International Journal of Current Engineering and Technology
E-ISSN 2277 – 4106, P-ISSN 2347 - 5161

Available at http://inpressco.com/category/ijcet

Research Article

Implementation of a Framework for Securing ATMs using Digital Image Processing

Kande Archana[Á*], P.Bhaksara Reddy[B], M. Yashwanth[Á] and D. Neelesh Varma[Á]

[Á]Department of Computer Science & Engineering, MLR Institute of Technology, JNTU Hyderabad, India
[B]Department of ECE, MLR Institute of Technology, JNTU Hyderabad, India

Accepted 30 Nov 2014, Available online 01 Dec 2014, **Vol.4, No.6 (Dec 2014)**

Abstract

Due to technological innovations in the banking domain, ATMs came into existence which facilitates customers to avail money round the clock. Moreover, the ATM network of one bank collaborates with other banks so as to enable customers to draw money from any bank's ATM. As ATMs are equipped with money there is possibility of robberies. In fact there were many such incidents reported. This paper proposes a framework which will provide high security in ATMs. The framework includes a PIR sensor, camera, processor, and microcontroller. When a person enters into ATM cabin, the PIR sensor can detect it. Then camera starts capturing video which is analyzed by a processor. The processor is capable of identifying abnormal incidents. When processor reports an unusual incident, the microcontroller causes the ATM door to be closed automatically. It also sends SMS alert to police station. The person who misbehaved in ATM is caught inside. Thus the proposed framework provides high security to ATMs. The experimental results revealed that the framework can provide high security to ATMs.

Keywords: *Microcontroller, PIR Sensor, Processor, Camera.*

Introduction

Banking sector plays a pivotal role a country's economy. One of its services is dispensing money through Automated Teller Machines (ATMs). As ATMs operate round the clock and interoperability with other banks, thanks to distributed computing, they get rid of time and geographical restrictions for monetary transactions. Moreover they are supporting a host of other services such as money transfer besides withdrawal of money. This led to ubiquitous usage of these wonderful machines across the globe. There have been plenty of ATM fraud cases reported in all counties where ATMs are operated. Security of Automated Teller Machine (ATM) is to be given paramount importance as financial institutions like banks heavily depend on them for facilitating monetary transactions. The term security refers to many aspects such as physical, transactional and integrity, customer identity integrity, device operation integrity, and customer security. Various attempts have been made in developed countries to have emergency PIN system but could not succeed due to lack of cooperation between banking lobby and police. With technological advances in ATM software, fraud cases are significantly reduced unless PIN is compromised. Though there is transactional security improved to the level of reliability, the misbehaving cases are alarming.

Human misbehavior with respect to ATM with the motive of stealing money of other human beings or banks include forced withdrawal, stealing entire ATM, breaking ATM machine using gas or explosive or other means to avail cash illegally, digging a concealed tunnel under ATM, targeting women and forcing them to withdraw money and hand over to criminal, attaching fake keypads to ATM for obtaining PINs, getting ATM cards and PINs forcibly from other customers in ATM cabin and so on. There is little research found in the literature towards an automatic misbehavior detection and notification systems. In this context there is inevitable and indispensable need for a highly secure ATM cabin that can safeguard interests of customers and banks. However, it is very challenging problem to be addressed. In this research work, a novel framework is proposed to be designed and implemented for securing ATMs using digital image processing. The framework makes use of inter-disciplinary devices and services in order to build a fool proof security system for ATMs. The focus of the research is to protect ATM security by studying human actions that enter ATM cabin and making necessary steps when misbehavior is reported. However, defining misbehavior patterns and training the proposed system with such know how is NP-hard. This research is intended to achieve this and help customers of banking sector to avail ATM services in safe and secure environment. As this has high significance and real world implications across the globe and can influence human lives of the entire planet, it is the motivation behind taking up this research work.

*Corresponding author **Kande Archana** is working as Assistant Professor; **Dr.P.Bhaksara Reddy** as Director Cum Principal; **M. Yashwanth** and **D. Neelesh Varma** are students

Objectives

The aim of the thesis is to design and implement a fool proof system that secures ATMs using digital image processing. It automatically identifies misbehaving humans who entered into ATM cabin and take necessary steps in such a way that the criminal who tries to misbehave is caught and brought to justice besides safeguarding interests of bankers and customers. To achieve the aim of the research, the following SMART objectives are conceived.

- To investigate human misbehavior patterns in ATM cabin for training the proposed system.
- To investigate inter-disciplinary techniques or mechanisms that contributes to the fully functional secure ATM system.
- To design and implement a framework for securing ATMs using digital image processing.
- To integrate the system with police for quick response and action.
- To test the system against all the human misbehavior patterns.
- To evaluate the system with respect to consequences and possible misconceptions from the two departments such as banking and police.
- To review and write thesis report.

These objectives help in achieving various milestones in the process of achieving research aim. They also provide a step by step flow of actions that govern the final output of the research.

Literature Review

Literature is in abundance on ATM related theft and other issues. There are many cases of ATM fraud. In other words ATM security might be physical or other. Mohammed (2011) investigated ATM fraud type such as skimming, card trapping etc. and proposed solutions. Shaikh and Shaw (2012) investigated bugs in ATM controller and bestowed fraud prevention measures. Nicholas (n.d) presented various means in which fraudsters manage uncaught. White Papar (n.d) on ATM fraud reveal that there are many fraudulent activities such as card and currency fraud, skimming, fishing, transaction reversal, data attacks, and physical attacks. Another white paper (2002) explored the ATM frauds such as card theft and skimming besides prevention measures such as surveillance, consumer education, and remote monitoring. Tedder (2009) explored cost of ATM frauds and the trends in making fraud. Litan (2005) explored the ways and means in which criminals explore consumer bank ATMs' vulnerabilities. The survey reveals that the ATM fraud cases are changing from time to time. Awodele and Akanni (2012) explored human biometric features to avoid ATM fraud cases. Adeoti (2011) investigated ATM frauds and the annual growth rate of the incidents. Michael Levi, Paul Bissell and Tony Richardson (1991) studied the prevention of cheque and credit card frauds. They provided prevention measures for collusive fraud, counterfeiting, and card misuse. Mohamad (2011) explored plastic card fraud. Dbresearch (2014) presented fraud value as a growing problem. Jog and Pardesi (2014) presented Hidden Markov Model (HMM) for monitoring ATM payments and detect fraud. Ramki (n.d) provides an account of biggest ATM heist. Bond *et al*. (2012) explored pre-play attack and cloning. Pratiksha *et al*. studied the problem of using multiple cryptographic algorithms in order to prevent ATM frauds. A common thread in all the researches in the past include that they focused on transaction security and other frauds while little research is found on the misbehavior of humans in ATM cabin.

Methodology

The methodology for designing and implementing a framework for securing ATMs using digital image processing is described here. It starts with further review of literature that provides insights into the human misbehaving patterns inside ATM cabin. Afterwards, datasets are obtained from Internet sources or synthesized to sync with the insights from review of literature. Inter-disciplinary requirements are analyzed as they are involved in coordinated effort to push the solution towards convergence. A security model and threat model are prepared keeping the aim of the research in mind. The threat model encapsulates misbehaving users in ATM cabin. The methodology is broadly presented in Figure 1.

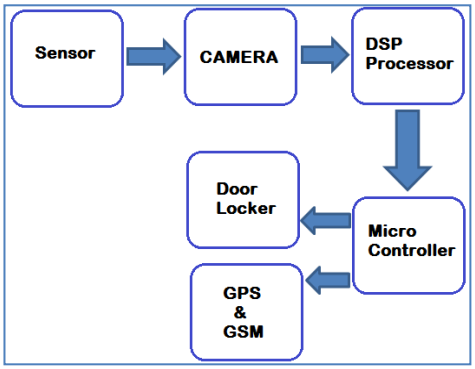

Figure 1 Run time flow of the proposed system

As can be seen in Figure 1, it is evident that the sensor is able to capture human presence in ATM and lets camera to be active and capture the live video for surveillance purposes. Afterwards, the captured video frames are analyzed by the DSP processor which is responsible to detect abnormal behavior and inform the micro controller to take necessary actions. The micro controller performs two jobs namely locking the door and informing concerned authority and using GPS and GSM for knowing position of the target ATM. The digital signals provided by micro controller are converted to mechanical force for locking the door. As the door is locked, the probable thief inside the ATM cabin can't come out of it. He gets caught red handed and thus the robbery of ATM is effectively avoided.

Expected Deliverables

There are many expected deliverables from this research work. They include literature review insights, proposed

design and implementation, devices used for inter-disciplinary communication, thesis analysis and design, code implementation, requirements specification, coding, testing, evaluation of results and possible future work. The main deliverable is the prototype that has miniature features of a real world system. The prototype is partly software and partly hardware. The prototype can be used to know how the human misbehaving in ATM cabin. The deliverables when used effectively secure ATM functionality is ensured. The solutions expected comprise of computer programs, micro controller, camera, DSP processor and door locker. GPS & GSM are the technologies used to ascertain the location and inform the event to police for quick response. Besides these deliverables, the proposed application needs to deliver user's manual, installation manual and troubleshooting FAQ.

As the solution makes use of multiple disciplines, the deliverables are given as conceived by methodology. Along with the software product, some of the hardware components such as camera, sensor, DSP processor, microcontroller and door locker are essential to test the efficiency of the proposed system. Human misbehavior patterns are also part of the deliverables.

Significance of the Expected Outcomes

The expected outcome provided in the thesis work, is very significant as they prove the successful implementation of the system to secure ATMs. Human misbehavior patterns can help in formalizing the scenarios that can provide insights into the misbehavior that causes the equipment to perform the detection and notify police to take necessary action. The expected prototype application can assume significance as it can bestow the following advantages or implications of the research in the real world.

- When ATM fraud case occurs with respect to the misbehavior or abnormal behavior, it is evident that the application has potential impact on the society at large.
- The proposed system can protect ATMs form banking sector besides encouraging customers to have safe and secure communications.
- The technology innovations can be utilized as the proposed system is modular in nature. This way the proposed system can have well defined requirements.
- The proposed application when used by banks it is possible that they can protect all ATMs of the bank. This can lead to much more secure environment to boost the economy as more and more customers will be using the ATM.
- The application has the provision to include communication to law enforcing agencies like police.

Conclusion

In this paper we presented a framework which provides integrated security that ensure can avoid ATM robberies. The framework functionality starts as soon as a warm object such as human being enters into ATM cabin. First of all a sensor senses the fact that the room environment is changed. Then the sensor sends signals to camera which starts capturing live video. The video is divided into frames and the frames are processed by digital image processor. When it encounters any abnormal behavior that differs from normal behavior beyond given threshold, it sends signals to micro controller. The microcontroller communicates digital signals to door locker that gets converted to mechanical force that causes the door to be locked automatically. At the same time the micro controller is programmed to send SMS to nearest police station through GPS & GSM technologies. The suspect is within the walls of ATM and can't come out. Thus is he is caught rend handed and the ATM robbery is effectively thwarted.

References

Lawan Ahmed Mohammed. (2011). Use of biometrics to tackle ATM fraud. *IACSIT*. p331-335.

Aijaz Ahmed Shaikh & Syed Mir Muhammad Shah1. (2012). Auto Teller Machine (ATM) Fraud – Case Study of a Commercial Bank in Pakistan.*International Journal of Business and Management*. 7 (22), p100-108.

Ted Nicholas. (n.d). ATM Fraud. *CFS*. p1-20.

White Paper (n.d). ATM Fraud and Security. *DIEBOLD*. p1-8.

White Paper. (2002). ATM Fraud And Security. *DIEBOLD*. p1-10.

Krista Tedder. (2009). Now You See It, Now You Don't: A Review of Fraud Costs and Trends. *A First Data White Paper*. p1-15.

Avivah Litan. (205). Criminals Exploit Consumer Bank Account and ATM System Weaknesses. *Gartner*. p1-5.

Oludele Awodele and Adeniyi Akanni. (2012). Combating Automated Teller Machine Frauds through Biometrics. *IJEATE*. 2 (11), p441-444.

Johnson Olabode Adeoti. (2011). Automated Teller Machine (ATM) Frauds in Nigeria: The Way Out. *IEEE*. p53-58.

Michael Levi, Paul Bissell and Tony Richardson. (1991). The prevention of cheque and credit card fraud. *Crime prevention unit paper*. p1-57.

Hanna Mohamad. (2011). Background Paper: Plastic Card Fraud.*NSW Government*. p1-15.

Deutsche Bank. (2014). Card fraud: A growing problem?. *Deutsche Bank Research*. 0 (0), p1-3.

Vivek V. Jog and Nilesh R. Pardeshi. (2014). Advanced Security Model for Detecting Frauds in ATM Transaction. *International Journal of Computer Applications*. 95 (15), p1-4.

Ramki. (n.d). The greatest ATM heist in history. *ATM Fraud*. p1-12.

Mike Bond, Omar Choudary, Steven J. Murdoch, Sergei Skorobogatov, and Ross Anderson. (2012). Chip and Skim: cloning EMV cards with the pre-play attack. *University of Cambridge*. p1-21

Pratiksha L. Meshram, Prof. Tarun Yenganti. (2013). Credit and ATM Card Fraud Prevention Using Multiple Cryptographic Algorithm.*IJARCSSE*. 3 (8), p1300-1305.

Authors Profiles

Kande Archana completed M.Tech in Computer Science at Jawaharlal Nehru Technological University Hyderabad. She has 8 Yrs, experience in teaching. Presently working in MLR Institute of Technology, Hyderabad as an Assistant Professor in Department of Computer Science and Engineering. Her specialized area is Network security and Image processing. She published 8

papers in that area, 7 are International Journals and one International Conference).

Dr. P. Bhaskara Reddy, B.E.(ECE), M.Tech., Ph.D., F.I.S.E.E., MCSI, MISTE, the Director MLR Institute of Technology is a young and dynamic professor of ECE, has 26 years of Teaching, Research and Administrative experience in Reputed Engineering Colleges and Industry. Recipient of Bharath Jyothi award in 2003 and Rastraprathiba award in 2004, Knowledge Award from Alumni of SVHCE for the year 2001, Published 1 Book (International Edition) "Information Technology in Technical Education – Economic Development by "LAMBERT Academic Publishing", Published 9 Laboratory Manuals, 65 Research papers at National and International Level on Education, Electronics Communication, I.T, Computer Networks, E-Commerce etc. Guided 5 Research Scholars for their Doctorates, about 50 M.Tech., M.C.A. and B.Tech projects and Conducted 10 National Level Technical Symposiums on various topics in Electronics & Communications, Computers etc.

M. Yashwanth Tejacurrently pursuing his B.Tech final year in Computer Science & Engineering, MLR Institute of Technology, Dundigal, Hyderabad. His current research interests include Network Security and Information Security, Computer Networks.

Dhanalakota Neelesh Varma, is Studying B.Tech, III year I sem at MLR Institute of Technology in the Department of computer science and Engineering at Dundigal Hyderabad. He is interested in field of Android, CyberNet Security.