International Journal of Research in Engineering and Science (IJRES)
ISSN (Online): 2320-9364, ISSN (Print): 2320-9356
www.ijres.org Volume 09 Issue 10 ǁ 2021 ǁ PP. 51-58

Two-Factor Authentication With Security Beyond Conventional Bound

P.R. Jebisha,
Project Assistant,Hi-Fy Technologies
Nagercoil, India

Dr.M.R.Geetha
Professor, Department of Electronics and Communication Engineering
Ponjesly College of Engineering Nagercoil, India

Abstract— *As the most prevailing two-factor authentication mechanism, smart-card-based password authentication has been a subject of intensive research in the past two decades. In most of these studies, there is no comprehensive and systematical metric available for schemes to be assessed objectively, and then present new schemes with assertions of the superior aspects over previous ones, while overlooking dimensions on which their schemes fare poorly. Unsurprisingly, most of them are far from satisfactory – either is found short of important security goals or lack of critical properties, especially being stuck with the security-usability tension. To overcome this issue, this paper first explicitly define a security model that can accurately capture the practical capabilities of an adversary and then suggest a broad set of twelve properties framed as a systematic methodology for comparative evaluation, allowing schemes to be rated across a common spectrum. A new scheme is advanced to resolve the various issues arising from user corruption and server compromise, and it is formally proved secure under the harshest adversary model so far. In particular, by integrating "honey-words", traditionally the purview of system security, with a "fuzzy-verifier", the proposed scheme hits "two birds": it not only eliminates the long-standing security-usability conflict that is considered intractable in the literature, but also achieves security guarantees beyond the conventional optimal security bound.*

Keywords— *Two factor authentication; Smart card; Honey-words; Fuzzy-verifier; Twelve criteria.*

Date of Submission: 17-10-2021 Date of acceptance: 01-11-2021

I. INTRODUCTION

An authentication factor is an independent category of credential used to verify user identity. In multilevel authentication, each additional level increases the assurance that an entity requesting access to some system is who, or what, they are declared to be and decreases the likelihood that an intruder can masquerade as them to gain access. The three most common categories of authentication factors are often described as something user know, something user have and something user are. The ID and password combination is still the most common form of SFA. More complex systems include Two-Factor Authentication (2FA) with three, four and even five level of authentication. Location factors - where the user is at the time of login, is one of the level argued for authentication. Again the ubiquity of Smartphone's can help ease authentication burdens here. Most Smartphone's have a GPS device enabling reasonable surety confirmation of the log in location. In two factor authentication the main example is online transaction: User can't physically use their ATM card in North America and then again in China within a few hours. This additional factor could be used to confirm ATM transactions and prevent many cases of online bank fraud.

Password authentication with smart card is one of the most convenient and effective two factor authentication mechanisms for remote systems to assure one communicating party of the legitimacy of the corresponding party by acquisition of corroborative evidence. This technique has been widely deployed for various kinds of authentication applications, such as remote host login, online banking, e-commerce and e-health. In addition, it also constitutes the basis of three level authentications. However, there still exists challenges in both security and performance aspects due to the stringent security requirements and resource-strained characteristics of the clients. Among the numerous methods for user access control, password-based authentication is the most widely used and acceptable mechanism because of its easy operation, scalability, compatibility and low-cost advantages. In such authentication schemes, each user is assumed to only hold a memorable, low-entropy password, while the server needs to store a password-related verifier table necessary to

verify the authenticity of users. An inherent limitation of this password-only mechanism is that, the server has to store a sensitive verifier table that contains the passwords of all the registered users.

Two-Factor Authentication (2FA), sometimes referred to as two-step verification or dual factor authentication, is a security process in which the user provides two different authentication factors to verify themselves to better protect both the user's credentials and the resources the user can access. Two-factor authentication adds an additional layer of security to the authentication process by making it harder for attackers to gain access to a person's devices or online accounts, because knowing the victim's password alone is not enough to pass the authentication check.

Considering the twelve criteria-related studies which is used to deceive the attack. First take a substantial step towards the underlying adversary model by eliminating the deficiencies. Explicitly characterize the practical capabilities of an adversary, and suggest a broad set of 12 independent criteria framed as a systematic methodology for comparative evaluation. It addresses the long-standing security-usability conflict and achieves security beyond the conventional optimal security bound.

Broad lists of 12 independent criteria which satisfy two-factor schemes:

C1. No password verifier-table: the server does not need to maintain a database for storing user passwords or some derived values of user passwords.

C2. Password friendly: the password is memorable, and can be chosen freely and changed locally by the user.

C3. No password exposure: the password cannot be derived by the privileged administrator of the server.

C4. No smart card loss attack: the scheme is free from smart card loss attack, i.e., unauthorized users getting a victim's card should not be able to easily change the password of the smart card.

C5. Resistance to known attacks: the scheme resists various kinds of basic/sophisticated attacks, including offline password guessing attack, replay attack, parallel session attack, de-synchronization attack, stolen verifier attack, impersonation attack, key control, unknown key share attack and known key attack.

C6. Sound repairability: the scheme provides smart card revocation with good repairability, i.e., a user can revoke her card without changing her identity.

C7. Provision of key agreement: the client and the server can establish a common session key for secure data communications during the authentication process.

C8. No clock synchronization: the scheme is not prone to the problems of clock synchronization and time delay, i.e., the server needs not to synchronize its time clock with these time clocks of all input devices used by smart cards, and vice versa.

C9. Timely typo detection: the user will be timely notified if she inputs a wrong password by mistake when login.

C10. Mutual authentication: the user and server can verify the authenticity of each other.

C11. User anonymity: the scheme can protect user identity and prevent user activities from being traced.

C12. Forward secrecy: the scheme provides the property of perfect forward secrecy.

The rest of this paper is structured as follows: section II describes the related works and the existing systems. Section III describes the proposed system and discusses its different components in detail. Result and Performance evaluation are provided in section IV and conclusion is drawn in section V.

II. RELATED WORK

This section deals with analyzing the existing system. It is the process of gathering information and diagnosing the problems in the existing system, then suggesting an idea for the improvement of the existing system.

In [5] V. Odelu, A. Das, (2015) uses biometrics-based smart card and Elliptic Curve Cryptography (ECC). This scheme is secure against passive and active attacks but it is very suitable for battery-limited mobile devices as compared. In [13] Q. Jiang, J. Ma, investigate the hypothesis that adding visible security features to a system increases user confidence in the security of a system. In [14] Zuowen Tan1,2, enables communication parties to authenticate the parties and agree on the session key over an insecure public network. In this work, it improves the three-party encrypted key exchange protocol by bilinear maps. The proposed three party authentication key exchange protocol is provable secure under Computational Diffie-Hellman assumptions in the standard model. In [2] Atiya Zahed, design biometric-based authentication systems that use physiological and/or behavioral traits are good alternatives to traditional methods. These systems are more reliable and more user-friendly. In [7] J. W. Byun, suggest a new privacy preserving Smart-Card based Password Authenticated Key Exchange (SC-PAKE) with provable security. Only the user who has two secrets (smart-card and password) can go through authentication with key exchange while concealing its identifier from outsider adversaries. In [3] Y. G. Wang, proposed a password based authenticated key exchange. These protocols are used for the protection of password based authentication between a client and a remote server. In [15] Wei Gao, introduce remote user authentication has been used to identify a user remotely. The proposed generic framework enhances the security of existing single-factor authentication schemes by upgrading them to next authentication schemes, without

exposing user privacy. In [6] Juels and R. L. Rivest, implement a smart card based password authentication which improving the security of hashed passwords.

III. PROPOSED SYSTEM

This section describes the problem statement and the proposed system. Also the different components in the proposed system are discussed here.

Problem statement

The most essential security goal of smart-card based password authentication schemes is to achieve "truly two factor security", which means that only the user who is in possession of both a smart card and the corresponding password can login the service server. However, no proper security justification (let alone an explicit security model) has been presented, in the existing systems. So these protocols previously claimed to be secure turn out to be vulnerable. Hence it is required to develop a better two-factor authentication scheme which can eliminate the deficiencies.

Proposed framework

A simple, robust yet efficient smart-card based password authentication scheme has been proposed in this paper.

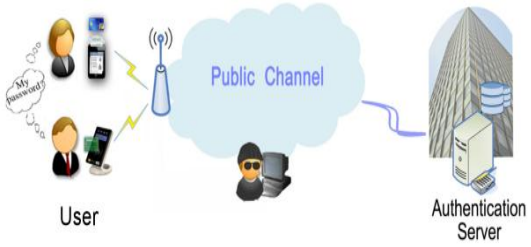

Fig 1: Block Diagram

A systematic framework has been suggested for evaluating two-factor authentication schemes. It is composed of a practical adversary model as well as a well-refined criteria set. The integration of "honey-words" with a "fuzzy-verifier" has been done only eliminate the long-standing security-usability tension as well as to achieve security beyond the conventional optimal bound. The participants of this sort of authentication (Fig.1) mainly involve a client and an authentication server. First, client registers submitting herself chosen credentials (e.g., her identity and password) to server, and then server securely issues client a smart-card with some security parameters. This is the user registration phase. Later on, user and server authenticate themselves to each other through the login phase. Besides, user may regularly change her password via the password change phase.

Basically, a simple but clever idea behind the study is the insertion of false passwords called as honey-words associated with each user's account. When an adversary gets the password list, he recovers many password candidates for each account and he cannot be sure about which word is genuine. Hence, the cracked password files can be detected by the system administrator if a login attempt is done with a honey-word by the adversary.

step 1: User ui enters a password g to login to the system. Server first checks whether or not H(g) is in list Vi.
step 2: If not, then login is denied.
step 3: Otherwise system checks to verify if it is a honey-word or the correct password.
step 4: Let v (i, j) = H(g). Then j value is delivered to
step 5: The honey-checker in an authenticated secure communication.
step 6: The honey-checker checks whether j = ci or not.
step 7: If the equality holds, it returns a TRUE value, otherwise it responses FALSE and may raise an alarm depending on security policy of the system

1. Registration phase

In registration phase, the authentication was mainly involved a client and an authentication server. This is the module for smartcard generation. The user gives username, password and public key to the server for getting approval. Then server checks the user details and stores all the necessary details to the smartcard and issue the smartcard to the user. Private Key is a unique and randomly generated password known only to the customer, which can be changed to his/her convenience. This is a means of authentication required to be provided by the customer for putting through the transaction in his/her/their/its accounts with Bank through Internet Banking.

2. *Login phase*

Login Password is a unique and randomly generated password known only to the customer, which can be changed by the user to his/her convenience. When a user wishes to login into the server S for obtaining some services, he/she first attaches his/her smart card to a device reader, and inputs IDi and PWi . The smart card first computes and then selects a random number. On receiving the authentication request message, S checks if IDi is

valid. If either or both are invalid, the request is rejected. After receiving the message, the smart card checks IDi and compares the time that the message is received.

3. Verification phase

To provide the admired property of "local and secure password", the "fuzzy Verifier" is more effective in dividing adversary password guessing space. In this phase user allowed to perform the transaction by giving the correct session key and private key. Session key is valid for a particular time period. Private Key is issued along with the smart card, and it cannot be modified in the future. If private key was invalid then the account will be blocked. The online guessing can be effectively thwarted by locking the account after several failed in login attempts or by only allowing a probabilistic number of failed guesses.

4. Password change phase

Password change phase is used for security purpose. It is used to protect user account by changing the current password to new password. For the sake of security, user friendliness and communication efficiency satisfy the second criterion. In this phase the user is allowed to change their account password for their convenience. To change the password user first submit the smartcard and after verification they are allowed to change the password by submitting old password and new password.

IV. RESULT AND PERFORMANCE EVALUATION

In this section it shows the result and performance evaluation of two factor authentication with security beyond conventional bound integrating the honey-words and fuzzy verifier.

a) Registration details

The participants of this sort of authentication mainly involve a client and an authentication server. In Registration form the user registers his/her username, password, address and public key to the server as in Fig 2 Server checks all the details and issues the smartcard to user

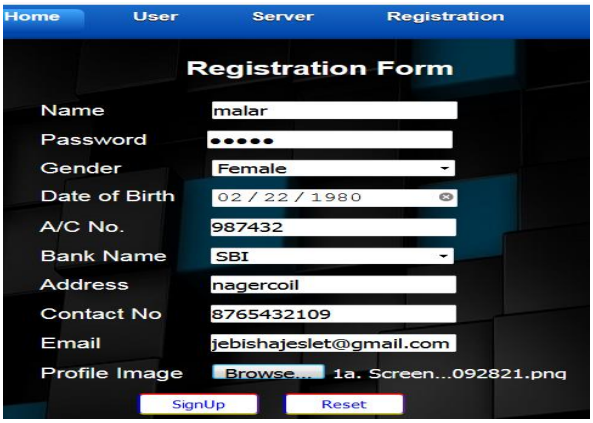

Fig. 2: Registration details

b) Honey-words Generation

Honey words will be generated after completing the registration phase is shown in Fig 3. Honey-words create bogus passwords which are placed in the password file of an authentication server to deceive attackers.

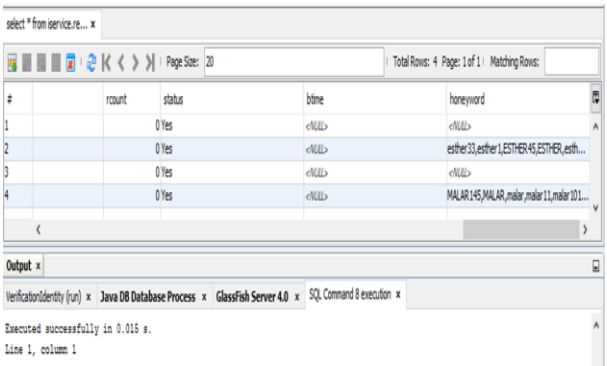

Fig. 3: Honey-words Generation

c) Smart card Insertion:

After completing the registration process the user will receive one smart card through internet which can be inserted in the smart card reader is shown in Fig 4.

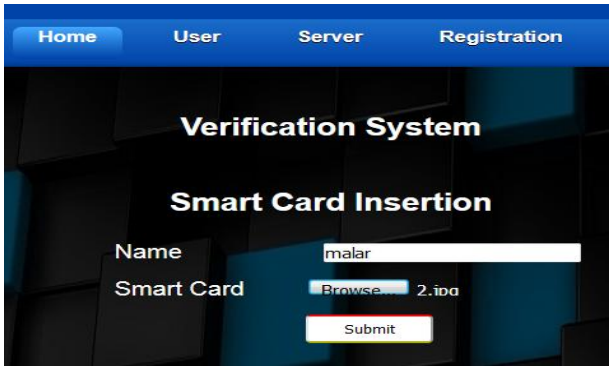

Fig 4: Smart card Insertion

d) User Login:

In login page, user gives the username and password to the server for authentication. If the details are correct then server allows accessing otherwise reject the login request which is shown in Fig 5.

Fig 5: User login

e) Verification System

Verification system performs a set of actions used to check the correctness of the elements such as name, transaction password (private key) and session key in Fig 6. Private key and session key is issued by the server to the user for verification purpose.

Fig 6: Verification system

f) Money transaction between two accounts

Inter money transaction enables the transfer of funds from the account of the remitter in one bank to the account of the beneficiary maintained with any other bank which is shown in Fig 7.

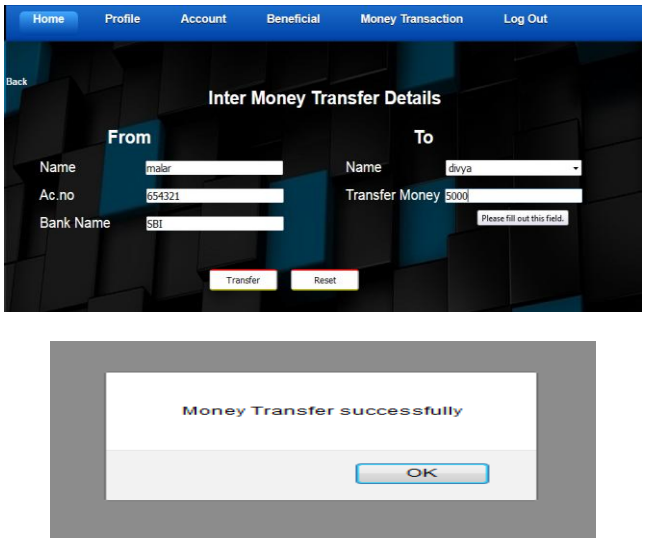

Fig 7: Final output

g) Performance of Authentication Scheme

2FA compares the performance and the fulfillment of the criteria among relevant schemes like local password change, session key agreement and user anonymity with the proposed scheme. The comparison results are depicted in Table I and Table II.

TABLE I. AUTHENTICATION SCHEMES

Existing Scheme (References)	Communication Cost		Storage Cost
	User side	*Server side*	
1	1408 bits	1408 bits	3200 bits
3	1408 bits	1152 bits	3456 bits
4	2304 bits	1152 bits	3456 bits
6	1408 bits	1408 bits	4096 bits
7	2176 bits	1152 bits	2176 bits
13	2304 bits	1152 bits	3328 bits
12	640 bits	1152 bits	384 bits
16	1408 bits	1408 bits	2176 bits
Proposed Scheme	1536 bits	1152 bits	3616 bits

TABLE II. PROPOSED TWELVE EVALUATION CRITERIA

Existing Scheme (References)	The proposed twelve evaluation criteria											
	c 1	c 2	c 3	c 4	c 5	c 6	c 7	c 8	c 9	c 10	c 11	c 12
1	✓	×	×	×	×	×	✓	×	×	✓	×	✓
3	✓	✓	✓	×	✓	×	✓	✓	✓	✓	✓	✓
4	✓	✓	✓	×	✓	✓	✓	✓	✓	×	✓	✓
6	✓	✓	×	×	✓	×	✓	×	✓	✓	×	✓
7	×	×	✓	✓	✓	✓	✓	✓	×	✓	✓	✓
13	✓	✓	×	✓	✓	×	✓	×	✓	✓	×	×
12	✓	✓	×	×	✓	×	✓	✓	✓	✓	×	✓
16	✓	✓	✓	×	✓	✓	✓	✓	✓	✓	✓	✓

Existing Scheme (References)	The proposed twelve evaluation criteria											
	c 1	c 2	c 3	c 4	c 5	c 6	c 7	c 8	c 9	c 10	c 11	c 12
Proposed Scheme	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

h) Authentication Time

Time-based authentication is a special procedure to prove an individual's identity and authenticity on appearance simply by detecting with the presence at a scheduled time within a time interval. Authentication Time is the length of time required to perform during computational process.

The comparison between one factor Authentication and Two factor Authentication results are shown in Table III.

TABLE III. AUTHENTICATION TIME

Scheme	Authentication Time
One factor Authentication	6.8
Two factor Authentication	6.2

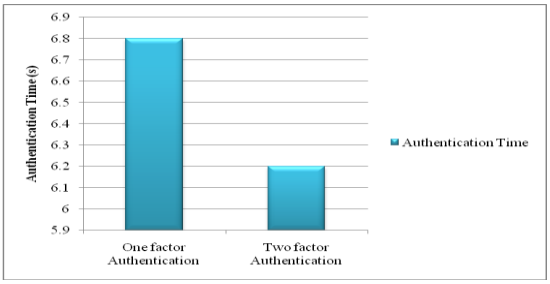

Fig 8: Authentication Time

The authentication Time for the existing system (One factor Authentication) is 6.8. While comparing with the proposed system (Two factor Authentication) the authentication time is 6.2 is shown in Fig 8.

i) Security level

Authentication allows an administrator to specify the security level of the authentication modules used in a particular authentication process. Each authentication module can be assigned a security level. The security level of Single Level Authentication is 62% and Multi Level Authentication is 90% is shown in Table IV.

TABLE IV. SECURITY LEVEL

Authentication Levels	Security (%)
Single Level Authentication	62%
Multi Level Authentication	90%

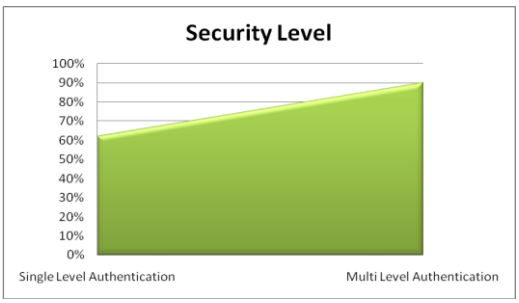

Fig 9: Security Level

Security level measures the strength of both Multi Level and single Level Authentication where Multi Level Authentication is more secure then single Level Authentication which is represented in Fig 9.

j) Comparison With Existing System

The Table V describes the comparison of one factor authentication and two factor authentications. In the one factor method the computation time is high while compared to two factor authentication. Security level is improved in the two factor authentication scheme. The attacker can't able to predict any of the user information because the user details are encrypted and stored into the smart card. Any user without smart-card can't access the server.

TABLE V. COMPARISONS OF SFA AND 2FA

Comparison Metrics	Existing System	Proposed System
Computation Time	High	Low
Authentication Time	High	Low
Successful Login Rate	Less	High
Security	Low	High

V. CONCLUSION AND FUTURE ENHANCEMENT

In this work the first step was taken towards breaking the "break-fix-break-fix cycle" in the two-factor authentication research area. Beyond the proposal of a new scheme which meets practicability, simplicity, and strong notions of security, the proposed adversary model and criteria set provide a benchmark for the evaluation of current and future two-factor authentication proposals. For the first time, it introduces "honey-words", traditionally the purview of system security, into two-factor cryptographic protocol design. By integrating "honey-words" with the proposed "fuzzy-verifier", this scheme can timely detect user card corruption to thwart online guessing and well addresses the seemingly intractable security-usability issue left in a practical scheme should also be able to withstand various passive and active attacks.

The proposed system depicts an application level entity authentication mechanism. But in near future two factor authentications would not be enough and three factor authentication is already on its way. IP tracing can also be included to catch the intruder after two unsuccessful attempts in the proceeding of any transaction.

REFERENCES

[1]. J. Xu,W. Zhu, and D. Feng, "An improved smart card based password authentication scheme with provable security", Comput. Stand. & Inter., vol. 31, no. 4, pp. 723–728, 2009.

[2]. International Journal of Computer and Electrical Engineering, Vol. 3, No. 4, August 2011"A novel technique for enhancing security in biometric based authentication systems", Atiya Zahed and Mohammad Reza Sakhi.

[3]. D. Wang, C. G. Ma, and P. Wu, "Secure password-based remote user authentication scheme with non-tamper resistant smart cards," in Proc. DBSec 2012, ser. LNCS. Springer, 2012, vol. 7371, pp. 114–121.

[4]. S. H. Wu, Y. F. Zhu, and Q. Pu, "Robust smart-cards-based user authentication scheme with user anonymity," Secur. Commun. Netw., vol. 5, no. 2, pp. 236–248, 2012.

[5]. V. Odelu, A. Das, and A. Goswami, "A secure biometrics-based multi server authentication protocol using smart cards", IEEE Trans. Inform. Foren. Secur., vol. 10, no. 9, pp. 1953–1966, 2015.

[6]. X. Li, J. Niu, M. K. Khan, and J. Liao, "An enhanced smart card based remote user password authentication scheme," J. Netw. Comput. Appl., vol. 36, no. 5, pp. 1365–1371, 2013.

[7]. J. W. Byun, "Privacy preserving smart-card based authentication system with provable security", Securi. Commun. Netw., vol. 8, no. 17, pp. 3028-3044, 2015.

[8]. Q. Yan, J. Han, Y. Li, and R. H. Deng, "On limitations of designing leakage-resilient password systems: Attacks, principles and usability", in Proc. NDSS 2012. The Internet Society, 2012, pp. 1-16.

[9]. Y. G. Wang, "Password protected smart card and memory stick authentication against off-line dictionary attacks", in Proc. SEC 2012.

[10]. Juels and R. L. Rivest, "Honey-words: Making password-cracking detectable", in Proc. ACM CCS 2013, pp. 145-160.

[11]. "Three level password authentication system", Swarna Lakshmi M1, Roobini S2, Shalie Monicka A3, Saraswathi V4, Ms. N. Radha5.

[12]. T.-T. Truong, M.-T. Tran, A.-D. Duong, and I. Echizen, "Chaotic chebyshev polynomials based remote user authentication scheme in client-server environment," in Proc. SEC 2015, pp. 479–494.

[13]. Q. Jiang, J. Ma, G. Li, and X. Li, "Improvement of robust smart-card based password authentication scheme", Int. J. Commun. Syst., vol. 28, no. 2, pp. 383–393, 2015.

[14]. "An improvement on a three-party authentication key exchange protocol using elliptic curve cryptography", Zuowen Tan1,2.

[15]. "An efficient generic framework for three level authentications with provably secure", Instantiation Jiangshan Yu_, Guilin Wang, Yi Mu, Senior Member, IEEE and Wei Gao.

[16]. S. Islam, "Design and analysis of an improved smartcard-based remote user password authentication scheme," Int. J. Commun. Syst., vol. 29, no. 11, pp. 1708–1719, 2016.