ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 3, Issue 2, pp: (1010-1015), Month: April - June 2015, Available at: www.researchpublish.com

A Novel Multi-factor Authenticated Key Exchange Scheme with Provably Secure Instantiation

[1]Gowthami M, [2]R.Ramesh

[1]Master of Engineering, [2]Head of Department,
[12]Department of Computer Science and Engineering, Veerammal Engineering College. Dindigul

Abstract: **In secure instantiation generic framework, password authentication is the most common authentication system. Passwords provide a convenient and inexpensive methodology. However, remembering multiple passwords and changing them frequently lead to the usage of lower entropy passwords which are susceptible to adversaries' guessing attacks. In this paper, a new multi-factor authenticated key exchange scheme, which combines with biometrics, image recogonization, password and the smart card, is proposed. Compared with the previous schemes, this scheme has higher security in remote authentication and preserves privacy of biometrics, and most of the previous schemes rely on the smart card to verify biometrics. The advantage of these approaches is that the user's biometrics is not shared with the remote server, which can resist insider's attack and preserve the privacy of the biometrics. The disadvantage is that the remote server must trust the smart card to perform authentication, which leads to various vulnerabilities. To achieve multifactor authentication, a new function called one-way function with distance-keeping, which is used to preserve privacy of user's biometrics, is introduced. This scheme has advantages as multi-factor authentication, privacy preserving and lower communication complexity etc. It is proven secure under the random oracle and is suitable to the environment which lacked communication resource and needed higher security.**

Keywords: **Authentication, security, privacy, password, smart card, image recogonization biometrics.**

I. INTRODUCTION

Authentication is the act of confirming the truth of an attribute of a single piece of data (datum) or entity. Authentication is the process of actually confirming that identity. It might involve confirming the identity of a person by validating their identity documents, verifying the validity of a Website with a digital certificate, tracing the age of an artifact by carbon dating, or ensuring that a product is what its packaging and labeling claim to be. In other words, authentication often involves verifying the validity of at least one form of identification. Authentication has relevance to multiple fields. In art, antiques, and anthropology, a common problem is verifying that a given artifact was produced by a certain person or was produced in a certain place or period of history. In computer science, verifying a person's identity is often required to secure access to confidential data or systems.

Need:

The single factor and two-factor authentication, which uses one of three factors or combines two of the three factors(what you know, what you have and who you are) have some drawbacks in security. The authentication scheme, which combines these multi factors, has become a new direction in authentication because these multi-factor authentication schemes can overcome some drawbacks compared with traditional one or two-factor authentication schemes.

Objective:

For thousands of years individuals have used passwords to authenticate their identity. The security system first implemented on computers 40 years ago was password. Authorities today agree that effective authentication of a person's

identity requires a combination of at least two of the three independent means of authentication, or factors. The factors are IP, Smartcard, Image recognition, Biometrics (iris) along with the steganography(concealing the message). Most early authentication mechanisms were purely based on passwords, which have much vulnerability. To strength the security, two factor authentication mechanisms were used. The two factors are password and smart-card; it could also fail if both the authentication factors are compromised. In this case the multi factor authentication mechanism was used to improve the security. The factors are password, smart-card, image matching and biometrics. But passwords have various attacks like password guessing attack and dictionary attack so in our scheme we are using IP instead of password. In order to provide more security we are using steganography along with biometric characteristics (iris) of the users.

Factors and Identity:

The ways in which someone may be authenticated fall into three categories, based on what are known as the factors of authentication: something the user knows, something the user has, and something the user is. Each authentication factor covers a range of elements used to authenticate or verify a person's identity prior to being granted access, approving a transaction request, signing a document or other work product, granting authority to others, and establishing a chain of authority.

Security research has determined that for a positive authentication, elements from at least two, and preferably all three, factors should be verified.[2] The three factors (classes) and some of elements of each factor are:

1) The knowledge factors: Something the user knows (e.g., a password, pass phrase, or personal identification number (PIN), challenge response (the user must answer a question, or pattern)

2) The ownership factors: Something the user has (e.g., wrist band, ID card, security token, cell phone with built-in hardware token, software token, or cell phone holding a software token)

3) The selection factors: Something the user to select during registration(e.g., image).

4) The inherence factors: Something the user is or does (e.g., fingerprint, retinal pattern, DNA sequence (there are assorted definitions of what is sufficient), signature, face, voice, unique bio-electric signals, or other biometric identifier).

Authorization:

A soldier checks a driver's identification card before allowing her to enter a military base. The process of authorization is distinct from that of authentication. Whereas authentication is the process of verifying that "you are who you say you are", authorization is the process of verifying that "you are permitted to do what you are trying to do". Authorization thus presupposes authentication.

For example, a client showing proper identification credentials to a bank teller is asking to be authenticated that he really is the one whose identification he is showing. A client whose authentication request is approved becomes authorized to access the accounts of that account holder, but no others.

However note that if a stranger tries to access someone else's account with his own identification credentials, the stranger's identification credentials will still be successfully authenticated because they are genuine and not counterfeit, however the stranger will not be successfully authorized to access the account, as the stranger's identification credentials had not been previously set to be eligible to access the account, even if valid (i.e. authentic).

Similarly when someone tries to log on a computer, they are usually first requested to identify themselves with a login name and support that with a password. Afterwards, this combination is checked against an existing login-password validity record to check if the combination is authentic. If so, the user becomes authenticated (i.e. the identification he supplied in step 1 is valid, or authentic). Finally, a set of pre-defined permissions and restrictions for that particular login name is assigned to this user, which completes the final step, authorization. Even though authorization cannot occur without authentication, the former term is sometimes used to mean the combination of both.

To distinguish "authentication" from the closely related "authorization", the shorthand notations **A1** (authentication), **A2** (authorization) as well as **AuthN** / **AuthZ** (**AuthR**) or **Au** / **Az** are used in some communities.[7]

Normally delegation was considered to be a part of authorization domain. Recently authentication is also used for various type of delegation tasks. Delegation in IT network is also a new but evolving field.[8]

ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 3, Issue 2, pp: (1010-1015), Month: April - June 2015, Available at: www.researchpublish.com

II. ARCHITECTURES

A. Existing Architecture:

In this system, Remote authentication has been widely studied and adapted in distributed systems. The security of remote authentication mechanisms mostly relies on one of or the combination of three factors: 1) something users know—password; 2) something users have—smart card; and 3) something users are—biometric characteristics. This paper introduces an efficient generic framework for three-factor authentication. The proposed generic framework enhances the security of existing two-factor authentication schemes by upgrading them to three factor authentication schemes, without exposing user privacy. In addition, we present a case study by upgrading a secure two factor authentication scheme to a secure three-factor authentication scheme. Furthermore, implementation analysis, formal proof, and privacy discussion are provided to show that the derived scheme is practical, secure, and privacy preserving. The communication complexity of this scheme is higher. Lacks a means of checking on biometrics in the server side

B. Proposed Architecture:

In this system, we formalize the definition of one-way function with distance-keeping, which is used to keep biometric privacy and matching the correct image parts, where individual image was provided during registration and a multi-factor authenticated key exchange scheme is proposed. Compared with the existing work, this scheme is more efficient in communication complexity. It consist of key distribution scheme, and the proposed scheme is a key exchange scheme. Rough speaking, in a key distribution scheme, a session key is picked by one party, and it is transferred to another party in a secure manner, but in a key exchange scheme, a session key is computed by two parties in a secure manner, the key exchange scheme has advantages in security. Computation complexity is less. It provides higher security in remote authentication. Highly secure under the standard model.

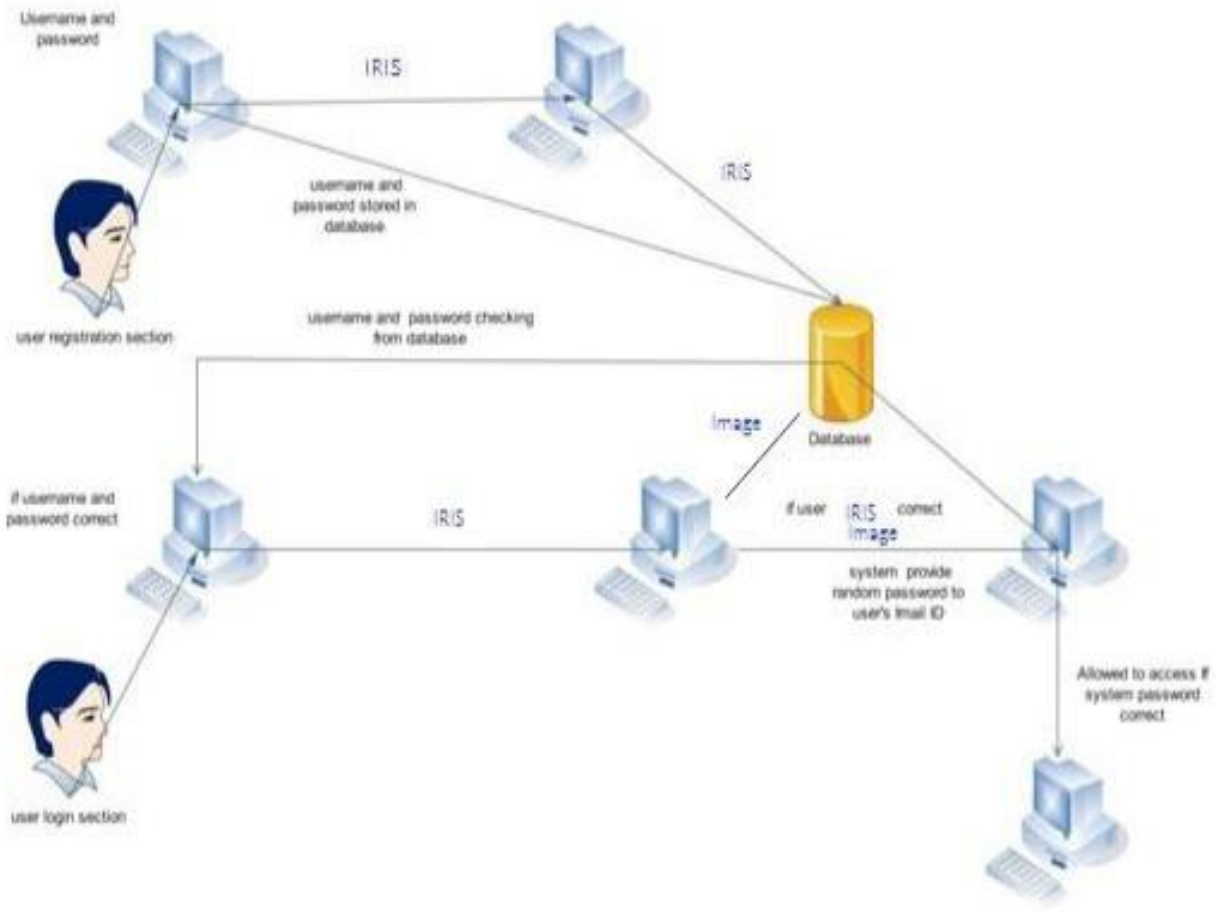

Fig.1. Proposed System Diagram

ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 3, Issue 2, pp: (1010-1015), Month: April - June 2015, Available at: www.researchpublish.com

Proposed Scheme:

In this stage, a user Ui chooses his identity IDi, password PWi and two hash functions h(:) and H(:). A fuzzy commitment scheme (Commit;Decommit) is created by the user, where Commit and Decommit are commitment and decommitment algorithm, respectively. The server S generates its symmetric encryption key x and asymmetric key pair (pk; sk), which are used in a public-key encryption scheme and a digital signature scheme. (Ex;Dx) represents symmetric encryption and decryption algorithm, (Epk;Dsk) represents asymmetric encryption and decryption algorithm, respectively, and Signsk(m) and Verify pk(m;δ) represent algorithm of signing and verifying, respectively. In our scheme, the symmetric encryption scheme and the asymmetric encryption scheme are secure against adaptively chosen ciphertext attack, and the digital signature scheme is secure against existential forgery under chosen message attack.

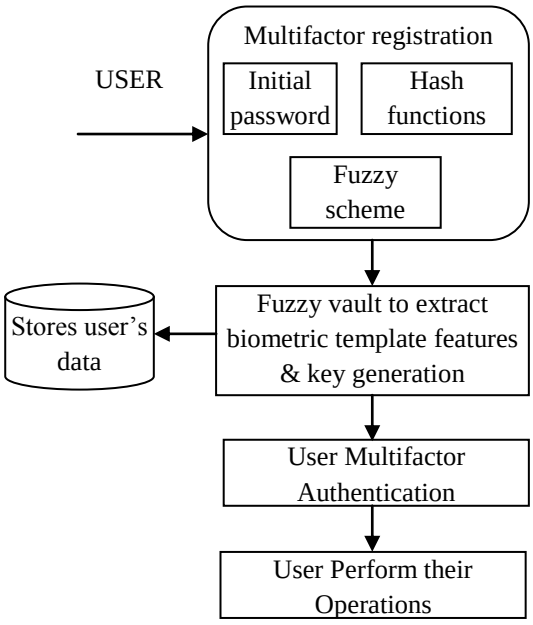

Fig.2. Proposed flow Diagram

III. METHODOLOGY

Fuzzy Vault:

Fuzzy vault is a cryptographic construction for data protection and user authentication, whose security relies on unexposed biometric characteristics and smart card. The error tolerance in fuzzy vault is achieved by using the Euclidean distance measurement which has been widely accepted by the majority of biometric applications. The operations of the fuzzy vault are described as follows. First, a user extracts biometric template *X* by scanning her biometric characteristics (e.g. fingerprint). Then, she encodes a pre-self-generated secret string *K* into a self-selected polynomial *Pol*, and evaluates the polynomial on all elements in *X*. She also needs to choose a large number of random points which do not lie on *Pol* as the noise. The final vault *V* is the collection of the points which lie on *Pol* and the noise points which do not lie on *Pol*. She can recover the secret string *K* from vault *V* by providing a biometric template *X_* such that the difference between *X* and *X_* satisfies $|X - X\_| < \_$, where $X - X\_ = \{x | x \in X, x /\in X\_\}$, and _ is an integer which is the fuzziness parameter. This is because that the polynomial *Pol* can be reconstructed if a sufficient number of points on *Pol* can be identified.

Protocol:

The basic idea of our concrete protocol is that using $PW = H\_(PW1||PW2)$ as the password in Yang *et al*'s scheme, where *PW*1 is the real password, and *PW*2 is the biometric key encrypted through fuzzy vault scheme. A user can pass authentication only if s/he provides the correct password, smart card, and the biometric features which is close enough with the one used in the registration phase. *1) Registration:* In the registration phase, a user *Ui* performs exactly the same as in Yang *et al.*'s scheme. However, after *Ui* receiving the smart card and the initial password *PW*0, she needs to additionally selects a new password *PW*1, a polynomial *Pol* and a biometric key *PW*2. In addition, she extracts her

biometric template *X*, encrypts *PW*2 through fuzzy vault device which outputs a vault *V*. Then *Ui* writes *V* into the smart card, and calculates $PW = H\_(PW1||PW2)$, and updates *B* by computing $B = Ci \oplus H\_(PW0) \oplus PW$. The 'fuzzy vault' procedures are reviewed in the Section II-A, thus we omit the detail here. *2) Login-and-Authentication Phase:* User $U\_ i$ attaches her smart card to a card reader device, inputs password $PW\_ 1$ and scans her biometric features. The fuzzy vault device extracts the biometric template $X\_$, then the fuzzy vault device calculates $Pol\_ = Dec(X\_, V)$, and $PW\_ 2 = Rec(Pol\_)$. The smart card *SC* calculates $C\_ i = B \oplus PW\_$, where $PW\_ = H\_(PW\_ 1 ||PW\_ 2)$. Then, the protocol runs the login phase as the same as Yang *et al*'s scheme by using $PW\_$. *3) Password-Changing:* To change an old password *PW*1, *Ui* performs the following steps. 1) Chooses a new password $PW\_ 1$. 2) Calculates $PWnew = H\_ (PW\_ 1 ||PW2)$ and computes $Bnew = B \oplus PW \oplus PWnew$, where $PW = H\_(PW1||PW2)$. 3) Replace *B* with *Bnew* in the smart card. The biometric key *PW*2 and the biometric features can be changed in a similar way, in which case, the vault *V* in the smart card should also be updated.

Fuzzy Extractor:

Fuzzy extractors [8] convert biometric information into random strings that makes it doable to use cryptographical techniques for biometric security. They're accustomed encipher and attest users records, with biometric inputs as a key. Codeword is evaluated by polynomial and therefore the secret message is inserted because the coefficients of the polynomial. The polynomial is evaluated for various values of a collection of options of the biometric information. therefore Fuzzy commitment and Fuzzy Vault were per-cursor to Fuzzy extractors. Fuzzy extractor could be a biometric tool to attest a user victimisation its own biometric guide as a key [10]. As fuzzy extractors modify a way to generate robust keys from life science and alternative clangorous information, it applies cryptography paradigms to biometric information which means that (1) build very little assumptions concerning the biometric information (these information comes from form of unwanted soundurces and do not need individual to take advantage of that so it is best to assume the input is unpredictable) (2) Apply cryptographical application techniques to the input. (for that fuzzy extractor translates biometric details into secret code, uniformly random and dependably consistent random string).

Multi-Factor Authentication:

Multi-factor authentication is extremely kind of like smart-card primarily based positive identification authentication; with the distinction that it needs are biometric characteristics as an extra authentication issue. Then At the end of registration process a unique image is provided for every registered user, the image is divided into two parts, first part of the image is stored in the server and the other part is built-in inside the smart card. During card insertion, if the image gets matched, it will be an authenticated user. A multi-factor protocol involves a consumer C and a server S, and consists of five phases. A multi-factor authentication protocol may also face passive attackers and active attackers as outlined in SCPAP. A passive (an active) assaulter is often any classified into the subsequent three varieties. Attacker has the charge account credit and therefore the biometric characteristics of the consumer. It's not given the security code of that customer. Assailant has the secret code and therefore the biometric characteristics. It's not allowed to get the information within the charge account credit. Assailant has the open-end credit and therefore the secret code of the consumer. It's not given the biometric characteristics of that consumer. Notice that such associate assailant is unengaged to mount any attacks on the (unknown) life science, as well as life science faking and attacks on the data (related to the biometrics) hold on within the charge account credit. IRIS authentication Steps:

1. Scan EYE
2. Grayscale EYE
3. Median Filter
4. Pupil center detection
5. Canny Edge Detection.
6. Pupil/ iris Radius detection
7. IRIS Localization
8. IRIS unrolling (unwrapping).

Iris recognition is an automated method of biometric identification that uses mathematical pattern-recognition techniques on video images of one or both of the irises of an individual's eyes, whose complex random patterns are unique, stable, and can be seen from some distance.

IV. CONCLUSION AND FUTUTRE WORK

In this paper, a new multi-factor authenticated key exchange scheme, which combines with biometrics, password and smart card, is proposed. This scheme provides higher security in remote authentication and privacy preserving in biometrics. Compared with the previous schemes, our scheme has advantages such as multi-factor authentication, privacy preserving and lower communication complexity etc.

In the future, we will propose new multi-factor authenticated key exchange scheme which can be proven secure under the standard model. It is used to fully identify the practical threats on multi-factor authentication and develop concrete multi-factor authentication protocols with better performances.

REFERENCES

[1] Abhilasha Bhargav-Spantzel, Anna Squicciarini, and Elisa Bertino.(2006) "Privacy preserving multi-factor authentication with biometrics". In Proc. of the 2nd ACM workshop on Digital identity management (DIM'06), Alexandria, VA, USA, pages 63–72.

[2] Ari Juels and Martin Wattenberg. A fuzzy commitment scheme.(1999)," In Proc. of the 6th ACM conference on Computer and communications security" (CCS'99), Singapore, pages 28–36. ACM Press.

[3] Chun-Ta Li and Min-Shiang Hwang.(2010),"An efficient biometrics-based remote user authentication scheme using smart cards". J. Netw. Comput. Appl., 33(1):1–5.

[4] David Pointcheval and S´ebastien Zimmer.(2008),"Multi-factor authenticated key exchange". In Proc. of the 6th international conference on Applied cryptography and network security (ACNS'08), New York, USA, LNCS, volume 5037, pages 277–295. Springer-Verlag.

[5] Eun-Jun Yoon and Kee-Young Yoo.(2005)," A new efficient fingerprint-based remote user authentication scheme for multimedia systems". In Proc. of the 9th International Conference on Knowledge-Based Intelligent Information and Engineering Systems (KES'05), Melbourne, Australia, LNCS, volume 3683, pages 332–338. Springer-Verlag.

[6] Fan Chun-I and Lin Yi-Hui.(2009)." Provably secure remote truly three-factor authentication scheme with privacy protection on biometrics". Trans. Info. For. Sec., 4(4):933–945.

[7] Hyun-Sung Kim, Sung-Woon Lee, and Kee-Young Yoo.(2003)," ID-based password authentication scheme using smart cards and fingerprints". SIGOPS Oper. Syst. Rev., 37(4):32–41.

[8] JingXu,Wen-Tao Zhu, and Deng-Guo Feng.(2009) "An improved smart card based password authentication scheme with provable security". Computer Standards and Interfaces, 31(4):723–728.

[9] Julien Bringer, Herv´e Chabanne, and Bruno Kindarji.(2009)," Identification with encrypted biometric data made feasible". In Proc. of the International Conference on Communications 2009 (ICC'09), Dresden, Germany.

[10] Kwon Youngkwon Lee and Taekyoung.(2006)," An improved fingerprint-based remote user authentication scheme using smart cards". In Proc. of the 6th International Conference on Computational Science and Its Applications (ICCSA'06,), Glasgow, UK, LNCS, volume 3981, pages 915–922. Springer-Verlag.

[11] Lee J.K. and Ryu S.R.(2002)," Fingerprint-based remote user authentication scheme using smart cards". Electronics Letters, 38(12):554–555.

[12] Lin Chu-Hsing and Lai Yi-Yi.(2004). "A flexible biometrics remote user authentication scheme". Computer Standards Interfaces, 27(1):19–23.

[13] Mihir Bellare, David Pointcheval, and Phillip Rogaway, (2000), "Authenticated key exchange secure against dictionary attacks", In Proc. of the 19th International Conference on the Theory and Application of Cryptographic Techniques (EUROCRYPT'00), Bruges, Belgium, LNCS, volume 1087, pages 139–155. Springer-Verlag.

[14] Mihir Bellare and Phillip Rogaway.(1993), "Entity authentication and key distribution". In Proc. of the 13th Annual International Cryptology Conference (CRYPTO'93), Santa Barbara, California, USA, LNCS, volume 773, pages 232–249. Springer-Verlag,

[15] Yevgeniy Dodis.(2001)." Introduction to cryptography(commitment scheme)". G22.3033-003.