TWO-PARTY PASSWORD AUTHENTICATED KEY EXCHANGE PROTOCOL USING OTPK

[1]Pritaj Yadav, [2]Dr. Sitesh Kumar Sinha, [3]Dr. S. Veenadhari
[1]Research Scholar, [2]Professor, [3]Associate Professor
[123]Department of Computer Science & Engineering, Rabindranath Tagore University, Bhopal, India

Abstract- In this paper introduce the combinatorial method of password authentication key exchange (PAKE) without public key of severs side. Password Authenticated Key Exchange protocols enable two entities to agree on a common session key based on a pre-shared human memorable password. An efficient secure two-party PAKE protocol is designed to provide several securities attributes while the efficiency is also improved. In this implement an efficient key exchange mechanism using concept of an efficient secure two-party PAKE protocol is designed to provide several securities attributes while the efficiency is also improved. Here we are implementing a new technique of authentication between two parties on the basis of One Time Private Key**.**

Keywords: **PAKE, Authentication, Validation, Security, One Time Private Key, Session Key, Data Sharing**

I. INTRODUCTION

Password Authenticated Key Exchange (PAKE) allows two communication entities to certify one another and established a session key via simply memorable passwords. The primary PAKE protocol was introduced by Bellovin and Merritt in 1992 referred to as Encrypted Key Exchange (EKE).

Two-party password-based attested key exchange (two-PAKE) protocol is comparatively helpful for client-server architectures. However, in large-scale client-client communication environments wherever a user must communicate with a great deal of different users, Two-PAKE protocol is incredibly tough in key management that the amount of passwords that the user would wish to memories. A multilateral password-based key transfer protocol using server's public key. Later, a multilateral PAKE (three-PAKE) protocol between two clients while not server's public key.

Security in computers is info defense from unauthorized or accidental revealing whereas the info or the knowledge or the data is in transmission and whereas information is in storage. Authentication protocols give two entities to form certain that the counterparty is anticipated one whom he makes an attempt to communicate with over a diffident network. These protocols are often thought of three dimensions: sort, potency and security.

In general, there are two forms of authentication protocols, the password-based and therefore the public-key primarily based. During a password primarily based protocol, a user registers his account and password to a remote server. Later, he will access the remote server if he will prove his information of the password. The server sometimes maintains a password or verification table however this can build the system simply subjected to a stolen-verifier attack. To deal with this drawback, recent studies recommend an approach with none password or verification table within the server. Moreover, to reinforce password protection, recent studies conjointly introduce a tamper-resistant smart card within the user end. During a public key-based system, a user ought to register himself to a trust party, named KGC (Key Generation Center) to get his public key and corresponding non-public key. Then, they'll be recognized by a network entity through his public key. To modify the key management, an identity-based public-key cryptosystem is sometimes adopted, during which KGC problems user's ID as public key and computes corresponding non-public key for a user.

In this section discusses the introductory a part of the subject of the paper, remainder of the discusses only once non-public key in section II, in section III discusses the recent implements and their results, projected methodology discusses within the section IV, projected methodology results and their discussion i.e. comparison depict within the section V, last however not the smallest amount conclusion discusses within the section VI.

II. ONE TIME PRIVATE KEY

Although there are numerous techniques enforced that are required for the secure transmission of knowledge from the sender to the receiver. Throughout the transmission of knowledge from the sender to the receiver security plays a very important role as a result of the possibilities of attacks within the network are additional. Thence to beat these limitations there are security techniques enforced for the secure transmission of knowledge. Authentication is additionally one in all the technique through that the info are often send firmly.

One such conception of providing a powerful authentication is using key generation victimization just once personal key. As we all know that key's vital part for the authentication of the info wherever the sender and receiver uses his own key for the authentication, however if these keys can't be created robust then such techniques isn't a secure one. within the conception of key generation victimization OTPK throughout the generation of key by the sender or receiver or by any third party a secret's generated for the authentication or for the coding of knowledge or the info or the information for the coding a secret's used and as shortly because the sender and therefore the receiver gets attested and data is send firmly the key gets destroyed.

III. RECENT DEVELOPMENTS

Zhang Gegei et al. [1]: In this paper propose a general construction for KE protocols using smart card and password. The KE protocols generated from our construction can be used in various public key environments as a basic module. This new construction also satisfies the AKE security mentioned by Bellare, so that it can resist several attacks including off-line dictionary attack, while many other protocols can't. Applying their construction to the Diffe-Hellman integrated encryption scheme (DHIES) mentioned by M. Abdulla et al. a KE protocol can be obtained, which has not only better security properties, but also better computational efficiency in storage cost and operation time.

Qi Xie et al. [2]: In this paper, planned an Anonymous Two-Factor AKE theme that preserves security against varied at- tacks together with de-synchronization attack, lost-smart-card attack and password estimation attack, and supports many fascinating properties together with excellent forward secrecy, obscurity or un-traceability, adaptively password modification, no centralized password storage, and no long public key. Furthermore, our protocol maintain high efficiency in terms of storage demand, communication value also as process complexness. Our protocol needs solely a couple of or some or many number of message flows and every one transmitted messages are short in size. Additional, the planned theme is incontrovertibly secure in our extended security model of AKE. Therefore, the planned theme is appropriate for readying in varied low-power networks, specially, the pervasive and mobile computing networks.

Hung-Min Sun et al. [3]: Planned a shoulder- surfing resistant authentication system supported graphical passwords, named Pass-Matrix. Employing a one-time login indicator per image, users will signifies the placement of their pass-square while not directly clicking or touching it that is associate action prone to shoulder surfing attacks. as a result of the look of the horizontal and vertical bars that cowl the complete pass-image, it offers no clue for attackers to slender down the word area notwithstanding they need quite one login records of that account. Moreover, we tend to enforce a Pass-Matrix model on mechanical man and dispensed user experiments to judge the memorability and usefulness. The experimental result showed that users will log into the system with a mean of 1:64 tries (Median=1), and also the Total Accuracy of all login trials is 93:33% even fortnight when registration. The overall time consumed to log into Pass-Matrix with a mean of 3:2 pass-images is between 31:31 and 37:11 seconds and is taken into account acceptable by 83:33% of participants in our user study.

Based on the experimental results and survey knowledge, Pass-Matrix could be a novel and easy-to-use graphical password authentication system, which might effectively alleviate shoulder-surfing attacks. Additionally, Pass-Matrix is applied to any authentication state of affairs and device with straightforward input and output capabilities. The survey knowledge within the user study conjointly showed that Pass-Matrix is sensible within the globe.

R. Madhusudan et al. [4]: In this paper, presented the cryptanalysis of Wen and Lis an improved dynamic ID based remote user authentication scheme with key agreement, and identified its vulnerability. To overcome the security problems, we proposed improved scheme. Through security analysis, we have explained that, our scheme gives protection from all pointed weaknesses. By performance analysis, we compare the computation cost of our scheme with Wen and Li's scheme and illustrated that our scheme reduces 6 hash function, than their scheme. Hence our scheme is more efficient, particularly for user privacy, amplified security and low computation capability.

Zheng Xian Gao et el. [5]: In this paper, briefly reviews the recently development of Dynamic ID-based user authentication scheme using smart card. Then, they have reported security vulnerabilities on three well-designed remote user authentication schemes (Gao-Tu scheme, 2008; Yeh et al. scheme, 2010; Khan et al. scheme, 2011). Based on their cryptanalysis, Gao-Tu scheme is confronted with some threats including smart card forge attack, impersonation attack and message forge attack; Yeh et al. scheme cannot defend against smart card forge attack, impersonation attack and replay attack; insecure against resembling account attack, session key compromise attack and impersonation attack. In addition, we demonstrate some interesting issues on dynamic ID-based authentication scheme using smart cards. Furthermore, they have defined all the security requirements and all the goals an ideal password authentication scheme should satisfy and achieve, which is useful for the authentication scheme designers.

Xinyi Huang et al. [6]: This paper revisited the protection of two password attested key agreement protocols victimization sensible or smart cards, Whereas they were assumed to be secure, and tend to showed that these protocols are flawed beneath their own assumptions severally. specially, tend to took into consideration some forms of adversaries that weren't thought-about in their styles, e.g., adversaries with pre-computed information keep within the smart-card and adversaries with totally different or completely different information (with relevancy different time slots) keep within the sensible or smart-card. These adversaries represent the potential threats in distributed systems and are completely different from the ordinarily famed ones, that we tend to believe be the eye from each the world and also the trade. They tend to conjointly propose the solutions to fix the protection flaws. Their results highlight the importance of elaborate security models and formal security analysis on the planning of password-authenticated key agreement protocols victimization or using sensible or smart cards.

XioyiDuan et al. [7]: In this paper, they introduce three recent proposed authentication schemes using smart cards, and point out some weaknesses in these schemes such as smart card forge attacks, impersonation attack, message forge attack, replay attack and resembling account attack, etc. Furthermore, some advanced topics about dynamic ID-based authentication scheme are discussed and demonstrated which is useful for the authentication scheme designers.

Hsieh-Tsen Pan et al. [8]: Proposed an economical dynamic ID based mostly remote user password authentication theme for multi-server atmosphere. They claimed that his theme resisted completely different potential attacks embrace off-line identity guess attack, off-line countersign guess attack, and charge account credit purloined attack. However, we discover some

weaknesses of his theme during this article. They show that his theme is susceptible to off-line identity guess with charge account credit purloined attack and off-line countersign guess with charge account credit purloined attack.

IV. PROPOSED METHODOLOGY

This section revisited the privacy of two-factor PAKA (Password Authenticate Key Agreement) protocols through sensible (smart) cards. While they will have assumed to be secure, we shows that these protocols are flawed under their own assumptions respectively.

In particular, we take into account some kinds of adversaries which will not considered in existing designs or methodology, e.g., challengers with pre-calculated data saved like (registration info, and other related information of account and user identification) in the sensible-card and challengers with different information (with respect to dynamic time slots) saved in the sensible (smart) card.

These challengers represent the potential threats (means of a determination to inflict harm on another) in distributed systems and are different which attention from both the academia and the industry. We will also developing or designing the solutions to fix these security flaws. So propose several analysis, simulation results of our proposed methodology of password based smart card verification has highlight the importance of elaborate or brief analysis the security models and general security analysis on the design of PAKE protocols using smart cards.

The proposed methodology has some main objectives are as follows; firstly provide security from the un-authorized activities i.e. malicious network, authenticated or efficient techniques, less computational time and also less storage cost or value of the system.

In this proposed solution have two important phase to overcome the limitation of existing authentication password based scheme. First one registration i.e. verification and second one is actual signing. Flowchart for proposed solution shown in the figure 1.

Let us considering the first phase registration: Two factor authentication OTP token generated for the client or User through various communication link i.e. SMS, E-Mail, this procedure enhance focus or impact security. Another verification like face to face verification will take place in this stage if needed. This two factor authentication OTP token permit the user to certification authority or registration authority to authenticate during the certification process. For the first phase can also considered the biometric authentication under some circumstances whereas this biometric process authentication i.e. remote authentication is secure and safe. That is OTPK not only restricted to two factor authentication OTP, but this kind of authentication credentials would be time bounded to ensure for the fresher certificate request.

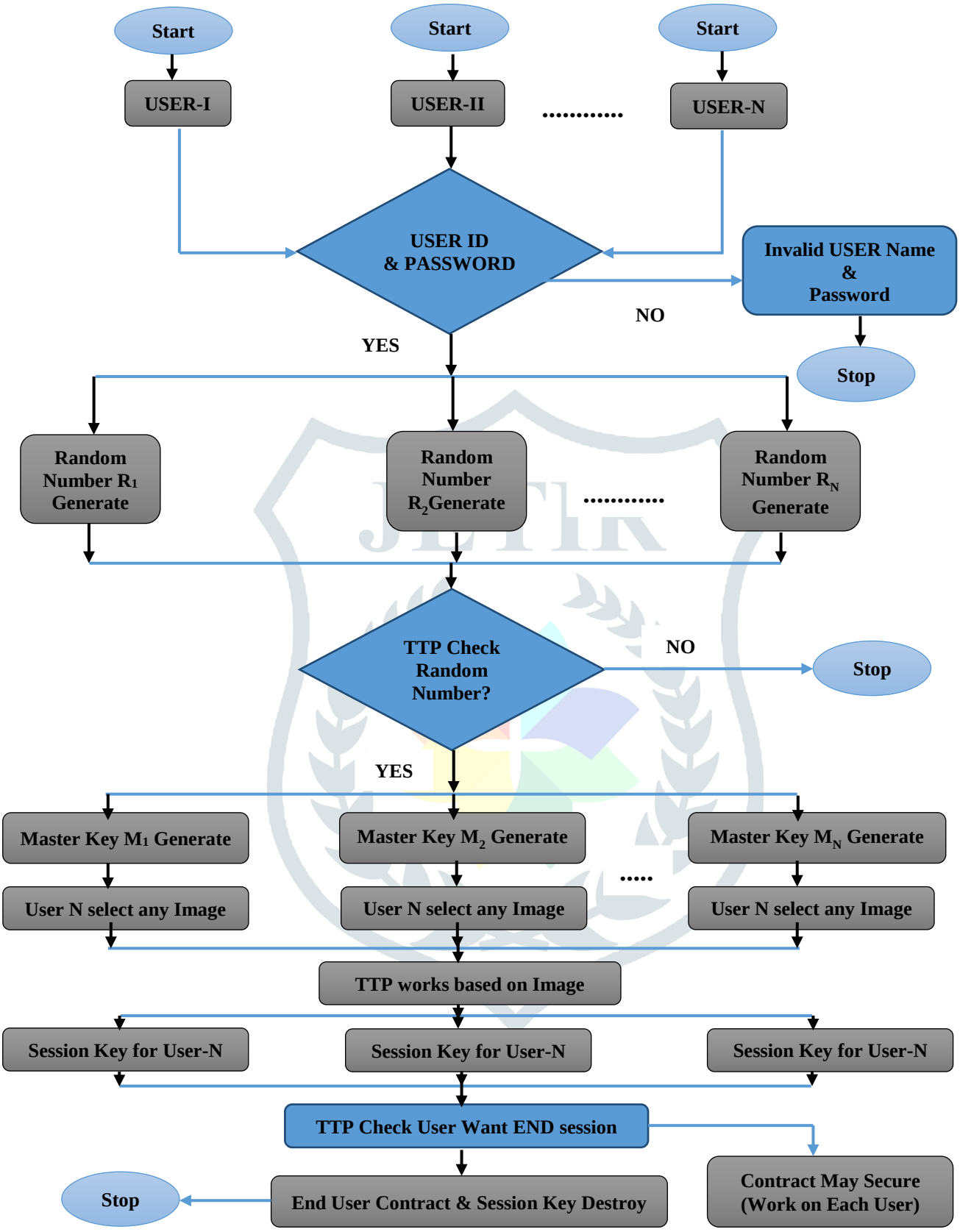


Figure 1: Flowchart for Proposed Methodology

Second Phase Signing: As know that the every transaction needed a digital signature i.e. an asymmetric decrypt operation. For completion of this process need to be download the OTPK module. This downloaded OTPK module would provide or generate public and private key pair, two factor authentication credential OTP for prompt the user, and also done embedding process within the certification request i.e. merge or embed or decrypt the two factor authentication OTP credential and the transaction hash (for time-stamping), in this second phase singing the system would have to encrypted the end to end certification request for

the certification authority or registration authority and then this certification request which were end to end encrypted send to the certification authority or registration authority. At last this certification request verify by the certification authority or registration authority via two factor authentication credentials and transaction credential i.e. very short period, provide a transaction hash and time purpose certificate, after that module back return to the digital signature of transaction and delete the private. Now User has a certificate and digital signature.

The running process of OTPK (One Time Private Key) PKI: Application server sends the record to be signed to the purchaser server (person) for Digital Signature. The consumer downloads OTPK module and enter Two Factor Authentication (2FA) details. (Inserts the cardboard/ token/ pen pressure / carry out the biometrics as given & told by using Certificate Authority (C.A.) / or Registration Authority (R.A.)). The consumer follows the instructions given via on line C.A. / R.A and Generate Certificate request the Digital Signature is created and application server, from time to time, uses OCSP protocol for look-up and follows up.

Algorithm (True Random Number Generation)

Scan pixel values of photo from pinnacle to bottom and left to proper.

[1] Concatenating the fee to generate random quantity which includes 0's & 1's.

[2] We can apply any rule for deriving random numbers like XOR, mapping, discarding etc.

[3] Random value may be generated by way of concatenating columns most effective or rows most effective or rows and columns.

[4] Similarly precise values may be generated for Alice and Bob from the same picture for authentication.

[5] Here we are the usage of OTPK with the security of key the usage of proper random number generation.

V. SIMULATION RESULTS

In this section of paper discuss the outcomes of our proposed mechanism for system which are protected from both attacks i.e. online dictionary attack and offline dictionary attack. That security analysis done with the help of Net-Beans graphical user interface. On this platform shows the all the phase which have used in our system propose two factor password authentication based smart card system.As above depicted figure 2 and 3 shows that the server and client window.

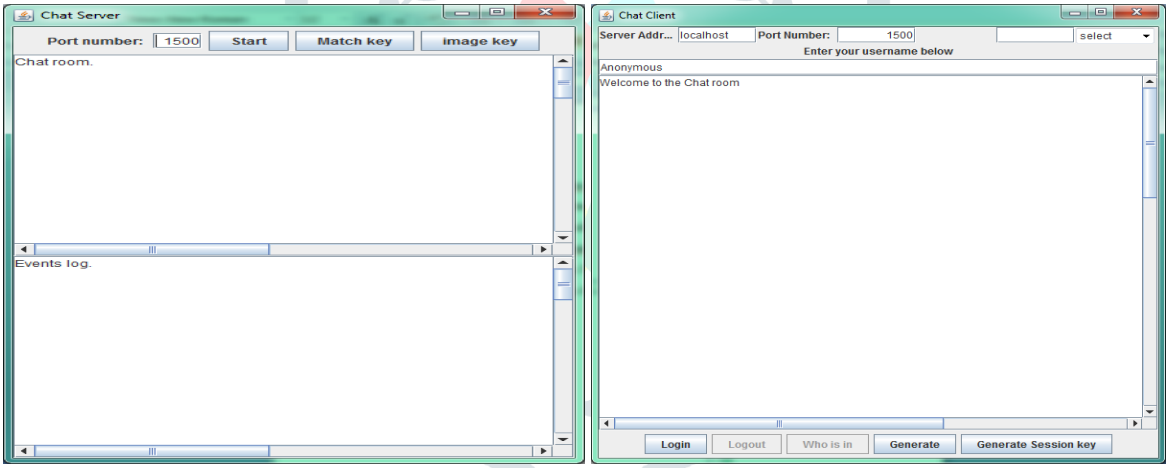
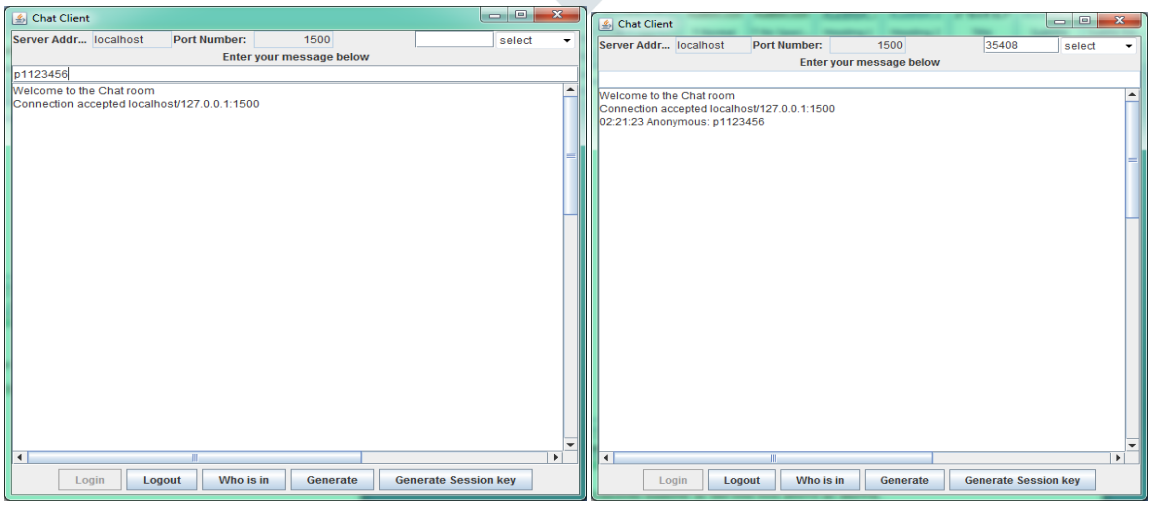


Figure 2: System GUI for server and Client window



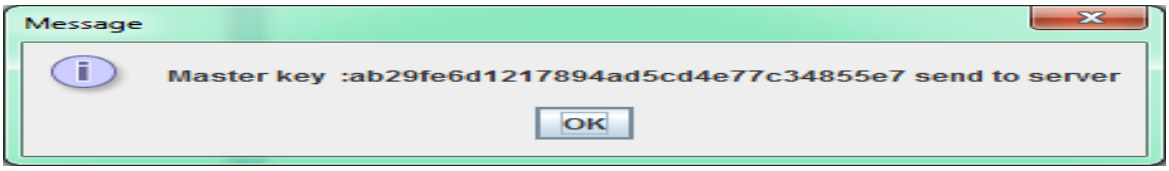


Figure 3: Server and Client window interaction

Table 1. Prevention from Various Attacks

Attack	(attack prevention)
Replay attack	No
Identity disclosure attack	No
Insider attack	Yes
Outsider attack	Yes
Eavesdropping	No
Identity Spoofing	Yes
Password based attack	Yes
Man-in the middle attack	No

Table 2:Computation with work

Computation Cost		Scheme
Smart Card	Registration Operation	-
	Session Run	2M+4H
	Password Operation	2H
Server	Registration Operation	2H+1E
	Session Run	2M+4H+1E
	Password Operation	-

Table 3: Storage judgment of the planned scheme

Storage/ scheme	Existing Work
Smart card	128 bits
Server	64 bits

In above table shows comparisons of storage judgment of planned scheme.Where, H denotes the cryptographic hash computation & M denotes the scalar multiplication computation over the elliptic curve & E denotes the symmetric encryption or decryption computation.In above table shows comparisons of Computation of planned scheme.It clearly shows that our scheme uses a less computation. Our scheme takes less time for computation and cost is low.

VI. CONCLUSION

In this paper introduce the beautify element primarily based authentication scheme wherein OTPK is only for One-time use, certificates is short-lived and Each time a signature is wanted; the key is generated, certified, used to signal the transaction, after which deleted. Key constantly remains in client possession all through the quick lifetime, and by no means saved on an authentication to the CA/RA. Security assaults prevention and low Storage value and everlasting foundation. Main security lies inside the on line certification process where the person would use robust (2-factor).

REFERENCES

[1] ZHANG Gefei, FAN Dan, ZHANG Yuqing and LI Xiaowei, “A Provably Secure General Construction for Key Exchange Protocols Using Smart Card and Password”, Chinese Journal of Electronics 2017.

[2] Qi Xie, Duncan S. Wong, Guilin Wang, Xiao Tan, Kefei Chen, Liming Fang," Provably Secure Dynamic ID-based Anonymous Two-factor Authenticated Key Exchange Protocol with Extended Security Model", IEEE Transaction 2016.

[3] Hung-Min Sun, Shiuan-Tung Chen, Jyh-Haw Yeh and Chia-Yun Cheng, "A Shoulder Surfing Resistant Graphical Authentication System", IEEE Transaction 2016.

[4] R. Madhusudhan and ManjunathHegde, "Cryptanalysis and Improvement of Remote User Authentication Scheme Using Smart Card", IEEE 2016.

[5] Zheng xianGao, ShouHsuan Stephen Huang, Wei Ding, "Cryptanalysis of Three Dynamic ID-Based Remote User Authentication Schemes Using Smart Cards", Proceeding of ICOACS IEEE 2016.

[6] Xinyi Huang, Xiaofeng Chen, Jin Li, Yang Xiang, and Li Xu, "Further Observations on Smart-Card-Based Password-Authenticated Key Agreement in Distributed Systems", IEEE Transaction 2016.

[7] XioyiDuan and BaoliNiu, "A Change Password Attack Resistant Scheme for Remote User Authentication using Smart Card", Proceeding of ICOACS IEEE 2016.

[8] Hsieh-Tsen Pan and Shyh-Chang Tsaur, "Cryptanalysis of Efficient Dynamic ID Based Remote User Authentication Scheme in Multi-server Environment using Smart Card", 12th International Conference on Computation Intelligence and Security IEEE 2016.