ENHANCEMENT OF SECURITY IN BANKING SECTOR USING SESSION SPANNING ALGORITHM

Shanmugapriya R [1], Supraja S [1], Varshini V S [1], Vishnu Priya S [1], Sasikumar R [2]

U.G. Students, Department of Computer Science and Engineering, K.Ramakrishan College of Engineering,
Kariyamanikam Road, Samayapuram, Trichy, Tamil Nadu, India [1]
Assistant Professor, Department of Computer Science and Engineering, K.Ramakrishan College of Engineering,
Kariyamanikam Road, Samayapuram, Trichy, Tamil Nadu, India [2]

Abstract

Smart card is the relevant way of retrieving amount from the bank . The lost card is the brink of disaster. Some people might be tempted to wait and hope the card turns up intact, the wiser course is to insist solution capable to manage ATM vulnerabilities in the absence of smart card . During the session of retrieving the replacement card the pull-out can be done through querying in the website. To achieve high level of security our proposed system proceeds with random key and session key protocols. In order to ensure secure withdrawal, from prediction and identification of increased vulnerabilities caused by both online and offline crisis, an algorithm of session spanning has been used. This provides compact security functionalities during online session. The issues of losing cards in the critical situation can be handled by this application ephemeral.

KEYWORDS: *PKRS, session key, random complaint number, password*

I. INTRODUCTION

Banking sector creates credits from the acceptance of user debits. Critical markets lend money either directly or indirectly. It provides financial stability between customers and the providers. The user's account balance is securely maintained by the bank database. Bank provides the credit and debit system through which deposit and withdrawal is made possible online. Today people prefer to secure their asserts through banks. Today banking achieve great reach, because of telecommunication and networking systems. This approach doesn't require customer's frequent visit to the bank. Banking allows automated processing of user's credentials, debits and credits. Today, most of the banks provide online services through internet. Moreover, online only banks are also available. Today, overseas transaction is a great demand and there exists several barrier to perform it. However, despite these barriers the banking sector has become globalized and has reached greater heights. Bank enables ATM facilities that allows people to perform financial transactions such as cash withdrawal, money deposits, fund transfer and provide customer's account details at any instance of time.

II. AN ATM SYSTEM MODEL

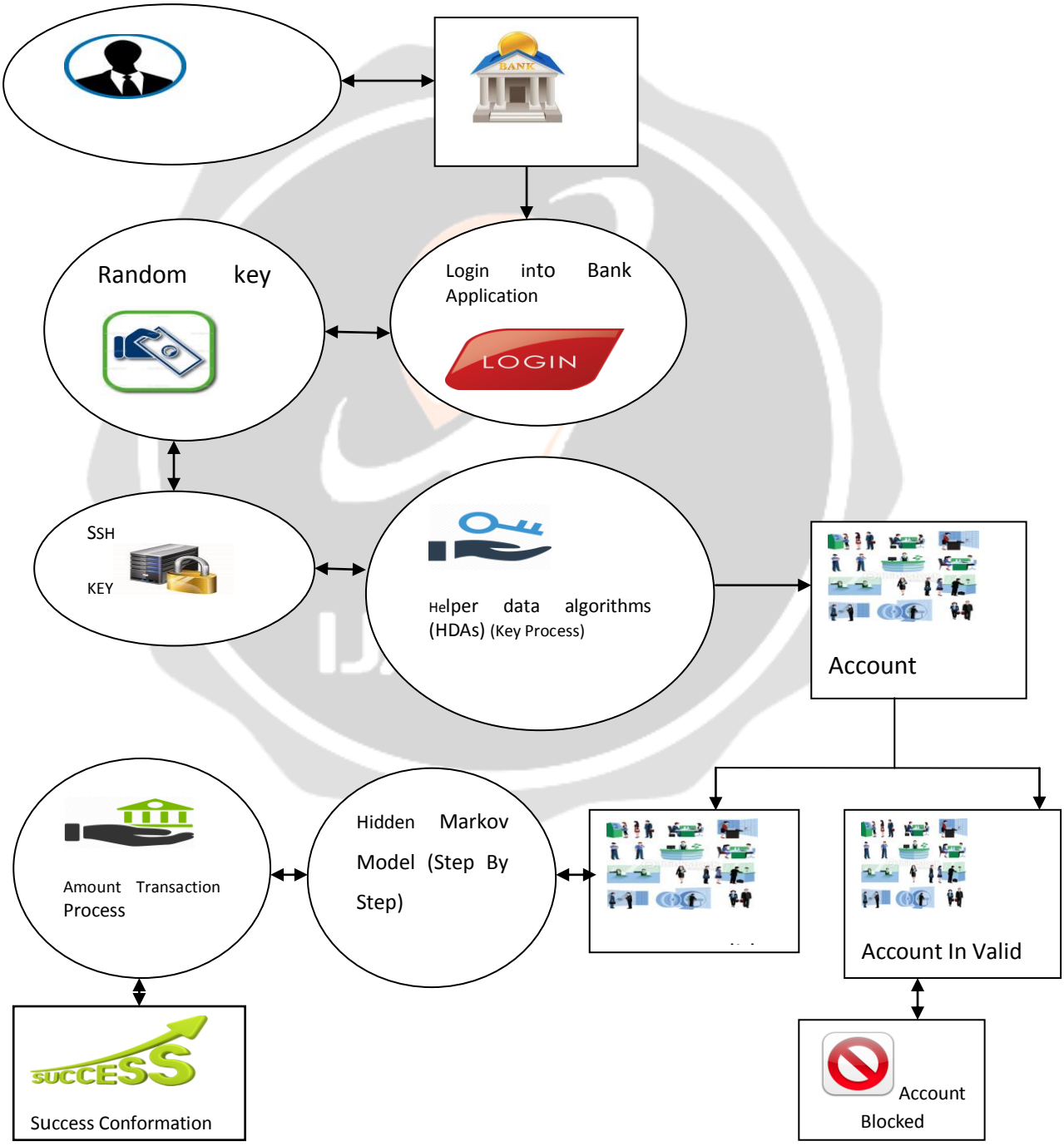
To perform transaction through banking we use ATM system model. The procedure is to insert the card in the card reader and use the pin for further processing. Information registered on the card's magnetic strip , that is stored in the database is verified and questions about the pin number. The pin number is verified for authentication. DES encryption method is used here. It has a 56-bit secret key to encrypt 64-bit block of input data . The DES encryption is preferred and the similarity is noted only for the output block rather than the pin verification. If the similarity is succeeded then the user could retrieve the cash. This ATM model ensures how an input is been given for DES encryption and the output is generated for cash withdrawal. DES algorithm is short-lived and so the process of retrieving the amount lasts for a predefined time. If the lifespan is shattered then reinsertion of card is mandatory.

III. SECURITY ISSUES

The ATM has a lot of security vulnerabilities though they use a high standards of security algorithms. Despite ATM being automated, it works over a computer which could be easily hacked. Tech-savy criminals can easily

hack ATMs. The software maintenance and updating is done through the track through which USB is connected. The system is prone to the third-party attack. The attacker can modify the existing program or can add some malicious details. This tactics allows the attacker to withdraw amount in the absence of plastic ATM card.

As there exists many insecurities in the security algorithms provided by the professionals, people tends to look for more securities in ATM. To secure data in ATM two-factor authentication is employed, which allows users to verify their personal credentials such as user id and password before performing transactions . To ensure further security in two-factor authentication several online services like social media and email services, enable security by not only verifying the PIN entered but also verifying the numeric code received as text message on the user's phone which is valid for only a short duration of time. This method is easily liable to attacks because it is so easy to falsely simulate cellphone numbers through the smart phone apps that generate new codes/physical keys for every few seconds.



ARCHITECTURE DIAGRAM

IV. CARD MISSING

Among these security issues if there is a chance of missing the card itself then it doubles the security that it actually consumes. As the world is very busy and competitive at present a card doesn't seeks the importance of individual personnel . The probability of missing card is high. The existing procedure like reporting, blocking,

request for temporary card will not suite for emergency situation. An immediate need of withdrawal cannot proceed through these approaches. Everyone wishes for an easy way that overcomes these misfortunes and finally results a secured cash withdrawal. The individual need not worry about hackers. Our proposed system illustrates a query session in every bank website. A Random key is generated to provide uniqueness in query session .A substitute of the card's pin number is the session key. Session spanning algorithm ensures secure session key generation, encryption and authentication. The generated session key and the key that is been used by the client is encrypted and matched. Random complaint number can be used till the replacement is been obtained.

V. SYSTEM MODULE

Three major protective methods are used

- Random key generation
- Session Spanning
- Symmetric key matching

Random key generation

The query page contains two ports one for new and other for existing person who has missed the card. Once a new user enters the session in accordance about missing card, it requires some identity of the user who has logged in. the identification is drawn out through account number, password, card holder name. To persue high level of security phone number and mail address is questioned. If all these essential information is submitted then a random key is generated. The key contains a four digit number which is stored in database. For every user there exists a random key. This key is used by the user to get the session key in order to access their account. The random key is sent to either to the mobile or to the mail. Once the user is logged in then he/she could use the same random key for further processes. Till the replacement is obtained random key is used. It is secured, as even any intruder identify the key they can't access the account due to the retrieval of session key which is next benchmark of security.

Session Spanning

Every time when we login using the random key a new session key is generated. The session key is any random text which is a combination of both alphabets and numbers such that no guesses for the session is applicable. The session is also popped through mobile or mail. This session key is used as pin number over the automated teller machine since the machine holds a separate path to retrieve cash. The session key is encrypted and stored in the database, hence it is not prone to any malicious attack. The span of a session key is short. A user is allowed to use this aliter it should not cause any troublesome. If the phone is lost then they could get it through mail and vice versa. The key lasts for about thirty minutes. The duration is extended so that it offends time to reach ATM.

Symmetric key matching

The session key is used to access the account in place of pin number. The text entered by the user, instead of pin number is encrypted. It is stored in the database where the details of user account along with encrypted session key. The encrypted text is matched with the session key that is stored in the database .If the encrypted text and session key matches for the provided random key, the process is continued else it stops

Our system insists an OTP method to ensure security using random key and session key generation. Usually ATM systems do not provide such an elegant feature for money withdrawal. The cash is curled by the unauthorized personnel if he holds ATM card and pin number. Even if the mobile is lost, then the process is

continued with mail address. The exchanges in mail is highly preserved nowadays **.**Dual range of security is preferred in our system as if like 3D security.

V1. CONCLUSION

The cash could be withdrawn without smart card in an efficient and secured manner. It possess less time consumption when compared `to other alternatives. The access proceeds for a period that lasts until the card pricks our hand. The activeness of either mobile or mail is mandatory. Within an ATM malware attack the criminal is able to run unauthorized software, or authorized software in an unauthorized manner, at the ATM PC in order to perform one of this attacks. Targets the control of the dispense function in order to "Cash-Out" the ATM.

REFERENCES

[1]"Security Analysis of Password-Authenticated Key Retrieval "SeongHan Shin, Non-Member, IEEE, and Kazukuni Kobara, Non-Member, IEEE,2017
[2] X. Boyen, ”Hidden Credential Retrieval from a Reusable Password”, In Proc. of ASIACCS 2009, pp. 228-238, ACM Press,2009.
[3] S. M. Bellovin and M. Merritt, ”Encrypted Key Exchange: Password-based Protocols Secure against Dictionary Attacks”, In Proc. of IEEE Symposium on Security and Privacy, pp. 72-84, IEEE Computer Society, 2012.
[4] S. M. Bellovin and M. Merritt, ”Augmented Encrypted Key Exchange: A Password-based Protocol Secure against Dictionary Attacks and Password File Compromise”, In Proc. of ACM CCS’93, pp. 244-250, ACM Press, 1993.
[5] W. Ford and B. S. Kaliski, ”Server-Assisted Generation of a Strong Secret from a Password”, In Proc. of the 9th IEEE International Workshops on Enabling Technologies: Infrastructure for Collaborative Enterprises (WET-ICE 2000), pp. 176-180, IEEE Press, 2000.
[6] L. Fang, S. Meder, O. Chevassut, and F. Siebenlist, ”Secure Password-based Authenticated Key Exchange for Web Services”, In Proc. of the ACM Workshop on Secure Web Services (SWS), ACM, 2004.
[7] IEEE 1363, ”IEEE Standard Specifications for Public-Key Cryptography”, IEEE Std 1363TM-2000, IEEE Computer Society,2000.
[8] Submissions to IEEE P1363.2. http://grouper.ieee.org/ groups/1363/passwdPK/submissions.html.
[9] IEEE 1363.2, ”IEEE Standard Specifications for Password based Public-Key Cryptographic Techniques”, IEEE Std 1363.2TM-2008, IEEE Computer Society, January 2009.
[10] ISO/IEC 11770-4, ”Information Technology□Security Techniques□Key Management□Part 4: Mechanisms Based on Weak Secrets”, International Standard ISO/IEC 11770- 4:2006(E), May 2006.
[11] Research Papers on Password-based Cryptography. http:// www.jablon.org/passwordlinks.html.
[12] D. P. Jablon, ”Password Authentication Using Multiple Servers”, In Proc. of CT-RSA 2001, LNCS 2020, pp. 344-360, Springer-Verlag, 2001.
[13] T. Kwon, ”Virtual Software Tokens - A Practical Way to Secure PKI Roaming”, In Proc. of the Infrastructure Security (InfraSec), LNCS 2437, pp. 288-302. Springer-Verlag, 2002.
[14] P. C. van Oorschot and M. J. Wiener, ”On Diffie-Hellman Key Agreement with Short Exponents”, In Proc. of EUROCRYPT’96, LNCS 1070, pp. 332-343, Springer-Verlag, 1996.
[15] R. Perlman and C. Kaufman, ”Secure Password-based Protocol for Downloading a Private Key”, In Proc. of Network and Distributed System Security Symposium, Internet Security, 1999.
[16] R. Sandhu, M. Bellare, and R. Ganesan, ”Password Enabled PKI: Virtual Smartcards vs. Virtual Soft Tokens”, In Proc. of the 1st Annual PKI Research Workshop, pp. 89-96, 2002.
[17] X. Wang, ”Intrusion-Tolerant Password-Enabled PKI”, In Proc. of the 2nd Annual PKI Research Workshop, pp. 44-53, 2003
[18] B.Kiran Bala, A Novel Approach to Generate a Key for Cryptographic Algorithm, Journal of Chemical and Pharmaceutical Sciences, Special Issue 2: February 2017, Pages 229-231.
[19] B.Kiran Bala, A Novel Approach to Identify the Micro calcification Images, Journal of Chemical and Pharmaceutical Sciences, SpecialIssue2: February 2017, Pages 190-192.
[20] B.Kiran Bala, J Lourdu, Multimodal Biometrics using Cryptographic Algorithm, European Journal of Academic Essays,2014, pages 6-10
[21] Bala B. K, Kumar A. B. The Combination of Steganography and Cryptography for Medical Image Applications. Biomed Pharmacol J 2017;10(4).
[22] B.Kiran Bala, Biometrics for Mobile Banking, International Journal of Technology and Engineering System, 2011, Volume 2, Issue 1,Pages95-97.

[23] B.Kiran Bala, R.Sasikumar, Identification Of Cancer From The Mammogram Images By Using Frequency Domain Approaches,International Journal of ChemTech Research, April 2017, Volume 10 No.5.
[24] B.Kiran Bala, T.m.nithya, Remedy For Disease Affected Iris In Iris Recognition, International Journal of Research in Engineering and Technology, November Issue 2012, ISSN: 2319 – 1163, page No. 332-334.
[25] B. Kiran Bala and R. Sasi Kumar, Different Variety of Tomato Cultivation without Soil by Using Internet of Things Research, Biosci. Biotech. Res. Comm. 10(4): 802-804 (2017).
[26] Bala B.K, Audithan S, Wavelet and curvelet analysis for the classification of micro calcification using mammogram images, 2 nd International Conference on Current Trends in Engineering and Technology, 2014.
[27] Kiran Bala B, Audithan S, Kannan G and Raja K, Frequency Domain Approaches for Breast Cancer Diagnosis, Australian Journal of Basic and Applied Sciences, 10 (2), 2016, 93-96.
[28] STUDY ON QUALITY OF WORK LIFE IN ADITYA TRADING SOLUTION PVT. LTD, B.Kiran Bala, IRACST- International Journal of Research in Management & Technology (IJRMT), ISSN: 2249-9563,Vol. 3, No.1, February 2013.
[29] B.KIRAN BALA, ENHANCED EXPRESSIVITY USING DEONTIC LOGIC AND REUSE MEASURE OF ONTOLOGIES, Elsevier, Procedia Computer Science 54 (2015) 318 – 326.