A Secure Multiserver Authentication Protocol for Smart Cards using Combined Logout Scheme and Biometrics

M.Sangeetha
Department of computer science
IFET college of engineering
Villupuram.

M.O.Ramkumar M.Tech
Assistant professor
IFET college of engineering
Villupuram,

Abstract: **Online transaction can be done by using biometrics-based smart card, but yet there is no proper authentication. We first analyze He-Wang's scheme and it is susceptible to discover session-specific temporary information attack and impersonation attack. In this proposed system, a three level of authentication scheme is used. Your finger print and your login id and OTP (One Time Password) are the three level of authentication. Rather than using cryptographic algorithm, a pixel matching algorithm is used. This biometrics is used in online money transaction in mobile recharge and amount transfer in bank side. The main advantage of this scheme is the logout scheme. Once we logout, one random number is send to your mail id. Unless a match of your first password and random number is found, we can find the new password for login.**

Keywords: Security, Authentication, Smart card, Revocation and re-registration, pixel matching.

I. Introduction

The accountable data transfer protocol between two entities is developed and analyze a novel within a malicious environment by building upon oblivious transfer, and signature primitives. My future work motivates further research on To provide the security of the online transaction. To provide bio metric values to secure the Online transaction and also provide OTP for online Transaction. In previos system of the project there is no proper authentication using while online transaction. Existing OTP (One time Password) has been used. One Random number send from bank server to user mobile or email. If user get the OTP and process the Online transaction. That OTP may be hacked from hacker. With the rapid development of the wireless communication networks and online applications, such as e-banking and transaction-oriented services[1], there is a growing demand to protect the user identification privacy. Nowadays more and more transactions for the mobile devices have been implemented on the Internet, because of the transportable property of devices, such as laptops, smart cards and smart phones [2]. two real-time scenarios for the smart card based authentication schemes in which the registered users may cancel and re-register with the same identity [3], [4], [5], [6]: (i) when unexpectedly the secret token of a permissible user is discovered and (ii) if the smart card of a authorized user is stolen or lost. Hence, the authentication schemes must support the user revocation and re-registration with the same identity. Only one Authentication scheme used in existing system and there is no any logout scheme used in existing system. In this paper, I am using three level of authentication scheme used. Your Finger Print and your login id and OTP these are three level of authentication. In existing some cryptography algorithm used. In proposed Pixel matching algorithm used. These bio-metrics are used in online money transaction in mobile Recharge and amount transfer in bank side. And logout scheme are implemented. Once your are logout, one random number sent to your mail id. You match the your first password and random number to find the new password for login.

II. Literature Survey

A. Biometric identification A. Jain, L. Hong, and S. Pankanti.

Biometric systems allow routine recognition of persons based on physical or behavioral features which belong to a certain person. Each biometric feature has its restrictions and no biometric system is perfect so unimodal biometric systems raise a variety of problems. To over satisfying few mentioned inconvenient and limitations and to increase the level of security the multimodal biometric systems are used.

B. The advantages of elliptic curve cryptography for wireless security K. Lauter.

Elliptic curve cryptography has changed from interesting theoretical alternative to cutting edge technology adopted by an increasing number of companies. There are two reasons for this development: one is that ECC, which is oldest, and has withstood a generation of attacks.

C. Differential power analysis P. Kocher, J. Jaffe, and B. Jun.

Cryptosystem designers frequently assume that secrets will be manipulated in closed, reliable computing environments. Unfortunately, actual computers and microchips leak information about the operations they process. This paper examines specific methods for analyzing power consumption measurements to find secret keys from tamper resistant devices. We also discuss approaches for building cryptosystems that can operate securely in existing hardware that leaks information.

D. On the security of public key protocols D. Dolev and A. C. Yao:

Recently, the use of public key encryption to provide secure network communication has received considerable attention. Such public key systems are usually effective against passive eavesdroppers, who merely tap the lines and try to decipher the message. It has been pointed out, however, that an improperly designed protocol could be vulnerable to an active saboteur, one who may impersonate another user or alter the message being transmitted. In this paper we formulate several models in which the security of protocols can be discussed precisely. Algorithms and characterizations that can be used to determine protocol security.

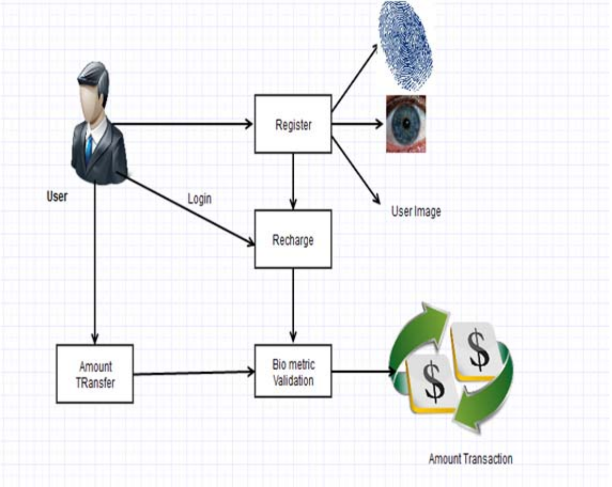
III. TECHNIQUES USED IN PIXEL METHOD:

The Hungarian algorithm is a tool to solve an assignment problem. For image matching, we can determine the best matching of pixels onto each other, where each pixel is matched exactly once. It is possible to directly use the Hungarian algorithm, but in many cases it is more appropriate to match the pixels onto each other such that each pixel is matched at least once or such that each pixel of the test image is matched exactly once. This last case corresponds to the most frequently used setting. We then require that the reference image explains all the pixels in the test image. We thus have three applications of the Hungarian algorithm for image matching: Each pixel matched exactly once. This case is trivial. Construct the weight matrix as discussed above and apply the Hungarian algorithm to obtain a minimum weight matching. Each pixel matched at least once. For this case, we need to solve the 'minimum weight edge cover' problem. A reduction to the exact match case can be done following an idea presented in [3].

Construct the weight matrix as discussed above 2. For each node find one of the incident edges with minimum weight 3. Subtract from each edge weight the minimum weight of both connected nodes as determined in the previous step 4. Make the edge weight matrix nonnegative (by subtracting the minimum weight) and apply the Hungarian algorithm 5. From the resulting matching, remove all edges with a nonzero weight (their nodes are covered better by using the minimum weight incident edges) 6. for each uncovered node add an edge with minimum weight to the cover Each pixel of the test image matched exactly once. This task is solved by the image distortion model, we only need to choose the best matching pixel for each pixel in the test image. Another method to obtain such a matching evolves from the previous algorithm if it is followed by the step: 7. for each pixel of the test image delete all edges in the cover except one with minimum weight.

IV. PROPOSED SYSTEM:

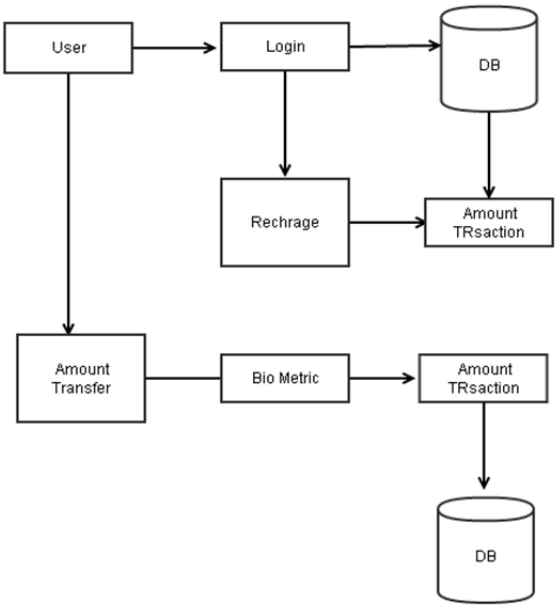
In Proposed system of this project, we are using three level of authentication scheme used. Your Finger Print and your login id and OTP these are three level of authentication .In existing some cryptography algorithm used. In proposed Pixel matching algorithm used. These bio-metrics are used in online money transaction in mobile Recharge and amount transfer in bank side. And logout scheme are implemented. Once your are logout, one random number sent to your mail id. You match the your first password and random number to find the new password for login



V. MODULE DESIGN

The proposed work is divided into the following steps:

- smart card registration
- authentication phase
- multiserver checking
- session key extraction
- re-registration process
- passeord changing process



A. Smart card Registration

User to register the own identity like user image and Iris image and finger print. That details to save to one package. If you login your account your have use to bio metric objects .It ensures that A cannot derive a user credentials, such as authentication parameter, user password and identity.

B. Authentication phase

If user login to account bio metric field will be activated. So on that time pixel mating algorithm will be activated. pixel matching algorithm will match the pixel of the image, if it correct access the login other wise account will go to login page. It ensures that an authentication scheme must provide the secure mutual authentication with the presence of the shared secret credentials.

C. Multiserver Checking:

In Multi-server authentication scheme using the Biometrics-based smart car

proposed a robust Biometrics-based authentication scheme for Multi server environment in order to withstand these security issues, and claimed that their scheme is secure against all possible known attacks.

D. Session Key Extraction

An authentication scheme should guarantee the security of the session key, called the session key. The leakage of a session key or session-specific temporary information will have no effects on the security of other sessions. such as the private keys of users or servers, which are used across the multiple sessions, will not necessarily compromise the secret information from all past sessions.

E. Re-Registration process

In Re-Registration process, registration center stores the user identity information to avoid many users to register with the same identity and thus, our scheme prevents the many logged-in users attack.

F. Password Changing process

In password changing proce1ss password will be change automatically when user logout. In password changing phase we are using session key changing algorithm. That algorithm will add the elements from session key and OTP key and updates to database.

VI. Mathematical Preliminaries

In this section, we briefly discuss the mathematical preliminaries to review and analyze He-Wang's scheme [7].

A. Elliptic curve over a prime field GF(p) A non-singular elliptic curve $y2 = x3 + ax + b$ over the finite field GF(p) is the set Ep of all the solutions (x,y)

$\in$ Zp×Zp to the congruence $y2 = x3+ax+b(\mathrm{mod}\ p)$, where $a,b \in$ Zp are constants such that $4a3 + 27b2$ 6= 0(modp), together with a special point O called the point at infinity or zero point, Zp $=\{0,1,...,p-1\}$ and $p > 3$ be a prime. The set of elliptic curve points, Ep forms an abelian group under addition modulo p operation [30]. Let G be a base point on Ep, whose order be n, that is, nG = G + G + ... + G (n times) = O. Assume that P = (xP,yP) and Q = (xQ,yQ) are two points on elliptic curve $y2 = x3 + ax + b(\mathrm{mod}p)$. Then R = (xR,yR) = P + Q is computed as follows [8]: $xR = (\delta 2 - xP - xQ)(\mathrm{mod}\ p)$, $yR = (\delta(xP - xR) - yP)(\mathrm{mod}\ p)$, where δ = (yQ−yP xQ−xP (mod p),ifP 6= Q 3xP 2+a 2yP (mod p),ifP = Q. In elliptic curve cryptography, the scalar multiplication is defined as the repeated additions. For example, if P $\in$ Ep, then 4P is computed as 4P = P + P + P + P. Definition 1 (Elliptic curve discrete logarithm problem (ECDLP)). Computing Q = kP is relatively easy for given k $\in$ Zp and P $\in$ Ep. However, given P $\in$ Ep and Q $\in$ Ep, it is computationally hard to compute the scalar k such that Q = kP. Definition 2 (Computational Diffie-Hellman problem (CDHP)). Given P,xP,yP $\in$ Ep, it is computationally hard to compute xyP $\in$ Ep without the knowledge of x $\in$ Z∗ p or y $\in$ Z∗ p, where Z∗ p = $\{a|0 < a < p, \gcd(a,p) = 1\} = \{1,2,3,...,p-1\}$. Definition 3 (Collision-resistant one-way hash function). A collision-resistant one-way hash function $H : X \to Y$, where $X = \{0,1\}*$ and $Y = \{0,1\}n$, is considered as a deterministic algorithm that takes an input as an arbitrary length binary string x $\in\{0,1\}*$, and outputs a binary string y $\in$ {0,1}n of fixed-length n [31], [32]. If AdvHASH A (t) is an adversary (attacker)A's advantage in finding collision, we then have AdvHASH A (t) = Pr[(x,x0)$\Leftarrow$R A: x 6= x0,H(x) = H(x0)], where Pr[E] denotes the probability of a random event E, and (x,x0)$\Leftarrow$R Adenotes the pair (x,x0) is selected randomly by A. In this case, the adversaryA is allowed to be probabilistic and the probability in the advantage is computed over the random choices made by the adversary A with the execution time t. A hash function H(·) is called collision-resistant, if AdvHASH A (t)≤ , for any sufficiently small > 0.

B. Biometrics and fuzzy extractor A metric space is a set Y with a distance function dis : $Y \times Y \to R+ = [0,\infty)$ [34]. An example of a metric space is the Hamming metric, Y = Γn, which is defined over some alphabet Γn (for example, Γ = {0,1}) and dis(ω,ω0) is the number of positions in which the strings ω and ω0 differ. The statistical distance is the distance between two probability distributions A and B defined by SD(A,B) =

1 2Pv |Pr[A = v] − Pr[B = v]|. Further, the min-entropy H∞(A) of a random variable A is −log(maxaPr[A = a]). A fuzzy extractor (Y,m,l,t,) extracts a nearly l-bit random string σ from its biometric characteristic input ω in an error-tolerant way [34], where m is the min-entropy of any distribution W on metric space Y and t the error tolerance threshold. If an input changes but it remains close to ω, then the extracted σ remains the same. To assist in recovering σ from the biometric characteristic input ω0, a fuzzy extractor outputs an auxiliary string θ. However, σ remains uniformly random for a given θ. The fuzzy extractor is given by the following two procedures, called the probabilistic generation procedure (Gen) and the deterministic reproduction procedure (Rep): • Gen is a probabilistic generation procedure, which on (biometric characteristic) input ω $\in$ Y, outputs an extracted string σ $\in$\{0,1\}l and auxiliary string θ. For any distribution W on metric space Y of min-entropy m, if hσ,θi ← Gen(ω), the statistical distance SD(hσ,θi, hUl,θi) ≤ , where Ul denotes the uniform distribution on l-bit binary strings and is the statistical distance between two given probability distributions hσ,θi and hUl,θi with l = m−2log(1)+ O(1) [9] [16]. • Rep is a deterministic reproduction procedure that allows to recover σ from the corresponding auxiliary string θ and any vector ω0 close to ω. For all ω,ω0 $\in$ Y satisfying dis(ω,ω0) ≤ t, if hσ,θi ← Gen(ω), then Rep(ω0,θ) = σ. The fuzzy extractor (Y,m,l,t,) is efficient, if Gen and Rep run in polynomial time in representation size of a point in Y. (Y,m,l,t,) is secure if it is difficult to recover σ from a

closed biometric input ω0 with the auxiliary string θ [10]. The uniqueness property of a biometric allows its applications in authentication protocols. As compared to the lowentropy passwords, the biometric keys have more advantages such as biometric keys cannot be lost or forgotten, biometric keys are hard to forge or distribute, biometric keys are difficult to copy or share, and as a result, guessing the biometric keys is a hard problem [11], [12]. As pointed out in [9], a strong fuzzy extractor (Y,m,l,t,) can extract at most l = m−2log(1)+O(1) nearly random bits. Thus, the probability to guess the biometric key data σ ∈{0,1}l by an attacker is approximately 1 2l, where l = m−2log(1)+O(1) [9].

VII. PERFORMANCE COMPARISON

In this section, we only compare the performance of our scheme with He-Wang's scheme[23], because we have pointed out the security pitfalls of He-Wang's scheme and then proposed a new scheme to withstand those security pitfalls found in their scheme. As in [7], we also assume that the length of the identity IDi, the output size of hash function H(·) (for example, SHA1 [13]), and an elliptic curve point P = (Px,Py) are 32 bits, 160bits, and320bits, respectively. In addition, we assume that the block size of symmetric encryption/decryption (for example, AES [14]) is 128 bits and a random number/nonce is 128 bits. The communication cost for the server registration phase for sending the identity SIDj and receiving the pair (kj,sj) is 32+(160+160) = 352 bits. To separately identify a server Sj at the RC, our scheme requires extra 160 bits for sj in the server registration phase. The communication cost for the user registration phase for sending the pair (IDi,H(pwi||σi)) and receiving the pair (zi,si) becomes (32+160) +(160+160) = 512 bits. Since the user Ui receives the smart card SCi before the registration, our scheme requires extra 320 bits to receive zi and si instead of receiving SCi as in He-Wang's scheme. During the login phase, and authentication and key agreement phase, our scheme requires (3×128) +320+160 = 864 bits, (3×128) +320+ 160+128 +160 = 1152 bits, 128+160 = 288 bits, 320+160 = 480 bits, and 160 bits for the messages M1 ={C1, X, h1}, M2 ={C1, X, h1, C2, h2}, M3 ={C3, h3}, M4 ={Y, h4}and M5 ={h5}, respectively.

TABLE I
COMPARISON OF COMMUNICATION COST

	Hevang	Ours
Server reg. phase	192 bits	352 bits
User reg. phase	192 bits	512 bits
Login & authentication phase	3520 bits	2944 bits

TABLE II
COMPARISON OF COMPUTATIONAL COST

	Hevang	Ours
User	3T(m)+7T(h)	3T(m)+7T(h)+1TΩ
Server	3T(m)+5T(h)	2T(m)+6T(h)+2TΩ
RC	3T(m)+9T(h)	1T(m)+11T(h)+3TΩ
Total cost	8T(m)+21T(h)	6t(m)+23T(h)+6TΩ
Total execution time	17.8563ms	10.4382ms

We have compared the computational costs of our scheme with He-Wang's scheme in Table IX. Let TH, TΩ and TM denote the time to execute a one-way hash function, a symmetric key encryption/decryption and an elliptic curve point multiplication, respectively. According to the results reported in [15], TH ≈0.0023ms, TΩ ≈0.0046ms and TM ≈2.226ms. From Table IX, we see that the computational costs required during the login phase, and authentication and key establishment phase of our scheme for the user Ui, server Sj and RC are 3TM+ 7TH+ 1TΩ, 2TM+ 6TH+ 2TΩ, and 1TM+ 11TH+ 3TΩ, respectively. The total computational cost is then 6TM+ 24TH+ 6TΩ. According to the execution time for different operations given in [15], the approximate time to execute our scheme is 13.4388ms, whereas He-Wang's scheme requires 17.8563ms.

V111. CONCLUSION

In multi-server authentication protocol for smart card using combined logout schme and biometrics. We have shown that our scheme is secure and provides more functionaries as compared to He-Wang's scheme. Using the pixel matching algorithm, we have proved that our scheme provides secure authentication through the formal security analysis. We have further simulated our scheme for the formal security verification using the widely-accepted AVISPA tool, and shown that our scheme is secure.In Future enhancement will use three level of bio metric with compatibly of Android mobile phones. And also will binary file authentication.

REFERENCE

[1] J. L. Tsai, N. W. Lo, and T. C. Wu, "Novel anonymous authentication scheme using smart cards," IEEE Transactions on Industrial Informatics, vol. 9, no. 4, pp. 2004–2013, 2013.

[2] S. Abolfazli, Z. Sanaei, E. Ahmed, A. Gani, and R. Buyya, "Cloudbased augmentation for mobile devices: Motivation, taxonomies, and open challenges," IEEE Communications Surveys & Tutorials, vol. 16, no. 1, 2014.

[3] E. Brickell and J. Li, "Enhanced privacy id: A direct anonymous attestation scheme with enhanced revocation capabilities," IEEE Transactions on Dependable and Secure Computing, vol. 9, no. 3, pp. 345–360, 2012.

[4] X. Huang, X. Chen, J. Li, Y. Xiang, and L. Xu, "Further observations on smart-card-based password-authenticated key agreement in distributed systems," IEEE Transactions on Parallel and Distributed Systems, vol. 25, no. 7, pp. 1767–1175, 2014.

[5] D. Wang, P. Wang, and D. He, "Anonymous two-factor authentication: Certain goals are beyond attainment," IEEE Transactions on Dependable and Secure Computing, 2014, DOI: 10.1109/TDSC.2014.2355850.

[6] D. He and D. Wang, "Robust biometrics-based authentication scheme for multiserver environment," IEEE Systems Journal, 2014, DOI:10.1109/JSYST.2014.2301517.

[7] W. Stallings, Cryptography and Network Security: Principles and Practices, 3rd ed. Prentice Hall, Cloth, 2003.

[8] Y. Dodis, L. Reyzin, and A. Smith, "Fuzzy extractors: How to generate strong keys from biometrics and other noisy data," in Advances in cryptology-Eurocrypt 2004. Interlaken, Switzerland: Springer, 2004, pp. 523–540.

[9] A. K. Das, "Analysis and improvement on an efficient biometric-based remote user authentication scheme using smart cards," IET Information Security, vol. 5, no. 3, pp. 145–151, 2011.

[10] Secure Hash Standard, FIPS PUB 180-1, National Institute of Standards and Technology (NIST), U.S. Department of Commerce, April 1995.

[11] Advanced Encryption Standard, FIPS PUB 197, National Institute of Standards and Technology (NIST), U.S. Department of Commerce, November 2001. http://csrc.nist.gov/publications/fips/fips197/fips197.pdf. Accessed on November 2010.

[12] AVISPA, "Automated Validation of Internet Security Protocols and Applications," http://www.avispa-project.org/. Accessed on January 2013.

[13] M. Burrows, M. Abadi, and R. Needham, "A logic of authentication," ACM Transactions on Computer Systems, vol. 8, no. 1, pp. 18–36, 1990.

[14] AVISPA, "Automated Validation of Internet Security Protocols and Applications," http://www.avispa-project.org/. Accessed on January 2013.

[15] C. Lv, M. Ma, H. L. amd J. Ma, and Y. Zhang, "An novel three-party authenticated key exchange protocol using one-time key," Journal of Network and Computer Applications, vol. 36, no. 1, pp. 498–503, 2011

[16] Suhasni,M.O.Ramkumar,Image Re-Ranking for websearch al,International Journal of Computer Science and Mobile Computing, Vol.4 Issue.3, March-2015