Available online at www.elixirpublishers.com (Elixir International Journal)

Information Technology

Elixir Inform. Tech. 85 (2015) 34261-34265

ISSN: 2229-712X

# Zero Wire Authentication System in ATMs Using GSM Technology

Kranti Narayan Gule[1], Rohit N. Devikar[1] and Tushar Ramesh Satpute[2]
[1]Department of IT, Amrutvahini College of Engineering, Sangamner, India.
[2]MIP Politechnico di Milano, Milan, Italy.

**ARTICLE INFO**

**Article history:**
Received: 30 June 2015;
Received in revised form:
1 August 2015;
Accepted: 5 August 2015;

**Keywords**
Security,
PIN Entry,
Mobile Devices,
ATMs,
Authentication.

**ABSTRACT**
Due to public location and permanent availability multiple people depends on the automated teller machine (ATM). Due to that they can easily fall victim to manipulation. Frauds and security attacks based on observation by person or via various cameras also get increased. So, new methods for authentication mechanisms get developed to reduce the ATM security problems related to personal identification numbers (PIN). The user's mobile phones play a central role in the trust establishment. Shift PIN entry away from possibly insecure ATMs PIN pad towards the user's mobile phones & then transmit it securely for authentication. Dual tone modulated frequency (DTMF) plays a major role in this technique.



## Introduction

Nowadays in human life Public terminals provide high level of convenience that many people would not like to miss. Whole 24 hours and 7 days in a week services can be accessed easily. No longer bound to opening or working times for customer. There are various public terminals or machines include like train ticket vending machines, check-in terminals at airports, cash machines (ATMs). To make use of these services, customers require authenticating to the given system [2].

In various countries large fraud happened in the year 2009. The particular of this case was the course of action taken by the defrauders to attack ATMs at large scale they employed a software integrity violation. Also there are some known software manipulations of ATMs targeted at stealing money, this is the first case that was published in which malware was set up on ATMs to grab user data. Sometimes attack was carried out by an insider who worked at the bank and who had legitimate permission to access the ATM [1].

How people can enter the personal identification numbers with the help of keypads, there are many attacks against the ATM. The way which is used by the users to protect the authentication is also important and which factors affect security and secure behavior. As online banking or ATM machines, is done in a very secure manner. Through the observation it is clear that during ATM use like phone calls, discussion with friends, or handling shopping bags are the obstacles of user. When you enter the personal identification numbers it is important to shield your hand on keypad but most of the users did not take care about that. Information technology and communication technology concepts are use to solve banking problems nowadays. E-Commerce and M-Commerce concepts have been introduced as alternatives to traditional methods.

Examples of such solutions are ATM services, credit card/debit card services [4].

## Literature Survey

An attacker is a person who illegally obtaining information from your account. The observations are performed in various cities. Those ATMs are available to users 24 hours in a day and seven days in a week. This allowed for unobtrusively observing actual ATM interactions.


**Figure 1. A typical Automated Teller Machine (ATM)**

## Various Attacks

### Attacker I

Various attacks those are carried out by the attacker also involves spying out the users PIN, for example, video surveillance, shoulder surfing or fake PIN pads come into question. This is basically the type of attacker that causes the most substantial harm for banks nowadays.

### Attacker II

A more skilled attacker is able, besides carrying out a skimming attack, to compromise a user's mobile phone as well. The goal for the attacker is to spy out the user PIN, which is now entered at his mobile phone and not at the ATM terminal which can be spied out much easier. An attacker may send a fake ATM application on his/her mobile phone. This could be done by sending the messages with a link to the download page that houses the fake application to the user. Security-enhanced authentication mechanisms divided into 2 categories.

The first includes systems that, like Mobile PIN, provide the better security against the traditional system of authentication such as password or PIN. An example of that is spy resistant keyboard Tan et al.(2005). By using standard normal keyboard

Tele:
E-mail addresses: kranti.gule@gmail.com

user can get protection against their passwords from watchful observer. But spy resistant keyboard provide better service to user. This keyboard randomizes the spatial location of all characters as each password character is entered. The Spy-Resistant Keyboard is composed of 42 Character Tiles, two Interact or Tiles, a feedback textbox, a backspace button, and an enter button.

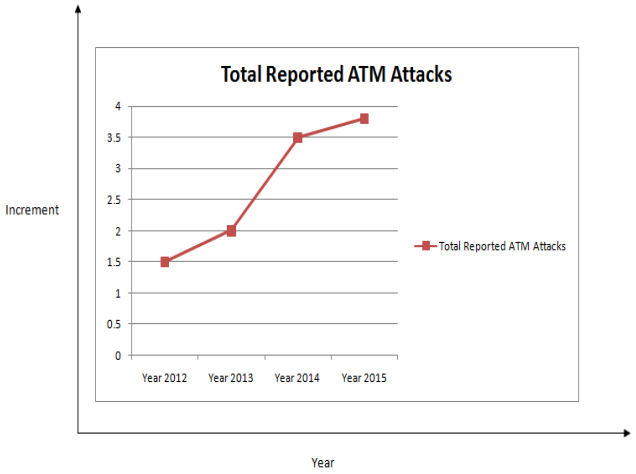


**Figure 2. ATM related attacks**

You can easily find ATMs in airports, and shopping malls, branches, convenience stores. With the prosperity of installed ATM, the reported ATM crime also has been grown. To build safe ATM use environment, maintain banks image as well as protect bank assets, all the involved organizations, institutions, and persons must research, develop & takes measures to meet the challenges faced by ATM crimes.

Related to ATM attack input entry method subject also discussed by Roth et al. (2004). An entry of PIN in ATM gives the shoulder surfing attack, for that proposed two variants of an interactive challenge-response protocol. Advantage of that it is easily won if the PIN is known, and hard to win otherwise. The cognitive capabilities of a human are generally not sufficient to derive the genuine PIN through observation of the entire games input and output.


**Figure 3. A staged example of a user that cannot hide the entry of PIN due to physical hindrance.**

Interesting research has also been performed on completely different authentication approaches. The use biometric for authentication for ATM discussed by Coventry et al. (2003). According to usability as well as speed, biometry gives performs better and which is hard to deploy and more expensive than other approaches. Biometry is that users do not have to recall any secret information like a PIN.

The machine or terminal which is used to share data or information with the consumers and increase the systems security by giving the feedback in tactile form by Deyle et al. (2006). The tactile PIN entry mechanism requires palpable actuators that can be managed by computer process. In our prototype, we use solenoids with pins that can be raised or lowered by applying an electric current to the embedded electromagnet.

## Related Work

### Shoulder Surfing Attack

When user reach to ATM center for doing transaction swapping of card is essential. If user swap card & giving PIN no.via the fix PIN pad, someone do direct observation towards the user. Or looking over one's shoulder. Observing what number that person enters onto the keyboard of device. Installed small video cameras close that PIN Pad With the help of easily obtained the number which is discretely of device. Ergonomic design means systematic design of study of the ATM to prevent shoulder surfing attack is used. In front of the ATM Fix mirror is placed. Cover the area of pin entry or shield your hand on keypad. A secure and nice environment gives customers by providing illuminated signage panels and surrounding street lights. Also keep or place ATM in high-traffic area of city [3].

**Figure 4. Shoulder Surfing Attack**

### ATM Fraud Techniques with skimming Devices

Illegally obtaining card track data the frequently used method is with skimming devices. The data which is stored on the magnetic strip. Firstly, read and then decipher information which is stored on magnetic strip. Through the small card readers which are placed on top of the actual card reader input slot work is done. Decks of cards are larger than skimming devices. Through that easily capture the account numbers, verification codes, and balances [1].

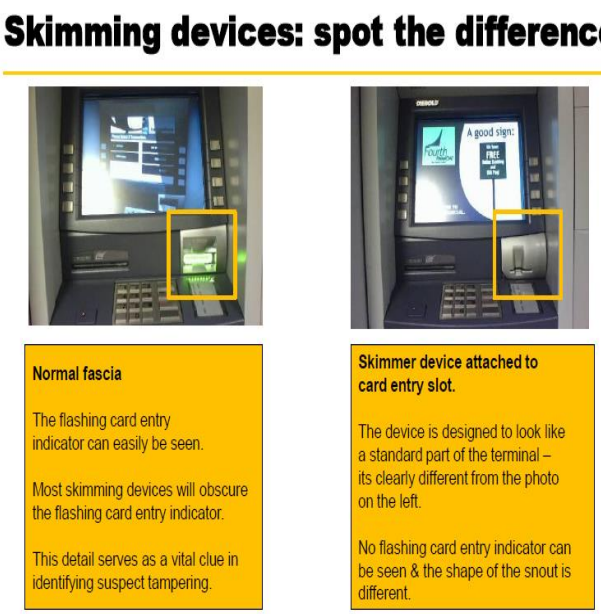


**Figure 5. Skimming Devices**

**Fake PIN Pad**

There is use of fake PIN pad which is keep over the original keypad. Firstly overlay captures the PIN data and then stores information into its own memory. After that fake pad removed. And recorded PINs are get downloaded. Those PINs are identical in the appearance and size of the original keypad. For that aware people & educate. Aware about look & feel of the ATM fascia on machines. While pay attention to the screen when enter PIN [5].

**Problems in the Existing System**

Against the cameras as well as shoulder surfers requires second hand or user other hand to shield the entry keypad. We observed several instances where users simply did not have a free hand to spare keypad. For instance, they were holding shopping bags that did not keep down. Other users were holding their mobile phone, having calls or even holding children in their arms. Four out of the six ATMs in study displayed users at such ATMs were not more likely provide protection. The remaining users that applied security measures did not hide the PIN entry, but instead checked their surrounding and verified that no one was standing nearby [10].

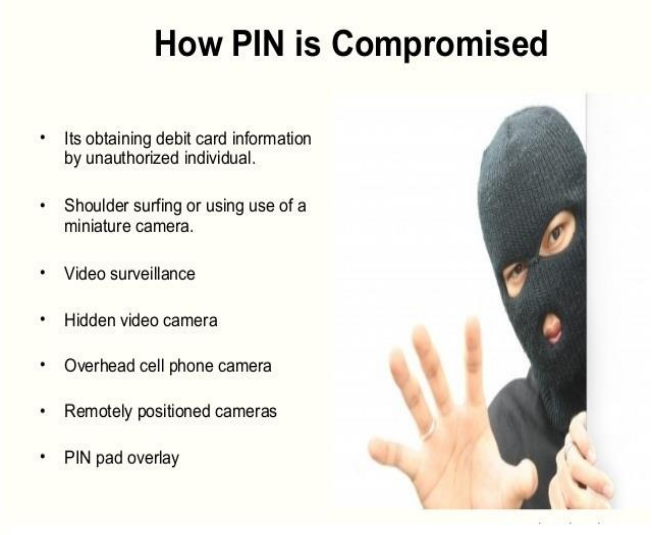


**Figure 6. How PIN is compromised**

**Proposed System**

Provide ATM machine authentication in very secure manner as well as better security to the video surveillance, shoulder surfing or fake PIN pads attack. Our system will give PIN entry via GSM is our main aim. Now a day's every individual having its own mobile phone. With the help of that make authentication more secure. Gives good balance between security and usability.

With the increase of ATM frauds, technology for new authentication mechanisms are get developed to overcome the security problems of personal identification numbers (PINs). User's mobile phones play a main role in the trust establishment & then transmit it securely for the authentication. Dual tone modulated frequency (DTMF) plays a major role in this technique. Dual tone modulated frequency is recognized from the keys press, combination of special character are recognized by DTMF IC and finally the ATM PIN is identified with very high GSM network security.

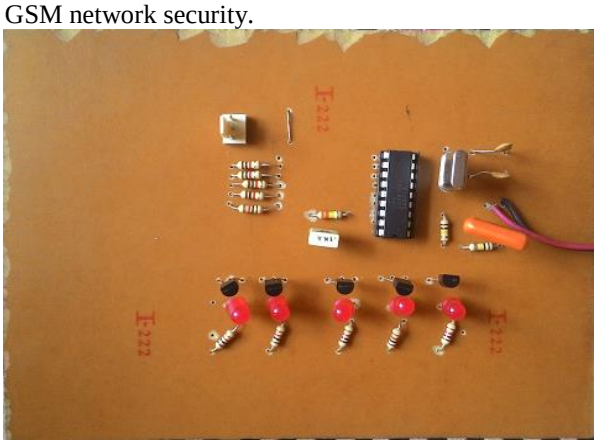

**Figure 7. DTMF board**

There is use of arduino UNO microcontroller. The microcontroller board is based on the ATmega328 IC. This is having 14 digital input/output pins, a USB connection, 6 analog inputs as well as 16 MHz ceramic resonator. The power jack & an ICSP header, reset button. For making computers that can sense and control more of the physical world than your desktop computer the arduino tool is used.

Arduino is used because it is cheap compared to other microcontroller platforms. It is runs on various platforms and provide clear programming environment. It is open source and extensible for software as well as hardware.

**Architecture**

PINs are capture or grabbed by micro cameras or by fake PIN pads nowadays in the ATMs. We have come up with a concept in this paper to solve the problem of PIN logging in an ATM by shifting the PIN entry from the potentially insecure ATM machine to the user's mobile phone.

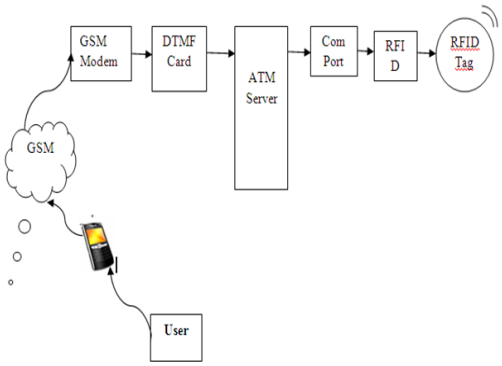


**Figure 8. Block Diagram of Secure ATM.**

**Process**

Step 1: We use Wireless sensor network (WSN) and Artificial intelligence (AI).

Step 2: User will reach the ATM and swap the card. The soon user see a message please dial a toll free number.
Step 3: Asking for to dial a toll free number. The soon user make a call and dial a password or PIN number. User can enter the PIN number with the help of his/her own mobile phone keypad.
Step 4: A GSM modem is placed at ATM with DTMF card internally connected to it.
Step 5: DTMF card receive those dialed numbers as sound signal or electrical signal. That signal is converted into binary pulse.

**Figure 9. A GSM modem connected to DTMF card.**

Step 6: Here MT8870 IC is used. For a convenience or testing the power supply is given by battery. After that the arduino microcontroller is mount and giving the power supply through the microcontroller 5Volt.
Step 7: Dial a number to the modem or simply toll free number which is connected to DTMF card.
Step 8: Once call is received, you can enter digit through remote location, it will pass through modem to the DTMF card.
Step 9: Display the output by glowing LED's on DTMF card.
Step 10: With the help of continuous search it recognize the binary digits and convert it into decimal numbers. Then decimal numbers get checked and append those numbers into the textbox of the screen.
Step 11: To check the length of password or PIN is necessary. If password length is match then & then only fire a query.
Step 12: If, entered password or PIN matches to particular user ID's PIN then only access is allowed otherwise transaction is fail.

When enter number 3 from mobile keypad display in Binary form on the DTMF board. Through the mobile phone user enter the PIN number or digit 3, which is received by the DTMF board and LED get glow.

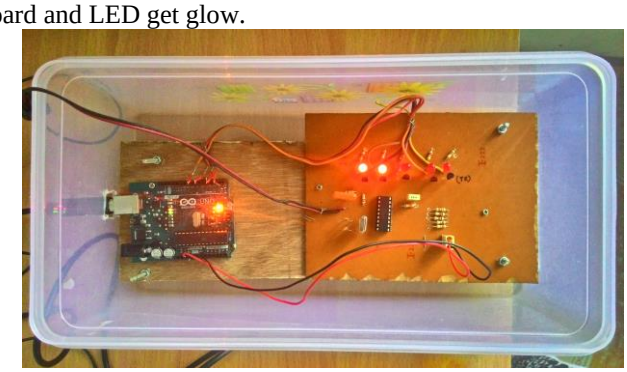

**Figure 10. On DTMF card LED's get glows by entering no. 3 through mobile phone.**

When enter number 3 from mobile keypad display in decimal, asterisk and binary form on the screen. This screen shows binary number textbox, entering 3 number of PIN in the text box. Also show that number in asterisk form.

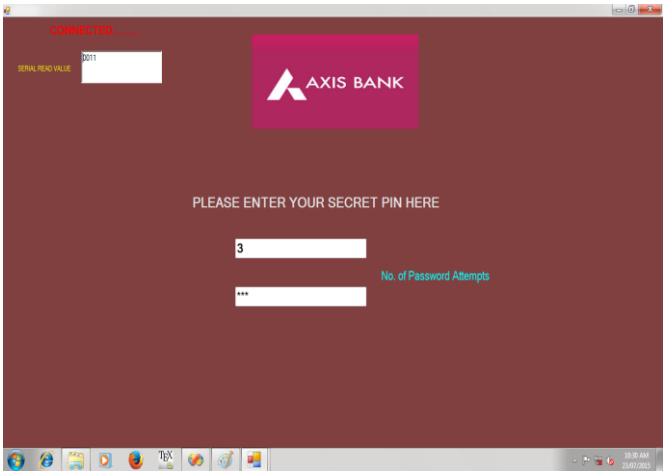


**Figure 11. Running Snapshot when enter no. 3 via mobile display on the screen**

We have plotted the graph by considering the year and how the attacks may be get reduced. This graph shows comparison between the traditional PIN entry system attacks as shown in above graph those are get reduced by using secure PIN entry method.

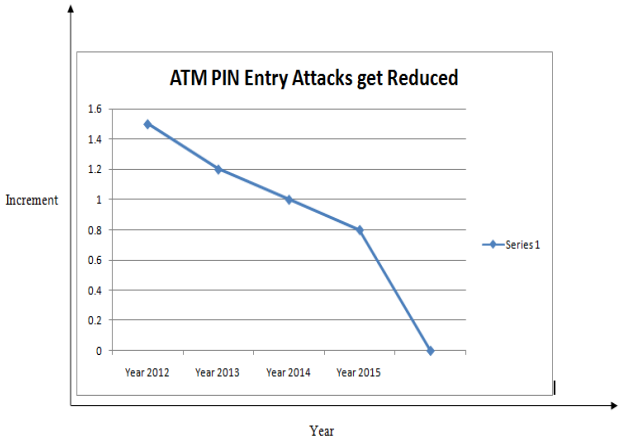


**Figure 12. Attacks get reduced with secure PIN entry method**

**Acknowledgement**

I am grateful to number of individuals whose professional guidance along with encouragement has made it very pleasant to undertake in this paper.

I take this opportunity to express my profound gratitude and deep regards to my guide and truly teacher of teachers Prof. R. N. Devikar for their exemplary guidance, monitoring and constant encouragement throughout this paper. I also express a deep sense of gratitude to Prof. B. S. Borkar, Head of Information Technology Engineering Department for their valuable guidance and encouragement.

I am obliged to our Principal Dr. G. J. Vikhe Patil for their inspiration and co-operation.

**Conclusion**

An ATM machine authentication is done in very secure manner as well as provides better security to the video surveillance, shoulder surfing or fake PIN pads attacks. System gives PIN entry via GSM. Gives good balance between security and usability. We improve state-of-the-art ATM security by introducing an integrity proof towards the user and shifting the PIN entry towards the user's mobile phone.

The advantage of system is that from a non-technical point of view for the customers. Thus, the customer is not confronted with any complicated authentication schemes. As most people carry a mobile phone with them and our application is quite straightforward, we think that the usability for the users is also right. Our scheme constitutes a practicable approach for banks to advance ATM security by keeping this authentication. For future work we believe that in defense our secure authentication system is useful. In various sensitive sectors for authentication the system provide better service. Moreover, our proposed secure system is useful for society.

**References**

[1] Ronald Petrlic, Christoph Sorge, "Establishing user trust in automated teller machine integrity," Computer Science Department, University of Paderborn, Paderborn, Germany, Vol. 8, Iss. 2, 2014, pp.132–139.

[2] Bernhard Frauendienst, Alexander De Luca, Sbastian Boring, Heinrich Hussmann, "My Phone is my Keypad: Privacy-Enhanced PIN-Entry on Public Terminals," Media Informatics Group, University of Munich Amalienstr, Munich, Germany, 2009, pp. 854-858.

[3] Richter, K., Roth, V., Freidinger, R., "A PIN entry method resilient against shoulder surfing," In: CCS '04: Proc. 11th ACM Conf. on Computer and Communications Security, New York, NY, USA, ACM, 2004, pp. 236-245.

[4] Alexander De Luca, Marc Langheinrich, Heinrich Hussmann, "Towards Understanding ATM Security: A Field Study of Real World ATM Use," Faculty of Informatics, University of Lugano, Via G. Buffi, Lugano, Switzerland, (2010).

[5] ATM Marketplace, "ATMs reprogrammed to print out ATM, debit details on receipts," 2009.

[6] ATM Marketplace, "Reprogrammed ATM helps minn. man get away," 2009.

[7] Berger, S., Cáceres, R., Goldman, K.A., Perez, R., Sailer, R., van Doorn, "vTPM: virtualizing the trusted platform module," In: USENIX-SS'06: Proc. 15th Conf. on USENIX Security Symp.Berkeley, CA, USA, USENIX Association, 2006.

[8] Stumpf, F., Benz, M., Hermanowski, M., Eckert, C., "An approach to a trust-worthy system architecture using virtualization," vol. 4610 of lecture notes in computer science, Springer Berlin Heidelberg, 2007, pp.191-202.

[9] Berger, S., Cáceres, R., Pendarakis, D., et al, "TVDc: managing security in the trusted virtual datacenter," SIGOPS Oper. Syst. Rev., 2008, pp.40-47.

[10] De Luca, A., Langheinrich, M., Hussmann, H., "Towards understanding ATM security: a field study of real world ATM use," In: Proc. Sixth Symp. on Usable Privacy and Security (SOUPS '10), New York, NY, USA, 2010, pp.16:1-16:10.

[11] De Angeli, A., Coventry, L., Johnson, G., Renaud, K., "Is a picture really worth a thousand words? Exploring the feasibility of graphical authentication systems," Int. J. Hum.-Comput.Stud., 2009, pp.128-152.

[12] GRGBanking Equipment (HK) Co., Ltd, "Best Practice for ATM Security," 2011.

[13] Becher, M., Freiling, F.C., Hoffmann, J., Holz, T., Uellenbeck, S., Wolf, C., "Mobile security catching up? Revealing the nuts and bolts of the security of mobile devices," In: 2011 IEEE Symp. on Security and Privacy (SP), 2011, pp .96-111.