Smart ATM - Reactive Measures against Physical Threats

Kaushal Meher
PG Scholar, Dept. Information Technology,
K. J. Somaiya College of Engineering, Vidyavihar, Mumbai 77

Ashwini Dalvi
Asst. professor, Dept. Information Technology,
K. J. Somaiya College of Engineering, Vidyavihar, Mumbai 77

Abstract- Automated Teller Machines (ATMs) security is the area of study that aims to find vulnerability in the system to protect physical theft from ATM machines. ATM frauds have been increased across the globe at an alarming rate. ATM risk and incidence management is necessary to reduce ATM crimes. ATM security problem has come up with a solution by using some internal functionality of ATM to secure ATM Machines. ATM Machine error codes can be used to alert Law enforcement agencies if any malicious activity has been carried out with ATM. It includes GUI maps system, SMS alerts and real time video surveillance. Companies working in ATM Maintenance industry have significant importance in building new secure ATM. Their existing infrastructure is useful to built reactive secure system. This paper proposes a system to develop a secure ATM in future.

Keywords – Automated Teller Machines, Security, Operators, Google Maps, Error codes, ATM Maintenance

I. INTRODUCTION

An automated teller machine (ATM) is a device that facilitates basic banking activities like withdrawal of money, checking balances etc so no need for an individual to visit bank. Currently, ATMs are protected by a combination of physical token, typically a magnetic card, and certain secret knowledge, e.g., personal identification numbers (PINs). Criminals now employ different ways to hunt for user's PIN. Current measures adopted by financial institutions are purely informative and do not sufficiently deal with the issues in real life scenario.Some of the measures list ATM card holders to optionally subscribe to financial transactions message alerts through Short Message Services (SMS) (debit and credit transactions) and the use of posters pasted in banking halls to warn customers on the need to protect PIN numbers from unauthorized users.

The Indian ATM Industry has witnessed huge growth in the past decade. An ATM is a part of more complex distributed system composed by various actors (ATM, Bank, and managing authorities) that communicates exchanging messages. ATM maintenance companies offer a complete set of software & services for ATM Management to help the banks and hosted ATM service providers maximize their ATM availability and offer targeted solutions to their ATM customers. The services include Site maintenance and management, Maintenance of all equipment like CCTV etc., ATM Installation and logistics services, ATM Incident Management services.

There has been increase in ATM frauds all over the world. It has been discussed in different literatures. **[3]**In India, Thane man loses Rs. 40000 from ATM as he forgot to cancel his transaction. In another case Andheri resident loses Rs 170,000 in skimming fraud along with three others. Delhi Police's Crime Branch has arrested two persons for allegedly blocking the cash dispenser of an ATM outlet after withdrawing cash, prompting it to generate an error message, on the basis of which they claimed the same amount again from the bank. **[5]**

All these incidences show that hackers are well aware of ATM working and inside of system. Even something as simple as a cash jam in an ATM can lead to a security issue. It may result in revenue loss and budget erosion. So security of ATM is an important issue to be addressed.

II. BACKGROUND WORK

There are many ATM Maintenance companies like CMS, DIEBOLD, and NCR which manages ATM network operations. Its Incident Management System provides event monitoring and calls management of ATM Infrastructure. **[4]**

2.1 Working of ATM Maintenance companies

2.1.1 ATM Machine → Error → Text File → Operator

- There are two types of errors, functional and security. These two types of error codes are as follows:

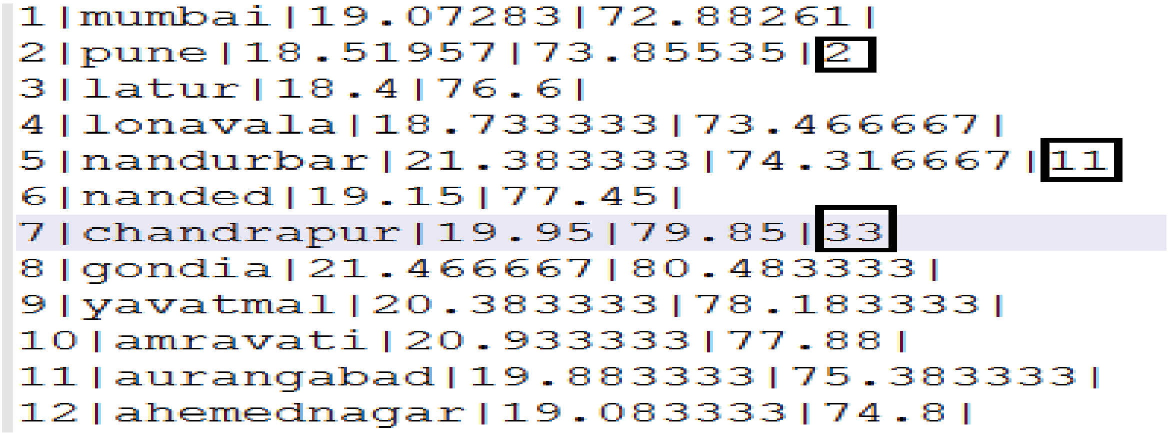
Functional error codes:

- 1 – Timed out
- 2 – hardware error
- 4- Error in modem data
- 11- No connect
- 33- Feed failure

Security error Codes:

- 37 - Too long at exit
- 38 - Blocked exit
- 49- Jam at exit
- 51 - Suspect exit accountancy
- 101 - Dispenser error
- 144 – Security module not responding
- 145 – Security module bad
- 166 – Bad dispenser
- 190 – Master key not configured.
- 565 - Cabinet door open
- 566 - Vault Door Open
- 568 - Security module com failed
- 577 - Card reader disabled

Current system addresses only functional errors. If any functional error generated, it is sent to the operator in text file. Then operator has to manually go through text file and needs to identify the issue by analyzing codes as shown in fig 1.



```
1|mumbai|19.07283|72.88261|
2|pune|18.51957|73.85535|2
3|latur|18.4|76.6|
4|lonavala|18.733333|73.466667|
5|nandurbar|21.383333|74.316667|11
6|nanded|19.15|77.45|
7|chandrapur|19.95|79.85|33
8|gondia|21.466667|80.483333|
9|yavatmal|20.383333|78.183333|
10|amravati|20.933333|77.88|
11|aurangabad|19.883333|75.383333|
12|ahemednagar|19.083333|74.8|
```

Fig 1: Text file with functional codes

2.1.2 Operator → Telephonic communication → Custodian

- Operator then calls custodian and explains error type and which machine custodian has to attend. It may contain delay due to network problem as in custodian might be out of coverage area.

2.1.3 Custodian → Fix Issue

- Custodian then visits the malfunction sight and fixes the issue. This whole process is very tedious.

Existing system mainly looks for functionality of ATM. It doesn't look into security aspect of it. Even system doesn't have any kind of GUI and communication is mainly telephonic.

2.2 Solutions discussed to address ATM security

Literature work on this topic discuss about securing ATM using embedded systems **[1]**. Technologies like RFID; Raspberry PI has been discussed in this paper. ATM security, comprising of the modules namely, authentication lock, web enabled control and sensors. Another work suggests SMS based scheme to be used while money withdraw **[2]**. It suggests that some on the fly scheme should be adopted to make ATM more secure.

III. PROPOSED SYSTEM

The main objective of proposed system is to develop a secure ATM with features like

Feature 1 - Threat identification using secure error codes

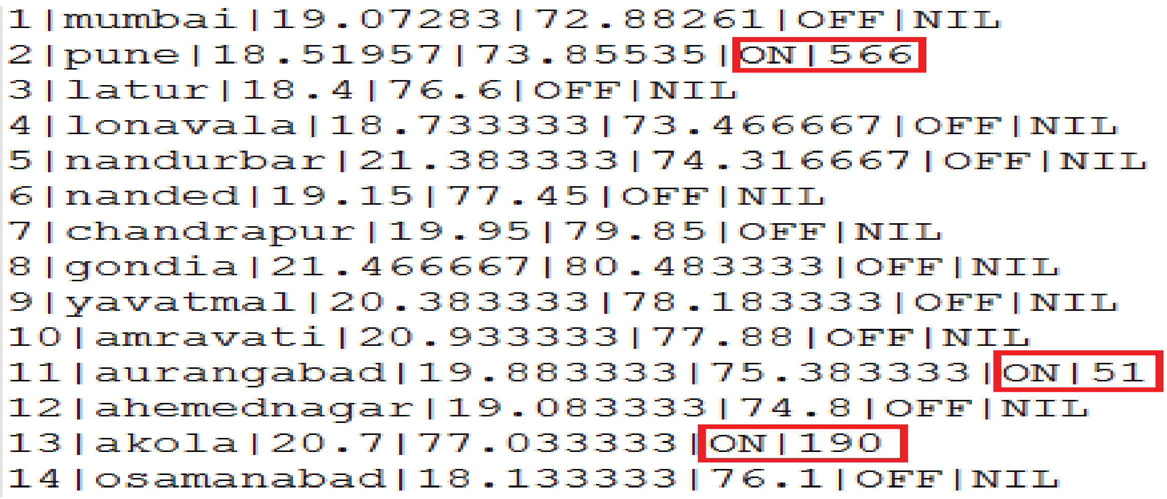
Feature 2 - GUI based remote monitoring system

Feature 3 - Real time video surveillance

The above features are discussed as follows:

Feature 1 - Threat identification using secure error codes

Using a set of predefined security codes, new system can correlates different events at a bank's ATMs to determine whether there is a security threat. For example, if the branch lobby door opens system identifies someone approaching the ATM, yet no transaction takes place within a given period of time, system may determine that a skimming device is being attached. It will then trigger an alarm at the bank's security centres. ATM maintenance companies can receive any of this error if occurred along with their regular maintenance file. If system receives any of error alerts, SMS can be sent to ATM guard. So he can look into the matter at the time of crime itself. As soon as alert is generated SMS would be send to guard.



```
1|mumbai|19.07283|72.88261|OFF|NIL
2|pune|18.51957|73.85535|ON|566
3|latur|18.4|76.6|OFF|NIL
4|lonavala|18.733333|73.466667|OFF|NIL
5|nandurbar|21.383333|74.316667|OFF|NIL
6|nanded|19.15|77.45|OFF|NIL
7|chandrapur|19.95|79.85|OFF|NIL
8|gondia|21.466667|80.483333|OFF|NIL
9|yavatmal|20.383333|78.183333|OFF|NIL
10|amravati|20.933333|77.88|OFF|NIL
11|aurangabad|19.883333|75.383333|ON|51
12|ahemednagar|19.083333|74.8|OFF|NIL
13|akola|20.7|77.033333|ON|190
14|osamanabad|18.133333|76.1|OFF|NIL
```

Fig 2: Text file with security codes

In above fig, security error codes are included in text file. Also ON/OFF flags are added.

Feature 2 - GUI based remote monitoring system

GUI with Google maps can be add-on to proposed system. As discussed earlier sites that have been compromised would send error in file. With help of XML this codes can be placed on Google maps to show the threat. ON/OFF flags included in text file as shown in Fig. 2 can be used to distinguish compromised ATMs than normal ones. If flag is ON, Respective ATM is highlighted with red colour and vice versa.

Graphical red alert notification would be helpful for operators as they need not have to analyze entire text file. Just with the click on marker they can see the error code or further the exact issue.

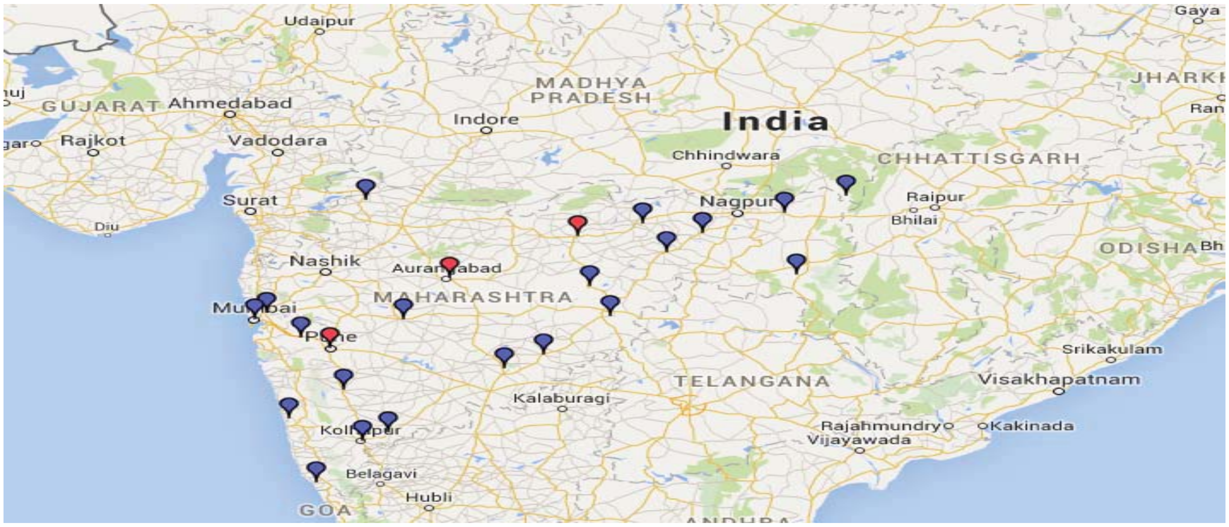


Fig 3: GUI integration

In above Fig Red marker indicates that some issue has occurred at those sites. While blue marker shows that those sites are working fine. If maintenance file contains any security error code in it, respective error code is updated in database. And then it is reflected on map with red colour.

Feature 3 – Real Time Video Surveillance

Video surveillance can also be useful for real time ATM monitoring. If any of above ATM error generates, live video feed for compromised ATM can be send to operator. So that he can guide security guard about inside situation. Also these feeds can be directly available for law and enforcement agencies. There is no need to run video forward or backward.

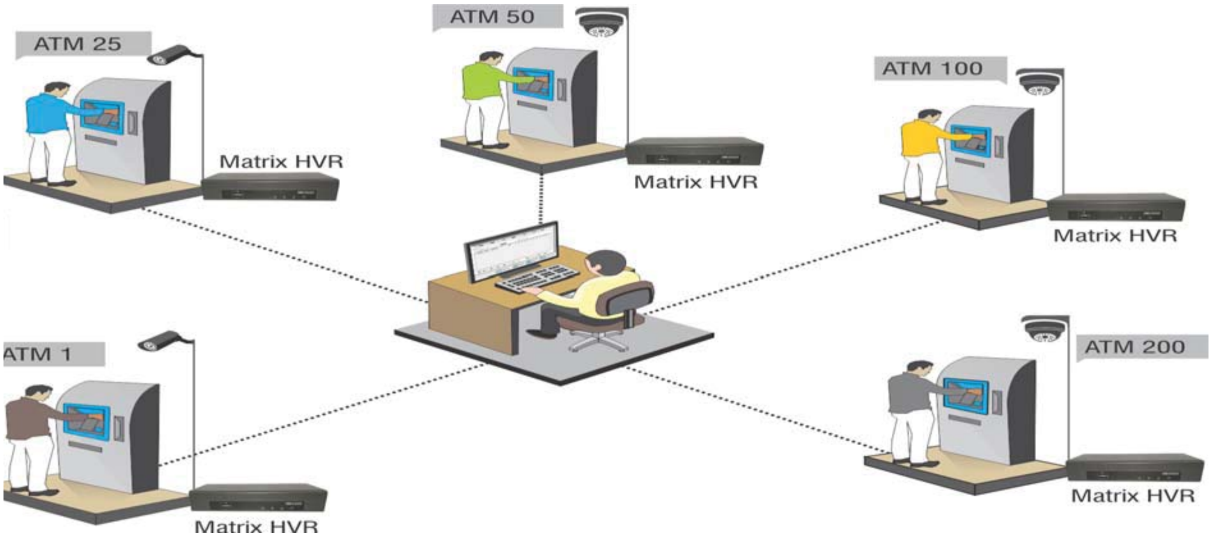


Fig 4: Real time ATM video monitoring

The remote real time video surveillance is nice security option, because ATMs at the time of incidence can be directly monitored from a single, central location.

Proposed smart ATM system has advantages in many aspects. Firstly, unlike current system it looks mainly for security aspect. With help of interactive GUI, operators work can become very convenient. Also the system is configured to work in real time to solve the problem on the fly. With the use of open source facility solution is also cost effective.

IV. CONCLUSION

The proposed work implements an efficient way in which ATM can be monitored so that security could be enhanced. Emphasis is on reactive measures so that law enforcement agencies can get their hands on fraudsters. Geographic based system, SMS alert and real time video monitoring based on ATM error alert is crucial to change traditional way of ATM monitoring. Cost effective solutions and real time implementation can keep ATM safe from theft and fraudsters.

REFERENCES

[1] Raj M, Anitha Julian, “Design and Implementation of Anti-theft ATM Machine using embedded systems”, 2015 International Conferences on Circuit, Power and Computing Technologies [ICCPCT].

[2] Ugochukwu Onwudebelu, Olumide Longe, Sanjo Fasola, Ndidi C. Obi and Olumuyiwa B. Alaba, “Real time SMS-based Hashing Scheme for Securing Financial Transactions on ATM Systems” 3rd IEEE International conference on adaptive science and technology (ICAST 2011).

[3] Solomon A. Adepoju,” Challenges of Automated Teller Machine (ATM) Usage and Fraud Occurrences in Nigeria– A Case Study of Selected Banks in Minna Metropolis “, JIBC August 2010, Vol.15, No. 2.

[4] Diebold, “ATM Fraud and Security”.

[5] www.ndtv.com/india-news