Shodhshauryam, International Scientific Refereed Research Journal
© 2018 SISRRJ | Volume 1 | Issue 4 | ISSN : 2581- 6306

Secured Payment card Transaction Using Face Recognition

Esaiya. L.C*[1], Baala Vibi. A[1], Jeevitha.C[1], Athithi Melli[1], Dhivya. S[2]

*[1]UG Scholar, Department of Computer Science Engineering, Avinashilingam Institute for Home Science and Higher Education for Women, Coimbatore, Tamil Nadu, India

[2]Assistant professor, Department of Computer Science Engineering, Avinashilingam Institute for Home Science and Higher Education for Women, Coimbatore, Tamil Nadu, India

ABSTRACT

Payment cards including the credit card and debit cards are part of a payment system issued by financial institutions, such as a bank, to a customer that enables the cardholder to access the funds in the designated bank accounts make payments by electronic funds transfer and access automated teller machines (ATM). These machines become insecure due to the operations such as identity verification only by the corresponding PIN number of card. This leads to the attempt of using the ATM card by others to perform the fraudsters' operations. In order to handle these insecure situations, the authenticated delegation method is proposed in this paper along with the method of facial recognition. The proposed system achieves the better security model in the ATM environment.

Keywords: Authentication, Banking, Delegation, Facial Recognition, VPN

I. INTRODUCTION

All ATM machines, at a minimum, will permit cash withdrawals of customers of the machine's owner (if a bank-operated machine) and for cards that are affiliated with any ATM network, the machine is also affiliated. They will report the amount of the withdrawal and any fees charged by the machine on the receipt. Most banks and credit unions will permit routine account-related banking transactions at the bank's own ATM, including deposits, checking the balance of an account, and transferring money between accounts.

There are a number of types of payment cards, the most common being credit cards and debit cards. Most commonly, a payment card is electronically linked to an account or accounts belonging to the cardholder. These accounts may be deposit accounts or loan or credit accounts, and the card is a means of authenticating the cardholder. However, stored-value cards store money on the card itself and are not necessarily linked to an account at a financial institution.

It can also be a smart card that contains a unique card number and some security information such as an expiration date or CVV or with a magnetic strip on the back enabling various machines to read and access information.

A security card system that includes a security card having an appearance like a real credit card or other bank card, and a security network that contains a security firm that enrolls persons in the system who have been provided with a security card by a card-issuing institution, and uses the security network for responding to emergency calls initiated by use of the

security card, reports fraud, and in general, implements an emergency system and acts as a theft warning.

Data security technologies include backups, data masking and data erasure. A primary data security technology is modelled with encryption, where digital data, software/hardware, and hard drives are encrypted and therefore rendered unreadable to unauthorized users and hackers. One of the most commonly encountered methods of practicing data security is the use of authentication. With authentication, users must provide a password, code, biometric data, or some other form of data to verify identity before access to a system or data is granted.

Online shopping and the banking process is the retrieval of product information via the Internet and issue of purchase order through electronic purchase request, filling of credit or debit card information and shipping of product by mail order or home delivery by courier. Identity theft and phishing are the common dangers of online shopping. Identity theft is the stealing of someone's identity in the form of personal information and misuse of that information for making purchase and opening of bank accounts or arranging credit cards. Phishing is a criminal mechanism that employs both social engineering and technical subterfuge to steal consumers' personal identity data and financial account credentials. In 2nd quarter of 2013, Payment Service, Financial and Retail Service are the most targeted industrial sectors of phishing attacks. Secure Socket Layer (SSL) encryption prevents the interception of consumer information in transit between the consumer and the online merchant.

A payment system that utilizes the Internet to gain access to an Internet banking system enabling a user to purchase merchandise bought through an online merchant or merchant who has Internet access in their store is disclosed. The payment system may also be utilized to provide a means for a user to retrieve and view balances and account transaction information for their bank accounts and to transfer funds between accounts. The system uses a "virtual pin-pad" which provides a web-based, stand-alone method of payment that is independent of banks and capable of performing real-time currency conversions.

II. RELATED WORK

Data security and privacy are now considered as the major concerns in the Banking environment. The web and mobile environment constructs an amazing infrastructure for the current day banking transactions. A genuine security issue revolves around electronic currency and digital cash which is built around critical customer information for which customer can be exposed to and thus information security and privacy becomes the important matter in digital economy. Building and implementing security within the banking system is fundamental to success. The safe storage of customer data is foremost importance and, for it to be achieved, it is crucial that the bank's system must not store the crucial and sensitive customer data unless it is key business requirement.

Data Security concerns the protection of data from accidental or intentional but unauthorized modification, destruction or disclosure through the use of physical security, administrative controls, logical controls, and other safeguards to limit accessibility.

Data Encryption, converting the data into a code that cannot be easily read without a key that unlocks it. Data Masking, masking certain areas of data so personnel without the required authorization cannot look at it. Data Erasure, ensuring that no longer used data is completely removed and cannot be recovered by unauthorized people. Data Backup, creating copies of data so it can be recovered if the original copy is lost.

Mobile devices and browser-based account access quickly became the preferred way to interact with the bank. Although banks deploy a number of strong security measures to keep the data safe, they can't protect against every threat. This is where VPNs come into play. Using a VPN while online banking can stop all sorts of attacks, including attempted identity thefts.

III. SYSTEM DESIGN

Attribute based encryption that is also known as ABE is a type of public-key encryption in which the secret key of a user and the cipher text are dependent upon attributes. In an ABE system, a user's keys and cipher texts are labelled with sets of descriptive attributes and a particular key can decrypt a particular cipher text only if there is a match between the attributes of the cipher text and the user's key. It reduces the number of key used and thus make encryption and decryption process faster.

Delegation is the assignment of any responsibility or authority to another person (normally from a manager to a subordinate) to carry out specific activities. It is one of the core concepts of management leadership. However, the person who delegated the work remains accountable for the outcome of the delegated work. Delegation empowers a subordinate to make decisions, i.e. it is a shifting of decision-making authority from one organizational level to a lower one. The opposite of effective delegation is micromanagement, where a manager provides too much input, direction, and review of delegated work. The delegation is mainly developed with the ABE to secure the data using the dynamic method of encryption.

VPNs, or virtual private networks, have been around for decades. Their use skyrocketed in the last few years thanks to increasing concern over basic online security. With governments tracking users, ISPs collecting and selling data, and hackers looking for an easy mark, there's no shortage of dangers on the world wide web. VPNs neatly defeat these problems by including encryption on every packet of data that leaves the device. VPN software wraps information in an unbreakable layer of code that prevents anyone from seeing what a packet contains.

VPNs also provide virtual location variability using the IP masking process. IP addresses can also use to identify the location of the device and even trace content back to ISP account, instantly removing any privacy information in the VPN. VPNs are perfect for daily use, but they're especially useful for obscuring sensitive information, things like e-mails, credit card numbers, and of course, online banking details.

IV. IMPLEMENTATION

The proposed delegation system is implemented using the VPN model along with the banking environment and the authentication process as follows.

A. VPN Processing

With a VPN in place, the only IP address the world sees is the one associated with their servers, allowing the connected device as remain hidden online. Each time the device connects to the internet then the IP address is reassigned. This collection of numbers allows data to be routed back to the device, almost like a mailing address for digital content.

1. User requests for VPN Remote Access Service are initiated through the departmental IT Technical Liaison or designated system administrator and VPN is available only to faculty and staff.
2. Departments determine who will be authorized for VPN Remote Access Service within their department.
3. VPN Remote Access Service is authorized only after the IT designated system administrator has

confirmed that the user has reviewed the University's VPN Service Policy, especially the requirements outlined in the Responsibility of Users section of the policy.

4. Information Technology supports the VPN network device, the VPN client, a method for Systems Administrators to grant their users access to the VPN service through the registration process, documentation for installing the VPN client.
5. The departmental IT Technical Liaisons or designated system administrators are the user's primary point of contact for assistance with installation of the VPN client and resolution of problems with individual user client set-up and operation.

B. Delegation environment

The figure-1 shows the working model of the proposed system.

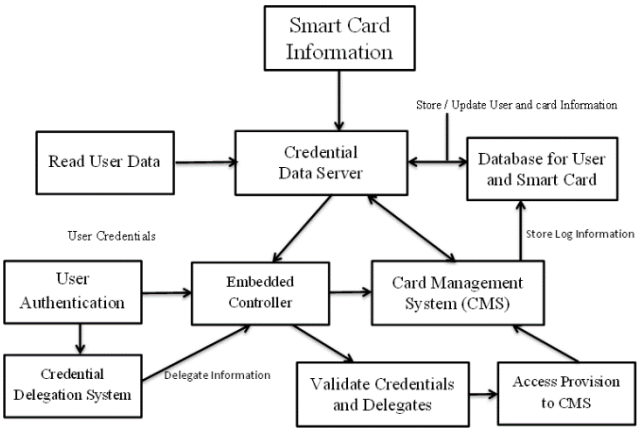

Figure 1. Authentication and Delegation system for payment card processing model.

The credential server is responsible for retrieving and storing the user information and session state, as well as admission control. In the banking system, the session management system lies in the critical connection and the corresponding requests validation process which needs to reliably perform its tasks in near real-time without substantial overhead in the authentication process.

Card Management System (CMS) is designed to maintain the access control and validation process during the smart card handling model. The smart card information corresponding to the banking user is maintained in the database. During the cash transactions performed in the ATM environment, the facial recognition process is executed by applying the pattern matching.

The facial recognition system is capable of identifying or verifying a person in the video frame retrieved from the video source operated in the ATM environment. By employing the feature extraction process, the facial points are retrieved and stored in the database. The retrieved points are used during the authentication process.

Before initiating data access to the alternate user, the delegated registration is performed to provide authorization. During delegated registration process, the unique id is generated from system to every registered user and it is provided in the form of OTP (One Time Password). And the corresponding user entry is created in database to establish authorized access to banking server.

The connected embedded controller fetches the information from the banking server and validates the user by applying the authentication and authorization process. Upon completion of the success authorization, the payment and other related operations are invoked. The same process of authentication for the delegated user is validated with the assistance of the OTP generated during the delegated registration process.

V. CONCLUSION

The payment cards possess the higher significance in the banking structure including in the ATM environment. These machines become insecure due to the indirect identity verification process which is only based on corresponding PIN number of card. In order to handle this insecure model, the authentication process is enhanced with the

delegation process. The proposed delegation system provides the higher level security using the delegated authentication and authorization process. In future the optimization model can be used to reduce the communication latency in the VPN environment.

VI.REFERENCES

[1] Dutta, Mithun, Kangkhita Keam Psyche, and Shamima Yasmin. "ATM Transaction Security Using Fingerprint Recognition." American Journal of Engineering Research (AJER) 6, no. 8 (2017): 41-45.

[2] Bist, Pooja Karan, Akansha Santosh Mekade, Anurag Mohan Nair, and Madhumita Chatterjee. "Secure VPN Server Deployed on Raspberry Pi." Journal of Network Communications and Emerging Technologies (JNCET) www. jncet. org 8, no. 5 (2018).

[3] Chiu, Chih-Cheng, Tung-Kuan Liu, Weu-Ting Lu, Wen-Ping Chen, and Jyh-Horng Chou. "A micro-control capture images technology for the finger vein recognition based on adaptive image segmentation." *Microsystem Technologies* (2018): 1-14.

[4] Jiang, Yinhao, Willy Susilo, Yi Mu, and Fuchun Guo. "Ciphertext-policy attribute-based encryption against key-delegation abuse in fog computing." Future Generation Computer Systems 78 (2018): 720-729.

[5] Lee, Wai-Kong, Chun-Farn Leong, Weng-Kin Lai, Lee-Kien Leow, and Thiah-Huat Yap. "ArchCam: Real time expert system for suspicious behaviour detection in ATM site." Expert Systems with Applications 109 (2018): 12-24.

[6] Masala, Giovanni L., Pietro Ruiu, and Enrico Grosso. "Biometric authentication and data security in cloud computing." In Computer and Network Security Essentials, pp. 337-353. Springer, Cham, 2018.

[7] Onyesolu, Moses O., and Amara C. Okpala. "Improving Security Using a Three-Tier Authentication for Automated Teller Machine (ATM)." International Journal of Computer Network and Information Security 9, no. 10 (2017): 50.

[8] Risodkar, Y. R., Ashwini B. Pawar, Sampada N. Chavanke, and Ashwini S. Pawar. "ATM Authentication with Enhance Security Using GSM." Journal of Science and Technology (JST) 2, no. 5 (2017): 01-05.

[9] Sahai, Amit, Hakan Seyalioglu, and Brent Waters. "Dynamic credentials and ciphertext delegation for attribute-based encryption." In Advances in Cryptology–CRYPTO 2012, pp. 199-217. Springer, Berlin, Heidelberg, 2012.

[10] Schaper, Meilin, Tim H. Stelkens-Kobsch, and Nils Carstengerdes. "From preparation to evaluation of integrated ATM-security-prototype validations." In Digital Avionics Systems Conference (DASC), 2017 IEEE/AIAA 36th, pp. 1-8. IEEE, 2017.

[11] Zhang, Tao, Jingjing Li, Wenjing Jia, Jun Sun, and Huihua Yang. "Fast and robust occluded face detection in ATM surveillance." Pattern Recognition Letters 107 (2018): 33-40.