signing keys and use their strong authentication to confirm the signing keys and sign the document, after this the signing keys will be wiped away [5].

The OTPK system is a model reallocate in PKI technology. It illustrates a easy and protected mechanism to arranged a large number of documentations across a large user base all over the world with reasonably minute charge and logistics. OTPK technology brings a new concept in which a user will generate a signing key with low cycle time (= key generation+ certificate request+ digital signing) takes less than 7 sec. The OTPK concept is simple to recognize. Whenever a digital signature is required, the private key is produced, certified, used to calculate the digital signature and immediately deleted [5].

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 [6].

In 2012, Wang, Y.G. 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 most important reason of the exceeding disappointment. For that reason, Wang presented three kinds of safety measures models, namely Type I, II and III, and additionally 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 [6].

In 2012, Aruna Averneni and Y.V.V.N. Vara Prasad offered an Authenticated Group Key Transfer Implementation Protocol Based on Secret Sharing. The KGC keeps tracking all registered users and take away any unsubscribed users. All through registration, KGC contribute to a secret with each user. In a large amount key transfer protocol, KGC encrypts the accidentally selected group key underneath the secret shared with each user during registration and sends the cipher text to each group associate independently. An authenticated message checksum is emotionally involved with the cipher text to provide group key authenticity. In this come close to, the confidentiality of group key is make sure that using any encryption algorithm which is computationally make safe. This protocol uses underground sharing proposal to replace the encryption algorithm [7].

In year 2011, Shuhua Wu and Yuefei Zhu suggested Improved Two-Factor Authenticated Key Exchange Protocol. They show that it is especially true in the cases of all these protocols. More specifically, if only the smart-cart (one factor) is compromised, the adversary will be able to break these schemes completely. Moreover, the adversary can even know session keys established before the corruption as well in the two schemes. Secure authenticated key exchange protocol that achieves fully two-factor authentication and provides forward security of session keys [8].

This scheme is still a secure password-based authenticated key exchange protocol that can protect the password information against dictionary attacks and guarantee the confidentiality of the session keys. Until at this instant, this method is simple and reasonably efficient. Firstly, this proposal uses just the once instead of timestamps to put off replay attacks and thus avoids the clock synchronization problem. In addition, this scheme allows each uses to change their password freely without any interaction with the sever. Secondly, our scheme simply utilizes each user's unique identity to accomplish authentication. Thus, the server does not need to maintain a large users' keys table while the number of users becomes very large. Thirdly, we can provide the rigorous proof of the security for our scheme. Actually, many previous cryptographic schemes containing only informal arguments for security were subsequently unsecured [8].

This protocol protects information broadcasted from KGC to all members. Here the service request and challenge messages are not authenticated. An attacker can impersonate a user to request for a group key service. Attacker can also modify information transmitted from users to KGC exclusive of being distinguished. Receiving upon a group key making ask for from any user, KGC needs to indiscriminately selects a group key and right to use all shared secrets with group members. KGC requires distributing this group key to all group members in a protected and verified manner. Key transfer protocols rely on a jointly trusted *key* generation center (KGC) to choose session keys and transport session keys to all communication entities secretly. A large amount regularly, KGC encrypts session keys underneath another secret key shared with each abd individual for the period of registration [9].

In the same year, A.B.Surekha & C.Shoba Bindu suggested Heterogeneous Tree Based Authenticated Group Key Transfer Protocol. Public keys of the communication entities play a key role in this protocol. They are exchanged to fix the value of session key. As the public key itself does not provide authentication, uses a digital signature. But the only drawback is that this is on whole applicable only two 2 users but not to a group. The importance of group key is found here as everyone ought to have it. This group key management protocol can be of 2 categories. Centralize group key management protocols, where the whole group is managed by a Group Key generation. Distributed group key management, where each individual manages the generation of key rather than a group key distribution [10].

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 has been implemented which can provide several security attributes while it has a remarkable computational efficiency and lower number of rounds. In [11], it is established that the Hitchcock et al.'s protocol is susceptible to transient key negotiation masquerade, off-line dictionary and Key Compromise Impersonation (KCI) attacks at the same time as it does not provide the mutual authentication and forward confidentiality attributes. It is also exposed that SPAKEI and SPAKE2 protocols are susceptible 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 [11].

In 2009 by S. Wanga, Z. Cao, K.-K. Choo, and L. Wang, The first formal security model for authenticated key exchange protocols between two parties. The latter has been extended to the password-based setting with security analyses of the above 2-party password-based key exchange, under idealized assumptions, such as the random oracle and the ideal cipher models. Password-based schemes, provably secure in the standard model, have been recently proposed but only for two parties. They believed that password-based protocols in the three party setting, but nobody of their proposals enjoy provable security. In fact, our generic construction seems to be the first provably-secure 3-party password-based authenticated key exchange protocol [12].

4 PROPOSED METHODOLOGY

The secure authentication using OTPK provides secure communication between parties. Her we are using the concept of OTPK with image based authentication.

4.1 NOTATIONS USED

r1	Random value of party P1
r2	Random value of Party p2
Pk1	Secrete key of P1
Pk2	Secrete key of P2
m1	Master key of P1
m2	Master key of P2

Table 1. Different notations used in algorithm.

1. First of all both the parties agreed on a pattern and chooses a random value r1, and r2 and send over the secure channel to the Server
2. TTP will generate a secrete Pk1 and Pk2 to both the parties that can be used as a Master Key for both the parties.

   Pk1=hash (r1)
   Pk2=hash (r2)

3. The party p1 will generate

   m1=sig1 (Pk1, Pk2, text, hash (r1))

4. The party p2 will generate

   m1=sig1 (Pk1, Pk2, text, hash (r1))

5. Both the parties will generate their master keys and send to the server over a secure channel.
6. Server will verifies both the parties, if the master keys generated are equal or not, if not terminate the process.
7. As soon as the parties get authenticated, it will a image and generate a key from the image pixels and using OTPK it will generate master key.
8. The parties also using the image and OTPK generate a key and send to the server.
9. The server verifies the keys and hence the second factor authentication verifies.

Here we are implementing the concept of 2 Factor authentication using OTPK and image based authentication.

Image based Authentication

1. Scan pixel values of image from top to bottom and left to right.
2. Concatenating the value to generate random number consisting of 0's & 1's.
3. We can apply any rule for deriving random numbers like XOR, mapping, discarding etc.
4. Random value can be generated by concatenating columns only or rows only or rows and columns.
5. Similarly unique values can be generated for multipartite from the same image for authentication

R RESULT ANALYSIS

As shown in the below table is the comparative analysis enhancement of the [2]. The analysis of different protocols that follows contract signing between two parties.

Parameters	Protocols				
	Escrows Based Protocol	Park et. al,'s RSA based protocol	Bao et. al.'s Protocol	Contract Signing Protocol based on RSA	Proposed Scheme
Replay attack	YES	YES	YES	YES	YES
Timeliness	YES	YE	YES(weak)	YES	YES
Multiple TTP	YES	YES	YES	YES	YES
Man-in-middle	[3]	[6]	[7]	[1]	YES
Confidentiability	[3]	[6]	[7]	[1]	YES
Additional Authentication	NO	NO	NO	NO	YES
Storage Cost	MORE	MORE	MORE	MORE	LESS

Table 2. Comparison of different Contract Signing Protocols

Security Parameter	Prevented by proposed techniuqe
Public verifiability	YES
Password impersonation	YES
Insider attack	YES
Outsider attack	YES
Password guessing attack	YES
Denning sacho attack	YES

Table 3. Other additional security analysis

As shown in the figure below is the number of keys generated as the party signs the protocol. Each time a party is new or old the keys generated is new. Since, here the key pair is not repeated for any party

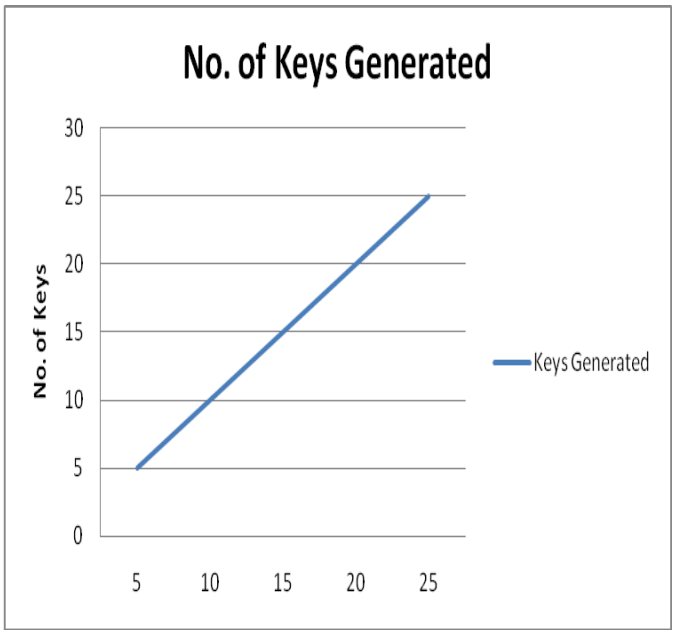

Figure. 3. Number of Keys generated according to parties

Images	Image Size	Time in ms
image1	19KB	210
image2	827KB	506
image3	582KB	615
image4	758KB	433
image5	763KB	592
image6	549KB	597
image7	760KB	894
image8	607KB	523

Figure 4. Time Computation of Image key generation

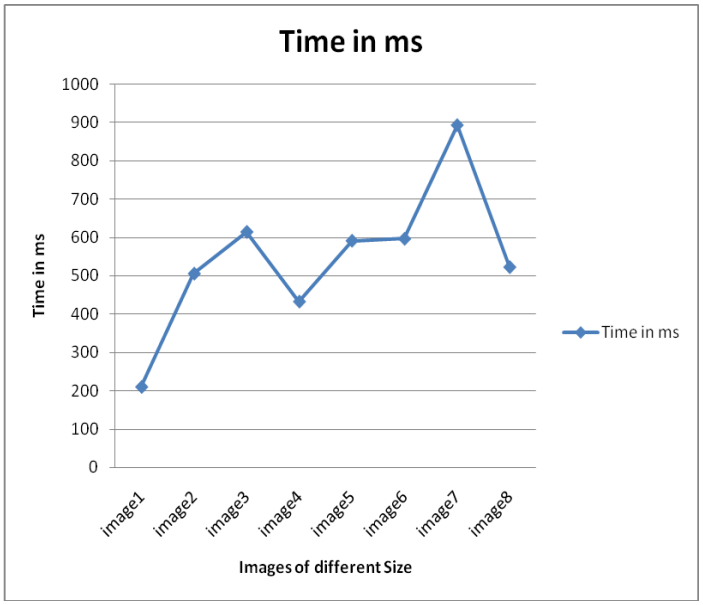

Figure 5. Generation of Time from image key

CONCLUSION

The proposed technique provides two factor authentication using One Time Private Key and Image based key generation. The proposed technique provides prevention from various attacks such as replay attack, DDOS attack and various attacks. The result analysis shows the performance of the proposed technique.

REFRENCES

[1] Vijaya lakshmi Pandranki, N. Krishna "Secure Group Key Transfer Protocol Based on Secret Sharing", International Journal of Computer Science and Information Technologies (IJCSIT), ISSN: 0975-9686, Vol. 3, issue 4, pp. 4712 – 4717, 2012.

[2] Vinod Moreshwar Vaze," Digital Signature on-line, One Time Private Key [OTPK]", International Journal of Scientific & Engineering Research Volume 3, Issue 3, March -2012 1 ISSN22295518".

[3] Bhagyashree Bodkhe,Ms. Pallavi Jain,"Token Based Contract Signing Protocol using OTPK" International Journal of Computational Engineering Research Vol, 03,Issue, 4 Pg. no: 43-46,2013.

[4] Journal of Computer Science and Information Technologies (IJCSIT), ISSN: 0975-9686, Vol. 3, issue 4, pp. 4712 – 4717, 2012.

[5] Vinod Moreshwar Vaze, "Digital Signature on-line, One Time Private Key [OTPK]" International Journal of Scientific & Engineering Research Volume 3, Issue 3, March -2012, ISSN 2229-5518.

[6] 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.

[7] Aruna Averneni, Y.V.V.N. Vara Prasad "Authenticated Group Key Transfer Implementation Protocol Based On Secret Sharing", Asian Journal Of Computer Science And Information Technology, ISSN: 2249-5126, vol. 2, No. 4, pp. 47- 51, 2012.

[8] Shuhua Wu and Yuefei Zhu "Improved Two-Factor Authenticated Key Exchange Protocol", The International Arab Journal of Information Technology, Vol. 8, No. 4, pp. 430 – 439, October 2011.

[9] Aruna Averneni, Y.V.V.N. Vara Prasad " Authenticated Group Key Transfer Implementation Protocol Based On Secret Sharing", Asian Journal Of Computer Science And Information Technology, ISSN: 2249-5126, vol. 2, No. 4, pp. 47- 51, 2012.

[10] A.B.Surekha & C.Shoba Bindu "Heterogeneous Tree Based Authenticated Group Key Transfer Protocol", Global Journal of Computer Science and Technology, Volume 12, Issue 7, 2012

[11] 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.

[12] S. Wanga, Z. Cao, K.-K. Choo, and L. Wang, "An improved identitybased key agreement protocol and its securi-

ty proof," An International Journal of Information Sceinces,
vol. 179, pp. 307-318, January. 2009.