ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 4, Issue 3, March 2017

PROTECTING PASSWORD FROM HACKERS IN SMART CARD USING ECC

Shakeela Joy A,
Assistant Professor in Computer Science Department
Loyola Institute of Technology of Science
Dr. R. Ravi.,
Professor & Research Centre Head,
Department of Computer Science and Engineering
Francis Xavier Engineering College,
Tirunelveli - 627003, Tamil Nadu State, India.
fxhodcse@gmail.com

Abstract
Password endorsement in the smart card acting a significant task in unconfident networks. Security slanting protocols used for endorsement between consumer and far-off server include a strapping covert password. But the present security slanting protocols are very expensive. Also the users desire to use easily memorize password. So the hackers can easily estimate the password leading to password guessing attack. The two password guessing attacks are online attack and offline attack. In this paper we proposed IRE Scheme for iris recognition using ECC for encryption and decryption for security, discretion and user friendly.

Keywords: attacks, password, smart card, Elliptic Curve Cryptography, iris recognitions

1 INTRODUCTION

Smart cards play an important role in our routine life. The smart card can be a cell phone card, a card carrying our medical information, banking information or an electronic purse. The smart card can store information and execute commands.

Smart card is a chip card with Integrated Circuit. It is made up of polyvinyl chloride. In Smart card data can be stored and transacts. The data may be either value or information. It is transacted through a card reader.

Smart cards provide security while transaction. It provides tamper-proof storage and description identity. In recent years the password in the Smart card is stolen by the hackers either in online or offline computation. Therefore security slanting protocols are used for authentication.

Biometric skill contracts with identifying the uniqueness of characters constructed on their exclusive physical or interactive features. Physical features such as thumbprint, palm print and iris patterns or behavioral features such as entering pattern and hand-written signature present exclusivematerialaround a person and can be used in authentication applications.

The paper is structured as Section 2 discuss about the password guessing attack. Section 3 describes the existing system. Section 4 describes the proposed scheme based on ECC. Section 5 discusses the steps in iris recognitions. Section 6 discusses the comparison and Section 7 discusses the conclusion.

2 PASSWORD GUESSING ATTACK

Password means Personal Account Security System Word. It can be a word or characters, mainly used for user identity. But nowadays passwords are guessed and cracked by unauthorized persons.

The passwords can be guessed by two ways (i.e.) either in online or in offline.

Online password guessing attack

It is broadly extend on each user login and peer to peer system. Eg: brute force attack and dictionary attacks

Phishing: The unauthorized persons directly hack the password through emails.

Brute force attack: In this the unauthorized persons prefer a term with all probable grouping of numbers and alphabets.

Malware: In this the typed message or the screen shots taken during login process can be recorded.

Dictionary attacks: In this the hackers choose words the dictionary

Masquerade attack: The forged identity can be to access the system.

Forgery attack: It is attack adopting or imitating figures, objects or identification with the target device.

Denial of Service attack (DoS): In this the computer resources unavailable to its anticipated users.

Offline password guessing attack

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 4, Issue 3, March 2017

In this the unauthorized persons must not interact the prey host.
Eg: guessing, recording the conversation, evesdropping
Guessing: The unauthorized persons can guess the password by predictability.
Spidering: The hackers can collect the required data from website sales material.
Key stroke dynamics: The password is guessed from the dynamics records of key press and the key timings.
Man-in-the middle attack: The hackers make an independent channel between the user, the server , the prey and the relay messages in between them, making them to believe that they talking to each other directly.

3 EXISTING SYSTEM

In [1] SIP Scheme based on Elliptic Curve Cryptography provides security as classical cryptosystem for smaller keys, In [2] Elliptic Curve Cryptography Scheme is used. It provides password authentication, login client exact identity and mutual authentication. It requires low computation cost. The drawback is unprotected to masquerade attack and forgery attack. In [3] PGRP protocol can be used to prevent online or offline attack. In PGRP when a user login from a new machine, for the first time it will not answer ATT test. (ie protocol need less ATT test). Whenever the ATT test answered the user can login otherwise the user cannot login. In [5] Hough transform is used to found the pupil and iris borders. Usually the iris color is light with varying pigmentation and the pupil color is dark. In non ideal situation, the iris may be dark and pupil may illuminated. In [7] Error rates are increased by the noise during the iris image is captured. False identification is found when fixing the lens in iris portion. In [8] SVM (Support Vector Machine] based quality enhancement algorithm found a quality portion from various iris images to generate one iris image with high quality. In [13] Pinkas and Sander (PS) protocol reply the ATT test first before entering the $\{ID_A, PW_A\}$ pair. If the user fails to response the ATT properly the user cannot proceeds further. The PS is effective for online dictionary attacks. The drawback is the login server should generate an ATT test for each user login. In [17] find the margin of pupil and the iris by applying integrodifferential operator. Using polar transformation the segmented iris is transformed to a rectangular form. In [20] Elliptic Curve Cryptography scheme is used. It authorizes login clients and remote server with a secure and privacy preserving authentication. The drawback is unprotected to offline password guessing attack, stolen-verifier and insider attack.

4 PROPOSED SCHEME

The proposed scheme consists of four phases. They are
1) Registration phase
2) Login phase
3) Password change phase
4) Authentication phase
5) Iris recognitions

1) Registration Phase

In registration phase the user U_B chooses his/her identity ID_B and password PW_B. The steps in the registration phase are given below:
Step 1: Selects a random number 'm' in the range of (1-(n-1)), calculate h ($m \oplus PW_B$).
Step 2: Submit the request for registration to the server.
Step 3: After receiving the registration request from U_B the server $V_B=h(ID_B || h (m \oplus PW_B)$
Step 4: Smart Card $\rightarrow \{ V_B \}$
Step 5: Scan the iris of the user and store it in the server.

2) Login Phase

In this phase whenever the user U_B need to access the server, the user U_B inserts the smart card in to the card reader and entershis/her ID_B and PW_B. The steps in the login phase are given below:
Step 1: Calculate $V_{B'}=h (ID_B || h (m \oplus PW_B)$.
Step 2: Check $V_B$and $V_{B'}$ are identical or not. If it not identical, then reject the login request. Otherwise the user can login to the server.
Step 3: Scan the iris of the user and check for the identity.If identical, then the user can proceed otherwise the user cannot proceed further.

3) Password revise phase

This phase is active whenever the user U_B require to revise the/her password PW_B. The steps in the password revise phase are given below:
Step 1: The user U_B inserts the smart card in to the card reader and enters his/her ID_B and PW_B.
Step 2: Calculate $V_{B'}=h (ID_B || h (m \oplus PW_B)$.
Step 3: Check $V_B$and $V_{B'}$ are identical or not.

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 4, Issue 3, March 2017

Step 4: If it not identical, then reject the login request. Otherwise the user can login to the server and progress to the next step.
Step 5: User $U_B$enters the new password PW_{BNEW}.
Step 6: Smart Card calculate $V_{BNEW}=h(ID_B|| h (m\oplus PW_{BNEW})$.
Step 7: Smart Card replaces V_B with V_{BNEW}.

4) Authentication phase
Step 1: Check the format of ID_A. If the format is wrong, the system discards the login request.
Step 2: Check the validity of time interval between T and T'. If $(T'-T) \geq \Delta T$, the system discards the login request. (ΔT is the expected valid time interval)
$(T'-T) \geq \Delta T \rightarrow$discard the login request

5) Iris recognitions
The following are the steps in iris recognitions
Step 1: Capturing
Capturing the image of iris is very difficult and complicated due to the size and color of iris. It varies from person to person. The average capturing distance is 2 to 3 feet within 1 to 2 seconds.
Step 2: Segmentation
In the segmentation the parts like pupil diameter, eyelid, eyelashes and sclera part of the eye are eliminated. Due to this efficiency is increased.
Step 3: Normalization
In normalization the image of the iris is changed to the rectangular strips by using radial scan method.
Step 4: Enhancement
In enhancement the effectiveness and accuracy of the iris is improved, due to
image preprocessing technique.
Step 5: Extraction
The iris image is extracted and used for comparison.
Step 6: Comparison
The extracted iris image is compared with original iris image.
Step 6: Decision
If the comparison is identicalthe user can login to the server, otherwise reject the login request.

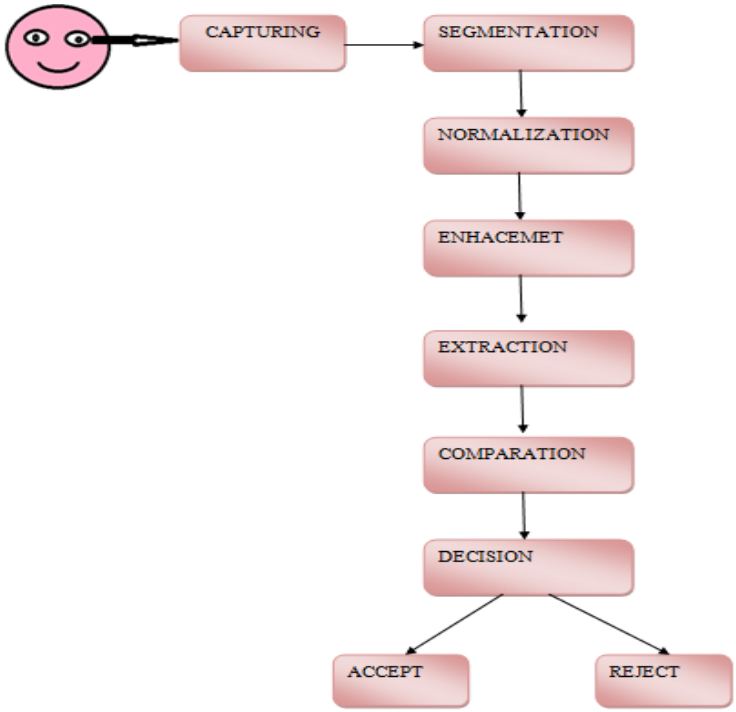

Figure: 1 Steps in iris recognitions

6 COMPARISION
The proposed IRE scheme is compared with existing algorithm.

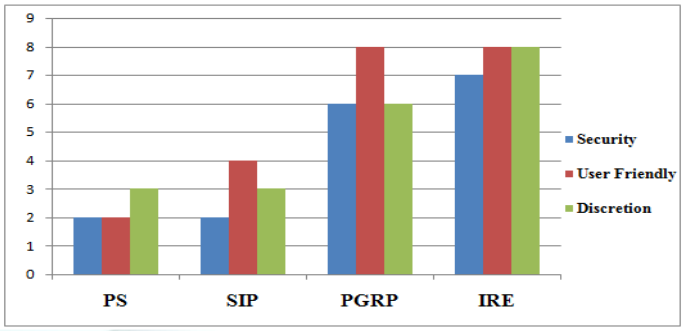

Figure: 2 Comparisons

7 CONCLUSIONS
Nowadays there are many protocols and techniques for password guessing attack, in online or offline In this paper we proposed IRE scheme iris recognition using ECC for encryption and decryption for security, discretion and user friendly .The proposed scheme consists of five phases. They are 1) Registration phase, 2) Login phase 3) Password change phase and 4) Authentication phase and 5) Iris recognitions
In the registration phase the user U_B chooses his/her identity ID_B and password PW_B using Elliptic Curve Cryptography and the iris of the user is scanned. In login phase whenever the user U_B need to access the

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 4, Issue 3, March 2017

server, the user U_B inserts the smart card in to the card reader and enters his/her ID_B and PW_B. The password revise phase is active whenever the user U_B require to revise the/her password PW_B. The authentication phase is used to verify the validity of smart card.

REFERENCES

[1]A.Durlanik, I. Sogukpinar . SIP authentication scheme using ECDH. World Enformatika Society Transaction on Engineering Computing and Technology 2005;

[2]A new password authentication and user anonymity scheme based on elliptic curve cryptography and smart card IET Information Security Chun-Ta Li Department of Information Management, Tainan University of Technology, 529Zhongzheng Road, Tainan City 71002

[3]Defence to curb online password guessing attacks, R. Kirushnaamoni PG Scholar, Dept. of Computer Science and Engineering,IEEE.

[4]C.C. Chang and T.C. Wu, "Remote password authentication with smart cards," *IEE Proceedings-E*, vol. 138, no. 3, pp. 165–168, 1993.[3] P. Wurzinger, L. Bilge, T. Holz, J. Goebel, C. Kruegel, and E. Kirda, "Automatically generating models for botnet detection", In 14th European Symposium on Research in Computer Security (ESORICS'09), 2009.

[5] L.Ma, T. Tan, Y,Wang, and D. Zhang, ""Efficient iris recogination by characterizing key local variation, "IEEE Trans. Image Process., vol. 13, no. 6. Pp. 739-750, June 2004.

[6]Li, C.T., Lee, C.C., Wang, L.J., Liu, C.J.: 'A secure billing service with two-factor user authentication in wireless sensor networks', Int. J. Innov. Comput., Inf. Control, 2011, 7, (8), pp. 4821–4831.

[7]Pradeep Kumar-Iris Recognition with Fake Identification. Computer Engineering and Inteligent Systems, ISSN 2222-1719 ,2011.

[8]R. Singh, M. Vatsa, and A.Noore, " Improving verification accuracy by synthesis of locally enhanced biometrics images and deformable model" Signal Process., vol 87, no. 11,pp.2746-2764, Nov 2007.

[9]B. Pinkas and T. Sander, "Securing Passwords against Dictionary Attack", Proc. ACM Conf. Computer and Comm. Security (CC' 02), 2002.

[10]K. Grabowski, W. Sankowski, M. Napieralska, M. Zubert and A. Napieralski, "Iris recognition algorithm optimized for Hardware implementation", IEEE, (2006).

[11]D.Florence, C Herley, and B Coskun, "Do Strong Web passwords Accomplish Anything?" Proc USENIX Workshop Hot Topics in Security(HotSec'07) 2007

[12]Song, R.: 'Advanced smart card based password authentication', Comput. Stand. Interfaces, 2010, 32, (5–6), pp. 321–325.

[13]J. Xu, W.T. Zhu, and D.G. Feng, "An improved smart card based password authentication scheme with provable security," *Computer Standards & Interfaces*, vol. 31, no. 4, pp. 723–728, 2009.

[14]J. Huang, Y. Wang, T. Tan and J. Cui, "A new iris segmentation method for recognition," in Proc. 17th Int. Conf. Pattern Recognition, vol. 3, (2004) August, pp. 554–557.

[15]K. Grabowski, W. Sankowski, M. Napieralska, M. Zubert and A. Napieralski, "Iris Recognition Algorithm Optimized for Hardware Implementation", IEEE, (2006).

[16]J.Daugman, "Probing the Uniqueness and Randomness of iris code", IEEE, (2006).

[17]J.G.Daugman, "High confidence viual recogination of persons by a test of statistical independence," IEEE trans. Pattern Anal.Mach.Intell., vol.15,no. 11,pp. 1148-1161, Nov. 1993.

[18] Li, C.T., Lee, C.C.: 'A novel user authentication and privacy preserving scheme with smart cards for wireless communications', Math. Comput.Model., 2012, 55, (1–2), pp. 35–44.

[19]Secure password based remote user authentication scheme against smart card security Breach Ding Wang, Chun-Guang-GuangMa,Qi-Ming Zhang,

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 4, Issue 3, March 2017

SendongZhao.Journal of networks, Vol 8, No 1,Jan 2013

[20]Islam, S.H., Biswas, G.P.: 'Design of improved password authentication and update scheme based on elliptic curve cryptography', Math. Comput.Model., 2012,