International Journal of Advanced Technology in Engineering and Science
Vol. No.7, Issue No. 03, March 2019
www.ijates.com
ijates
ISSN 2348 - 7550

REMOTE ACCESS TO IMPROVE ATM SECURITY BY USING IOT

Deepan.S, Sathishkumar.N, Naveen Kumar.S

Department of Electrical and Electronics Engineering,

Sengunthar Engineering College, Tiruchengode, Namakkal-637205, Tamil Nadu (India)

GOHILA.T M.Tech

Associate Professor of EEE,

Sengunthar Engineering College, Tiruchengode, Namakkal-637205, Tamilnadu (India)

ABSTRACT

Our project proposes a securedATM (Automated Teller Machine) system using a card scanning system along with LINK system for improved security. Usual ATM systems do not contain the LINK feature for money withdrawal. If an attacker manages to get hold of ATM card and the pin number, he may easily use it to withdraw money fraudulent. So our proposed system supports the ATM card scanning system along with an LINK system. This user may scan his card and login to the system. But after user is through with this authentication he may view details but is asked to enter LINK as soon as he clicks money withdrawal option. At this stage the system generates and sends an LINK to the registered mobile number to that particular user. The password is generated ad sent to the user mobile phone. He now needs to enter the LINK in the system in order to withdraw money. Thus our system provides a totally secure way to perform ATM transactions with two level security structure.

***Key Words*: ATM,Bio-metric,GSM,GPS,PIN**

1. INTRODUCTION

An embedded system is some combination of computer hardware and software, either fixed in capability or programmable, that is designed for a specific function or for specific functions within a larger system. Industrial machines, agricultural and process industry devices, automobiles, medical equipment, cameras, household appliances, airplanes, vending machines and toys as well as mobile devices are all possible locations for an embedded system. Embedded systems are computing systems, but can range from having no user interface (UI) -- for example, on devices in which the embedded system is designed to perform a single task -- to complex graphical user interfaces (GUI), such as in mobile devices. User interfaces can include buttons, LEDs, touchscreen sensing and more. Some systems use remote user interfaces as well. Embedded systems can be microprocessor or microcontroller based. In either case, there is an integrated circuit (IC) at the heart of the product that is generally designed to carry out computation for real-time operations. Microprocessors are visually indistinguishable from microcontrollers, but whereas the microprocessor only implements a central processing unit (CPU) and thus requires the addition of other components such as memory chips, microcontrollers are designed as self-contained systems. Embedded systems can be

microprocessor or microcontroller based. In either case, there is an integrated circuit (IC) at the heart of the product that is generally designed to carry out computation for real-time operations. Microprocessors are visually indistinguishable from microcontrollers, but whereas the microprocessor only implements a central processing unit (CPU) and thus requires the addition of other components such as memory chips, microcontrollers are designed as self-contained systems.

With the development of computer network technology and e-commerce, the self-service banking system has got extensive popularization with the characteristic offering high-quality 24 hours service for customer. Nowadays, using the ATM (Automatic Teller Machine) which provides customers with the convenient banknote trading is very common. However, the financial crime case rises repeatedly in recent years; a lot of criminals tamper with the ATM terminal and steal user's credit card and password by illegal means. Once user's bank card is lost and the password is stolen, the criminal will draw all cash in the shortest time, which will bring enormous financial losses to customer. How to carry on the valid identity to the customer becomes the focus in current financial circle. Traditional ATM systems authenticate generally by using the credit card and the password, the method has some defects[4]. Using credit card and password cannot verify the client's identity exactly. Anyone who knows the PIN and have the ATM card can easily access the user account.

Figure1. ATM. This paper describes a new method combining with the traditional method. Here RFID and GSM is used to improve the security of the transaction[2][3]. To overcome the disadvantages of inserting the ATM card into the ATM machine, RFID card is used. It reads the user information by sensing and it also manages different banks accounts in a single RFID card. The GSM is used to improve the security by providing OTP and also informs the user by an SMS in case the entered password is wrong.

The Internet of Things (IoT) is a system of interrelated computing devices, mechanical and digital machines, objects, animals or people that are provided with unique identifiers and the ability to transfer data over a network without requiring human-to-human or human-to-computer interaction. The IoT is a giant network of connected things and people – all of which collect and share data about the way they are used and about the environment around them. That includes an extraordinary number of objects of all shapes and sizes – from smart microwaves, which automatically cook your food for the right length of time, to self- driving cars, whose complex sensors detect objects in their path, to wearable fitness devices that measure your heart rate and the number of steps you've taken that day, then use that information to suggest exercise plans tailored to you. There are even connected footballs that can track how far and fast they are thrown and record those statistics via an app for future training purposes.

2. LITERATURE SURVEY

1. Enhancing security and privacy in biometrics- based authentication systems: N. K. Ratha, J. H. Connell, R. M. Bolle

Reliable user authentication is becoming an increasingly important task in the Web-enabled world. The consequences of an insecure authentication system in a corporate or enterprise environment can be catastrophic, and may include loss of confidential information, denial of service, and compromised data integrity. The value of reliable user authentication is not limited to just computer or network access. Many other applications in everyday life also require user authentication, such as banking, ecommerce, and physical access control to computer resources, and could benefit from enhanced security. It is important that such biometrics-based

authentication systems be designed to withstand attacks when employed in security-critical applications, especially in unattended remote applications such as ecommerce. In this paper we outline the inherent strengths of biometrics-based authentication, identify the weak links in systems employing biometrics-based authentication, and present new solutions for eliminating some of these weak links. Although, for illustration purposes, fingerprint authentication is used throughout, our analysis extends to other biometrics-based methods.

2. Graphical Password Authentication: Implementation and Evaluation of Personalized Persuasive Cued Click Points: Asher D'Mello, Rohan Bagwe, Victor Fernandes, Ankita Karia

Persuasive Cued Click-Points (PCCP) is an integrated evaluation of the graphical password scheme, including usability and security evaluations, and implementation considerations. The systematic examination provides a comprehensive and integrated evaluation of PCCP covering both usability and security issues. An important usability goal for knowledge-based authentication systems is to support users in selecting passwords of higher security, in the sense of being from an expanded effective security space. This research work explores the possibility of designing and constructing a module that is easily pluggable into the existing authentication systems being used as of now. The working prototype is an open source simulation consisting of all the necessary modules to build the authentication system. This system is built using Java and Oracle 10g Express Edition as thedatabase although most database systems can be used.

3. A Smart User Interface to Prevent Shoulder Surfing Attack Using Color Code: Yathiraj GR, Santosh VG, Sushma KR, Muthappa KU

Classical PIN entry mechanism is broadly used for authenticating a user. It is a popular scheme because it properly balances the usability and safety aspects of a organism. However ,if this scheme is to be used in a public system then the design might endure since accept surfing attack. In this attack, an unauthorized user can completely or partially watch the login session .Even the activities of the login gathering can be recorded which the attacker can use it soon after to get the actual PIN. In this paper ,we suggest an intelligent user interface, known as Color Pass to oppose the accept surfing attack so that any authentic user can enter the session PIN without disclosing the authentic PIN. The Color Pass is based on a partially noticeable attacker model. The experimental analysis shows that the Color Pass interface is secure and simple to use even for novice users.

4. Biometric Online Signature Verification: Fincy Francis1, Aparna M.S, Anitta Vincent

Person identification can be done precisely by Biometrical method, where physiological or behavioral characteristics are used for this purpose. Handwritten signature is a behavioral trait it can be used for person identification accurately. There are two types of identification modes either online or offline mode. Which depends upon the signature acquisition method. In offline acquisition method the shape of the signature is used for authenticating signer. While in online signature verification uses dynamic characters that is dynamic time dependent of the signature to authenticate the signer. This paper describes the implementation on field programmable gate arrays (FPGAs) of an embedded system for online signature verification. The online signature recognition algorithm mainly consists of three stages. Initial pre-processing is the first stage which is applied on the captured signature for removing noise and normalizing information related to horizontal and vertical positions. Dynamic time warping algorithm is used to align this processed signature with its template previously stored in a database. Finally, a set of features is extracted and passed through a Gaussian Mixture Model. Degree of similarity between both signatures can be find out from this. For fast computation of floating

point calculations vector floating point unit is used

(VFPU). Additionally system consists of a microprocessor which interacts with the VFPU. All the procedures of verification can be done in software. Furthermore this paper studies about online signature verification on touch interface- based mobile devices. A simple and effective method for signature verification is developed. An online signature is represented with a discriminative feature vector derived from attributes of several histograms that can be computed in linear time. The resulting signature template is compact and requires constant space.

5. Touchscreen Mobile Authentication Using Multi-Touch Sequential Gestures: Balaji Chaugule*, Prof. Asha Pawar

Recently all handheld devices are touch screen and the popularity of touchscreen devices increases more and more due to the easy fast Internet access and large storage capacity. People may store their all personal information such as banking detail, password, confidential documents, trade secrets etc. on the handheld devices. In any case such handheld device is lost or stolen then security of such handheld device are more important because it contains users personals, banking information, secrets of user and that can be misuse by unauthorized person in any terrorist activity or other purposes that harm to user financially and socially. Securing the personal data stored and accessed from android touchscreen mobile makes user authentication a problem of paramount importance. The rigidity between security and usability renders however the task of user authentication on mobile devices a challenging task. This paper introduces Multi-Touch Authentication and unauthorized user tracking technique to protect mobile banking data stored on touch screen mobile devices (Finger gestures with priority Authentication System using Touch screen Devices), a behavioural touch screen based authentication approach on mobile devices. Besides extracting touch data from touch screen equipped smart phones. This system complements and validates this data using a touch screen mobile device. A addressable feature in the system is its continuity, users transparent post login authentication and tracing of location of mobile devices.

6. The Anatomy of Smartphone Unlocking: A Field Study of Android Lock Screens: Marian Harbach1, Alexander De Luca2, Serge Egelman

To prevent unauthorized parties from accessing data stored on their smartphones, users have the option of enabling a "lock screen" that requires a secret code (e.g., PIN, drawing a pattern, or biometric) to gain access to their devices. We present a detailed analysis of the smartphone locking mechanisms currently available to billions of smartphone users worldwide. Through a month-long field study, we logged events from a panel of users with instrumented smartphones. We are able to show how existing lock screen mechanisms provide users with distinct tradeoffs between usability (unlocking speed vs. unlocking frequency) and security. We find that PIN users take longer to enter their codes, but commit fewer errors than pattern users, who unlock more frequently and are very prone to errors. Overall, PIN and pattern users spent the same amount of time unlocking their devices on average. Additionally, unlock performance seemed unaffected for users enabling the stealth mode for patterns.

7. Color PIN- Securing PIN entry through indirect input: Alexander de luca

Automated teller machine (ATM) frauds are increasing drastically these days. When analyzing the most common attacks and the reasons for successful frauds, it becomes apparent that the main problem lies in the PIN

based authentication which in itself does not provide any security features (besides the use of asterisks). That is, security is solely based on a user's behavior. Indirect input is one way to solve this problem. This mostly comes at the costs of adding overhead to the input process. We present ColorPIN, an authentication mechanism that uses indirect input to provide security enhanced PIN entry. At the same time, ColorPIN remains aone-to- one relationship between the length of the PIN and the required number of clicks. A user study showed that ColorPIN is significantly more secure than standard PIN entry while enabling good authentication speed in comparison with related systems.

8. DRAW-A-PIN: Authentication using finger- drawn PIN on touch devices Toan Van Nguyen, Napa Sae-Bae , Nasir Memon

This paper presents DRAW-A-PIN, a user authentication system on a device with a touch interface that supports the use of PINs. In the proposed system, the user is asked to draw her PIN on the touch screen instead of typing it on a keypad.

Consequently, DRAW-A-PIN could offer better security by utilizing drawing traits or behavioral biometrics as an additional authentication factor beyond just the secrecy of the PIN. In addition, DRAW-A-PIN inherently provides acceptability and usability by leveraging user familiarity with PINs. To evaluate the security and usability of the approach, DRAW-A-PIN was implemented on Android phones and 3203 legitimate finger-drawn PINs and 4655 forgery samples were collected through an extensive and unsupervised field experiment over 10 consecutive days. Experimental results show that DRAW-A-PIN achieves an equal error rate of 4.84% in a scenario where the attacker already knows the PIN by shoulder surfing. Finally, results from a user study based on the System Usability Scale questionnaire confirm that DRAW- A-PIN is highly usable.

9. Reducing Shoulder-surfing by Using Gaze- based Password Entry: Manu Kumar, Tal Garfinkel, Dan Boneh, Terry Winograd

Shoulder-surfing – using direct observation techniques, such as looking over someone's shoulder, to get passwords, PINs and other sensitive personal information – is a problem that has been difficult to overcome. When a user enters information using a keyboard, mouse, touch screen or any traditional input device, a malicious observer may be able to acquire the user's password credentials. We present EyePassword, a system that mitigates the issues of shoulder surfing via a novel approach to user input. With EyePassword, a user enters sensitive input (password, PIN, etc.) by selecting from an on-screen keyboard using onlythe orientation of their pupils (i.e. the position of their gaze on screen), making eavesdropping by a malicious observer largely impractical. We present a number of design choices and discuss their effect on usability and security. We conducted user studies to evaluate the speed, accuracy and user acceptance of our approach. Our results demonstrate that gaze- based password entry requires marginal additional time over using a keyboard, error rates are similar to those of using a keyboard and subjects preferred the gaze-based password entry approach overtraditional methods

10. SkullConduct: Biometric User Identification on Eyewear Computers Using Bone Conduction Through the Skull: Stefan Schneegass, Youssef Oualil

Secure user identification is important for the increasing number of eyewear computers but limited input capabilities pose significant usability challenges for established knowledge based schemes, such as passwords or PINs. We present Skull- Conduct, a biometric system that uses bone conduction of sound through the user's

skull as well as a microphone readily integrated into many of these devices, such as Google Glass. At the core of SkullConduct is a method to analyze the characteristic frequency response created by the user's skull using a combination of Mel Frequency Cepstral Coefficient (MFCC) features as well as a computationally light-weight 1NN classifier. We report on a controlled experiment with 10 participants that shows that this frequency response is person specific and stable – even when taking off and putting on the device multiple times – and thus serves as a robust biometric.

We show that our method can identify users with 97.0% accuracy and authenticate them with an equal error rate of 6.9%, thereby bringing biometric user identification to eyewear computers equipped with bone conduction technology.

3. EXISTING SYSTEM

The existing ATM Simulation System was built for the original concept of regional private banks. Small banks in villages and towns will service the needs of the local community and will only require ledgers to record account details. This system is prone to human error and causes undue frustration to users. This system was augmented with the introduction of excel sheets and emails. Banks could now record all information in an excel sheet and then set an update schedule when they will mail all records to a central hub where these records will again be processed and consolidated to form a unified record of all account transactions. These systems did not enable easy access to money and were greatly prone to grievous errors.

Security of these details is also a top priority in this system. This central hub will be accessed by an ATM for secure customer transactions. In our project we are going to place an extra button in ATM machines. When that button got pressed the control window will be telecasted to accountant cellular phone. Then the accountant can enter the pin and amount manually in his mobiles telecasted pop-up window. By this control system accountant can keep his pin number with him and he can vend the amount by his own control by the desired person

5. METHODOLOGY

This project was developed by analyzing the requirements and by fully understanding the problems. The solution was made by using advanced methods implemented for the next level to give appropriate result

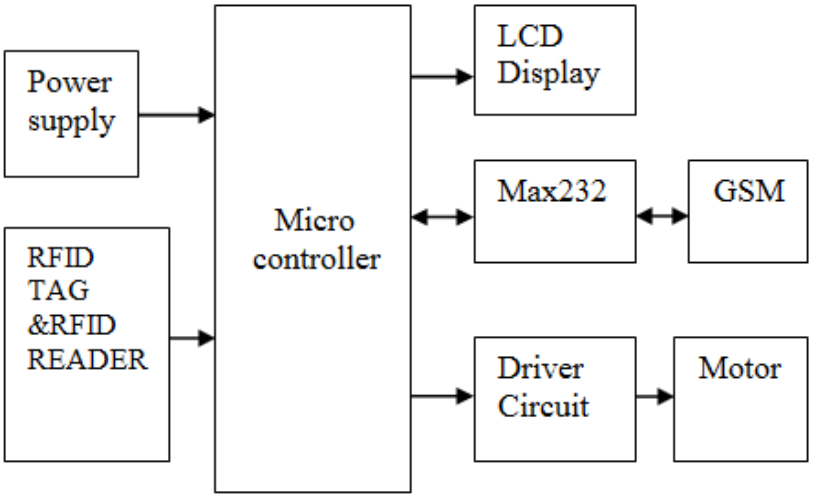

Fig.1

6. PROPOSED SYSTEM

The proposed system aims to solve all this by constant updating of bank records. The Java based construction of the system will enable transactions at any bank or ATM to be registered within a matter of seconds.

This block diagram shows the entire system for the development of the paper. This shows the total control is based on the microcontroller (ARDUINO). It includes the components are power supply,GSM, personal computer,RFID TAG AND RFID READER,LCD DISPLAY,MAX232, WIFI module motor.

7. CONCLUSION

This whole implementation ensures us a secured and authenticated transaction through RFID and GSM technique with lowest cost and minimum maintenance. Mankind will utilize new and secured type of money transactions. The only thing is that initial cost of RFID conversion of the entire system is the required one time investment. The value added service that this system provides increases the credibility of the financial institutions, the banks improves the convenience to its customer. Hence as the world progresses through the inevitable and an indomitable quest for knowledge, the aspect of security bound systems are bound to concede with the growing innovations and obviously more vulnerabilities. Hence our application might well solve the aspect of transaction security to a precise and great extent.

REFERENCE

1. G.Udaya Sree, M.Vinusha " Real Time SMS- Based Hashing Scheme for Securing Financial Transactions on ATM Terminal" ,IJSETR, ISSN 2319-8885 Vol.02,Issue.12, September-2013, Pages:1223-1227.
2. Khatmode Ranjit P, Kulkarni Ramchandra V, "ARM7 Based Smart ATM Access & Security System Using Fingerprint Recognition & GSM Technology", ISSN 2250-2459, ISO 9001:2008 Certified Journal, Volume 4, Issue 2, February 2014.
3. M.R.Dineshkumar,M.S.Geethanjali,"Protected Cash Withdrawal in ATM Using Mobile Phone", International Journal Of Engineering And Computer Science ISSN:2319-7242 Volume 2 Issue 4 April,

2013 Page No. 1346-1350 .

4. Zaid Imran,Rafay Nizaami ,"Advance Secure Login", International Journal For Science and Research Publications, Volume 1,Issue 1,December 2011.
5. M. Ajaykumar and N. Bharath Kumar," Anti- Theft ATM Machine Using Vibration Detection Sensor", IJARCSSC Volume 3, Issue 12, December 2013 ISSN: 2277 128X.
6. SURAJ B S and Dr. R GIRISHA, " ARM7 based Smart ATM Access System", International Journal on Recent and Innovation Trends in Computing and Communication ISSN: 2321-8169 Volume: 3 Issue: 5.
7. K.annan K, "Microcontroller Based Secure Pin Entry Method For ATM", International Journal of Scientific & Engineering Research, Volume 4, Issue 8, August-2013 ISSN 2229-5518.
8. Hyung-Woo Lee,"Security in Wireless Sensor Networks: Issues and Challenges", ICACT, ISBN 89-5519-129-4, Feb. 20-22, 2006.