International Journal of Soft Computing 12 (4): 224-227, 2017
ISSN: 1816-9503

A Novel Security for ATM by Using GPS and GSM Technologies with Image Processing

[1]Kande Archana, [1]Bhaskara Reddy and [2]A. Govardhan
[1]Department of CSE, MLR Institute of Technology, Hyderabad, India
[2]Department of CSE, JNTU School of Information Technology (SIT), Hyderabad, India

Abstract: In present, ATM environments technological innovations in the banking domain. ATMs are equipped with money there is possibility of robberies. This study proposes a framework which will provide high security in ATMs. The prototype includes a PIR sensor, camera, processor and microcontroller. When a person enters into ATM cabin, the PIR sensor can observe the human motion. Then, camera starts capturing video and sends to DSP processor, DSP processor analyzed based on human motion. The DSP processor is capable of identifying either normal or abnormal incidents. In case abnormal incident, then DSP processor reports to microcontroller, the microcontroller perform two functions, one is the ATM door will be closed automatically, then the person will be locked in the room, in the next second SMS and MMS are send to nearest police station and concerned bank through GSM and GPS modems. By this system, robberies will be stopped and the complaints cases also reduced maximally. Thus, the proposed framework results are revealed that the framework can provide high security to ATMs.

Key words: GSM, ATMs, MMS, GPS, GSM

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. 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.

Need for the study: 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. 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. 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.

Objectives of the study: The aim of the thesis is to design and implement a fool proof system that secures ATMs

Corresponding Author: Kande Archana, Department of CSE, MLR Institute of Technology, Hyderabad, India

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.

Hypotheses: From the initial review of literature the following hypotheses are conceived:

- ATM security can be enhanced further by investigating inter-disciplinary features or techniques through digital image processing
- A framework can be built to protect ATMs from human misbehavior and integrate the system with police for immediate action

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 study in 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 explored the ways and means in which criminals explore consumer bank ATM's 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. Levi *et al.* (1991) studied the prevention of cheque and credit card frauds. They provided prevention measures for collusive fraud, counterfeiting and card misuse. Hanna (2011) explored plastic card fraud. Dbresearch presented fraud value as a growing problem. Jog and Pardeshi (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 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.

MATERIALS AND METHODS

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 Fig. 1.

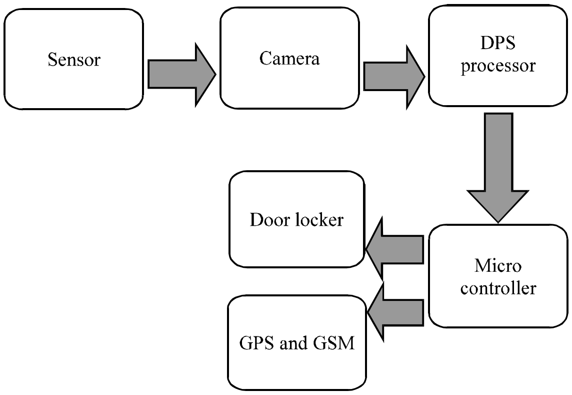

Fig. 1: Illustrates the run time flow of the proposed system

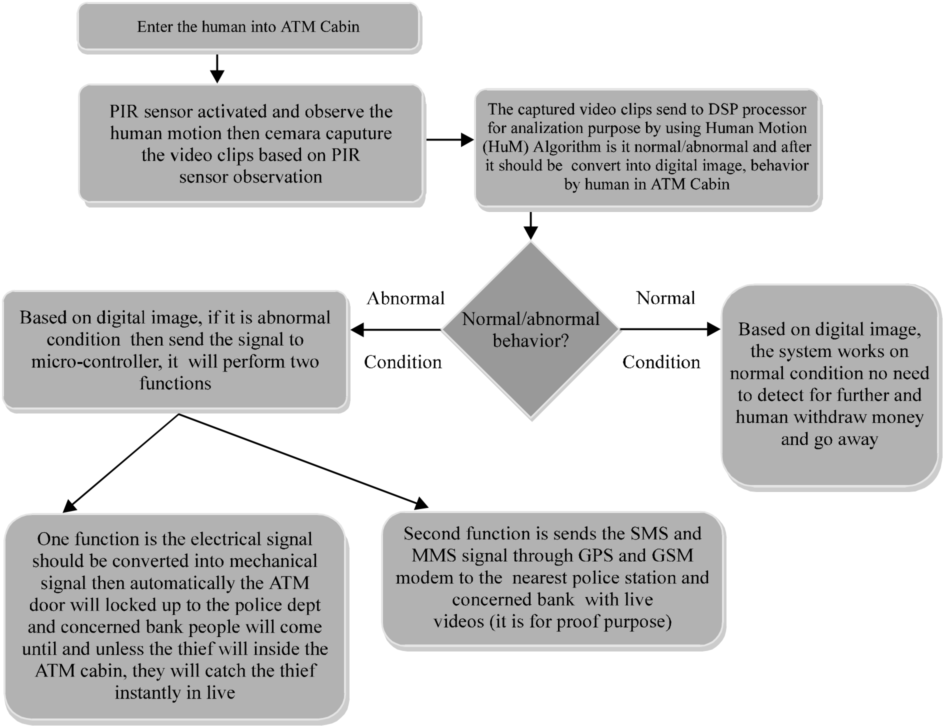
Enter the human into ATM Cabin
PIR sensor activated and observe the human motion then cemara caputure the video clips based on PIR sensor observation
The captured video clips send to DSP processor for analization purpose by using Human Motion (HuM) Algorithm is it normal/abnormal and after it should be convert into digital image, behavior by human in ATM Cabin
Normal/abnormal behavior?
Abnormal
Condition
Normal
Condition
Based on digital image, if it is abnormal condition then send the signal to micro-controller, it will perform two functions
Based on digital image, the system works on normal condition no need to detect for further and human withdraw money and go away
One function is the electrical signal should be converted into mechanical signal then automatically the ATM door will locked up to the police dept and concerned bank people will come until and unless the thief will inside the ATM cabin, they will catch the thief instantly in live
Second function is sends the SMS and MMS signal through GPS and GSM modem to the nearest police station and concerned bank with live videos (it is for proof purpose)

Fig. 2: Proposed system overview

As can be seen in Fig. 2, 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.

RESULTS AND DISCUSSION

Scope of the study: The scope of the study encompasses 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 and 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.

CONCLUSION

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.

IMPLICATIONS

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 misbehavioror 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

REFERENCES

Adeoti, J.O., 2011. Automated Teller Machine (ATM) frauds in Nigeria: The way out. J. Soc. Sci., 27: 53-58.

Awodele, O. and A. Akanni, 2012. Combating automated teller machine frauds through biometrics. Intl. J. Emerging Technol. Adv. Eng., 2: 441-444.

Bond, M., C. Omar, J.M. Steven, S. Sergei and A. Ross, 2012. Chip and skim: Cloning EMV cards with the pre-play attack. Finextra, London, England. https://www.finextra.com/blogposting/6920/chip-and-skim-cloning-emv-cards-with-the-pre-play-attack.

Hanna, M., 2011. Background paper: Plastic card fraud. New South Wales Government, New South Wales, Australian.

Jog, V.V. and N.R. Pardeshi, 2014. Advanced security model for detecting frauds in ATM transaction. Intl. J. Comput. Appl., 95: 47-47.

Levi, M., P. Bissell and T. Richardson, 1991. The Prevention of Cheque and Credit Card Fraud. Crime Prevention Unit Paper, London, England, ISBN:0-86252-633-7, Pages: 57.

Shaikh, A.A. and S.M.M. Shah, 2012. Auto Teller Machine (ATM) fraud case study of a commercial bank in Pakistan. Intl. J. Bus. Manage., 7: 100-108.

Tedder, K., 2009. Now you see it, Now you don't: A review of fraud costs and trends. First Data, Atlanta,Georgia. https://www.firstdata.com/en_ie/insights/fraud-costs-and-trends-.html.