Pin number theft recognition and cash transaction using sixth sense technology in ATM/CDM

Article *in* International Journal of Engineering and Technology · May 2018

DOI: 10.14419/ijet.v7i2.31.13435

2 authors, including:

S.Pradeep Kumar
Vels University
45 PUBLICATIONS **376** CITATIONS

SEE PROFILE

International Journal of Engineering & Technology, 7 (2.31) (2018) 178-180

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET

Research paper

Pin number theft recognition and cash transaction using sixth sense technology in ATM/CDM

S. Pradeep Kumar[1*], N. Shanmugasundaram[2]

[1]Department of Electrical and Electronics Engineering, School of Engineering, Vels Institute of Science Technology and Advanced Studies(VISTAS),Chennai, India.
[2]Department of Electrical and Electronics Engineering, School of Engineering, Vels Institute of Science Technology and Advanced Studies(VISTAS),Chennai, India.
**Corresponding author E-mail:pradeep88.se@velsuniv.ac.in*

Abstract

Nowadays peoples using credit/debit card for cash transaction for their daily needs. Meanwhile for deposit and withdrawal of huge amount the consumers use the automated teller machine or cash deposit machine. Due to this the crime related to ATM like pin number theft, fraud calls etc increasing day by day. This paper aim to reduce the risk related to pin number theft. We proposed a sixth sense technology which can access by our gestural interface to do the normal operation for cash transaction rather than touching the pin number plate which will be helpful for eliminating the theft related with pin number tracking. The experimental prototype model is designed and the results are verified and presented in this paper.

Keywords: *Automated teller machine, GSM, holographic keypad.*

1. Introduction

Automated Teller Machine was first invented by John Shepphard Barren on June 1967, at United Kingdom. Since 1967 it is one of the common systems used by many consumers. The first ATM was installed in London on June 1967, by Barclays bank. The ATM was known by different name all over the world such as Automated Transaction Machine (USA), Automated Banking Machine (Canada), Cash Point (England), Hole in the wall (Europe), Ban Comet (Russia) etc. Nowadays for operating several devices such as mobile, ATM we require pin number or password. Using that pin number and password without safely is the main complexity faced by consumers. Attacks on ATM are not only for cash but also to obtain the customers data. The criminals are using complicated cyber method to take the customer data and money [1]. An automatic video surveillance method using digital image processing along with the combination of computer vision and unsupervised machine learning techniques is used to prevent the ATM from theft in [2]. A liquid crystal display keypad is used to confuse the person standing nearby while transaction and a wireless medium using Bluetooth interface between user and ATM using UTLP kit for preventing from pin thefts was proposed in [3]. A low cost stand-alone embedded web server based on ARM11 processor and Linux operating system using Raspberry Pi was proposed for ATM security includes camera control, sensors shutter lock etc [4]. This system provides ATM traffic management to optimize the use of network resources and protect against network jamming and users performance [5]. This system proposed a users mobile phone towards for shift the pin number away from possible insecure ATM pin pad [6].

2. Classification of theft in ATM

Understanding all of the various attack vectors and crimes can seem complex and overwhelming at times but looking out over the landscape, a broader attack type and structure emerges. The attacks fall into three general categories: (i) Identity Theft (ii) Logical Theft of Valuable Media (iii) Physical Theft of Valuable Media.

Identity theft

Identity Theft refers to the category of crimes that capture the data used by a consumer to authenticate themselves at a Self-Service Terminal to enable their financial services. The most frequent attack vectors in this category include Card Skimming, Card Trapping, and Card "Sniffing." card skimming attack is defined as 'the unauthorized capture of magnetic stripe information by modifying the hardware or software of a payment device, or through the use of a separate card reader.' Skimming is often accompanied with the covert capture of customer PIN data. Armed with this information, the fraudsters create dummy cards and raid the customer's account. Eavesdropping Attacks: In this attack, a hole is made in the ATM or access gained to the top box of the ATM. Electronic hook ups are then attached directly to the card reader to attempt to capture card and PIN details. The eavesdropping attacks can be prevented by retrofitting existing ATMs with physical barriers around the internal card reader. Network sniffing attack: With this approach the criminals attempt to capture the cardholder information as it is being sent from the ATM to the ATM switch or host. This is done by attaching a device onto the network connection cables.

Logical theft

Logical Theft of valuable media refers to the category of crimes that are used to steal cash or other valuable media from the ATM using methods which do not physically breach the cash enclosure. This category is the one where there has been the greatest rise in number and variety of attacks. This category is also the one which makes use of the latest technology to exploit features of ATMs which would not have been considered vulnerable at the time of the original ATM design and manufacture. Since 2012, there has been an alarming increase in the frequency of these forms of attacks. Financial institutions, manufacturers and security experts have now seen successful logical attacks occur in all global regions. The nature of these crimes allows the attack to occur on a large number of ATMs at once. The outcome of the crime could be the theft of all of the cash in the ATM and lead to very significant financial losses in a very short period of time.
Typically, these attacks fall into three major categories:

- Black box attacks
- Malware in the Network
- Malware installed on the ATM

Physical theft

Physical Theft of valuable media-the category of crimes that are used to steal cash or other valuable media from the ATM using methods which physically breach the cash enclosure. This category includes all of the traditional robbery techniques that can be used to open a safe, and includes emerging trends such as the use of explosives. These crimes continue to be major problem for ATM operators. According to data provided by the European ATM Security Team (EAST), nearly 50 million Euros were lost from physical attacks on ATMs in 2015.

3. System architecture

In this paper we proposed a methodology for preventing from Pin number theft in ATM. In order to ensure a Hassle free Transaction we Propose a Color based non-contact / or sixth sense technology ATM for transactions system for safe transaction for the person using the ATM.

Contactless ATM mode

We use the Holographic keypad used in Sixth sense Technology to do all the Transaction which is done by pressing the keys in a ATM machine. A Holographic infra red sensor based keypad is interfaced serving as contactless Mouse for this process. This interface does all the Transaction which can be done using a mouse. Fig 1.represents the circuit diagram for the holographic IR keypad.

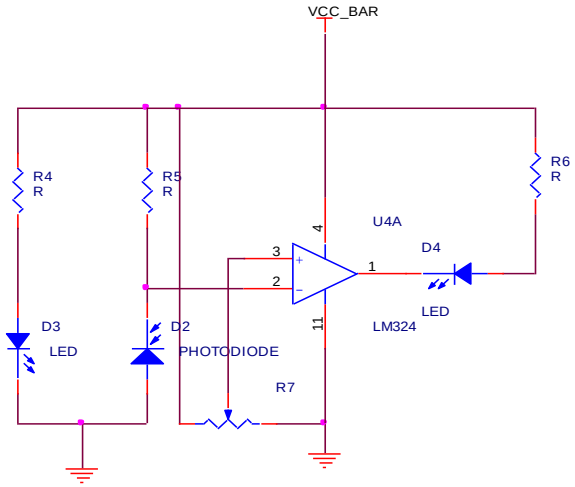

Fig. 1: Holographic IR keypad circuit diagram

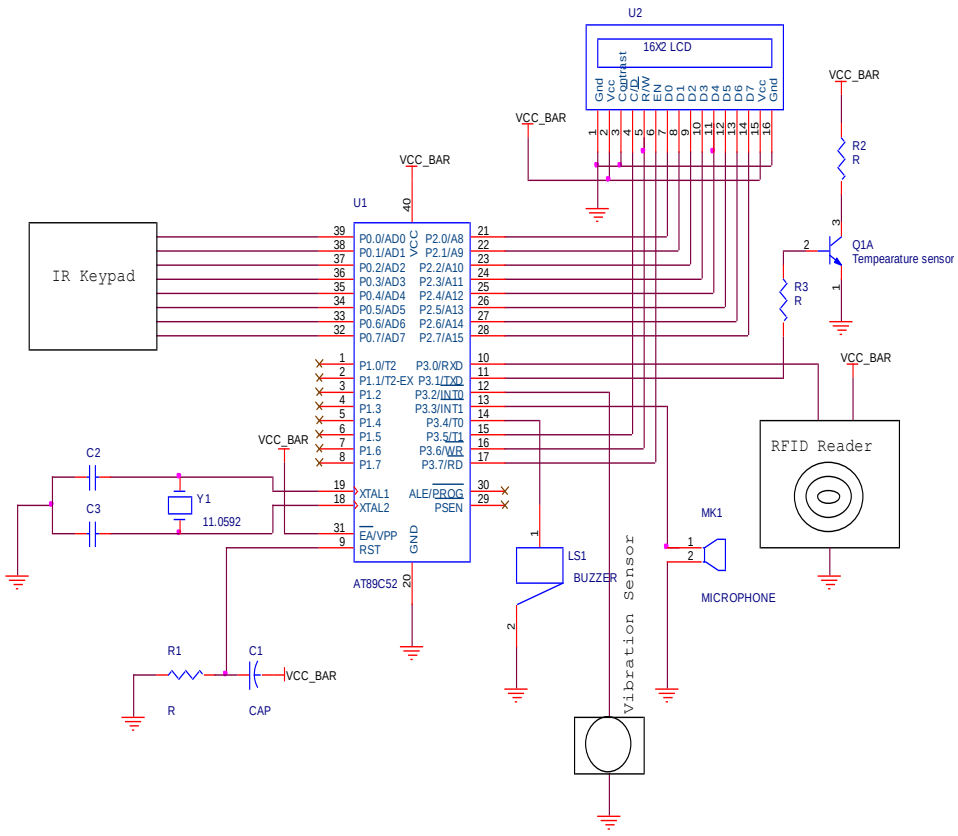

Fig. 2: Circuit diagram of the ATM setup

The above figure 2 represents the circuit diagram of our proposed system; here an IR keypad is used to sense the finger for pin number access.

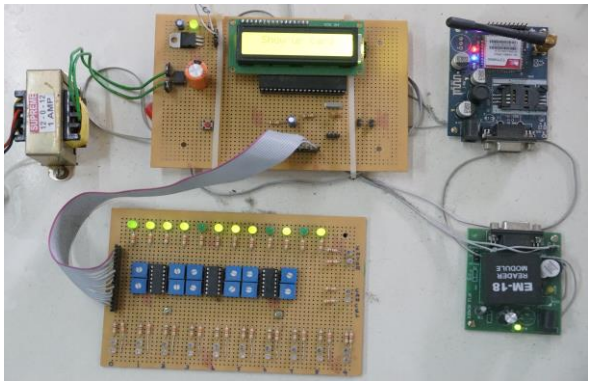

Fig. 3: Experimental prototype model of holographic keypad and ATM setup

4. Results

The prototype model was designed and the experimental verification was discussed here. A holographic keypad using IR sensor was used for accessing the pin number. Access can be done without touching the pin number plate if the finger is placed just above the pin number plate the IR sensor will sense the finger and get access. This will avoid the pin number tracking by the nearby person. The transaction process such as amount details, pin number access wrongly by unknown person will be intimated to the concern person using GSM technology, and the results will be displayed in the LCD.

5. Conclusion

This paper will provide an effective and safest way of cash transaction in Automated Teller Machine and Cash Deposit Machine. Using holographic keypad, the tracking and identification of pin number by unknown person will be detected and the malfunction information is reported to the account holder and bank authority using GSM Technology. The prototype model is constructed and the finger print information results are obtained. In this experiment, using sixth sense technology the complexity of problems related to pin tracing is reduced. In the next fragment we were planned to prevent the Automated Teller Machine from physical theft.

References

[1] Bradbury D, "Why we need better ATM security", *Engineering & Technology*, Vol.11, No.1, (2016), pp.32–35.

[2] Mandal R & Choudhury N, "Automatic video surveillance for theft detection in ATM machines: An enhanced approach", *3rd International Conference on Computing for Sustainable Global Development*, (2016), pp.2821–2826.

[3] Kumaresan S, Dinesh Kumar G & Radhika S, "Design of secured ATM by wireless password transfer and shuffling keypad", *International Conference on Innovations in Information, Embedded and Communication Systems*, (2015), pp.1-4.

[4] Raj MME & Julian A, "Design and implementation of anti-theft ATM machine using embedded systems", *International Conference on Circuits, Power and Computing Technologies*, (2015), pp.1-5.

[5] Giroux N, "A tutorial on ATM traffic management", *Canadian Journal of Electrical and Computer Engineering*, Vol.21, No.3, (1996), pp.103-106.

[6] Petrlic R & Sorge C, "Establishing user trust in automated teller machine integrity", *IET Information Security*, Vol.8, No.2, (2013), pp.132-139.