



Strategies and techniques of Banking security and ATMs

Shivam Chaurasiya¹, Chetan Prajapati²

¹(MCA, Viva Institute of Technology, India)

²(MCA, Viva Institute of Technology, India)

Abstract : Security may be a major issue in cash dispenser Machine (ATM).with the wide unfold utilization of electronic transactions it's necessary to extend customers recognition accuracy. Biometric systems can give a convenient and secure mode of authentication to the shoppers.Nowadays the banking sector is one among the foremost vital elements of an individual's day to day life. Banking facilities are unit wide used by folks for his or her economies activities.cash dispenser Machine (ATM) is an electronic machine that is employed for accessing a checking account from anyplace while not requiring the assistance of bank workers. The user will perform many banking activities like money withdrawal, cash transfer with the assistance of an ATM. it's discovered that the numbers of crime associated with ATM magnification thus have to be compelled to offer higher security to ATM machines.

Keywords: ATM machine,ATM security,Appropriate Password,Bank Passbook,Bank security,Customer details,Identity card,OTP and Password Security Guard.

I. INTRODUCTION

ATM is an electronic machine thus any device that allows the client of a financial organization to perform monetary transactions, money withdrawal, while not the requirement for an individual's gift. ATM trade Association, that features a record that about to three million ATMs area unit presently put in worldwide. Beside the growing convenience and practicableness of the ATMs, there's additionally a rise within the quantity of ATM thieving and driver fraud, that area unit developing at an forbidding rate. Within the neck of the woods of practicality versus security needed, the practicality additional needed. Security has continually been viewed upon as AN overhead or afterthought by computer code developers. However within the case of banking and cash transactions, the safety ought to hold the highest priority. Increase in daily attacks on ATM and banking security the developers older right track and putt security their necessary facet in developing comes. The multi issue authentication is an approach to authentication which requires the presentation of 2 or additional authentication issues: an information factor, a possession issue, And an inheritance issue. When presentation, every issue should be valid by the opposite party for authentication to occur. In gift days the ATM holds just one factor Pin to secure the cash saved within the bank if we tend to aren't considering the physical attacks. In our system we tend to area unit going on the far side this level of security to reinforce security of the ATM. We tend to introduce the conception of 1 time watchword OTP in ATM banking. Our system can give the second level of security victimization various factors to come up with OTP. This may send over customer's mobile range keep in records. In secure ATM, user can get to register mobile and its IMEI range in bank system. Once user puts/swipes card into machine, user get request to insert PIN (which is current approach of ATM banking). Within the projected system user can get OTP on mobile. Once user enters OTP to the system, he/she are having access to the machine else no group action are often created.

ATMs or automated teller machine area unit one thing that everyone is awake too recently. ATMs area unit helpful instrumentation that we tend to all use to induce money from banks. They save U.S. from waiting in long queues in banks for retreating money from our bank accounts. However, the shortage of awareness of users concerning the ATM security has been inflicting hassle and problems to the ATM users. The cases of ATM frauds and skimming are additional and additional common within the GB and across the world. This is regularly relevant even just in case of the young students United Nations agency area unit the new generation users of the ATM services.[3]

II. THE LITERATURE REVIEW

This section will help to provide the basic concepts of skimming and other related frauds at ATMs. It will also help in providing a basic understanding of the mechanism behind the skimming attacks and the mode of operation that is used by the fraudsters or the skimmers. Basically, an attempt will be made in order to describe the rising incidents of the skimming and the other fraud attacks on the ATMs at a global level and within the UK.

We have gone through the different types of researched work and papers on ATM security system some of them and have been reported in the literature. However, few relevant and significant works are reviewed here. Crime at ATMs has become a nationwide issue that faces not only customers, but also bank operators and this financial crime case rises repeatedly in recent years. A lot of criminal's tamper with the ATM terminal and steal customers' card details by illegal means. Once users' bank card is lost and the password is stolen, the users' account is vulnerable to attack. Traditional ATM systems authenticate generally by using a card (credit, debit, or smart) and a password or PIN which no doubt has some defects. The prevailing techniques of user authentication, which involves the use of either passwords and user IDs (identifiers), or identification cards and PIN (personal identification numbers), suffer from several limitations. Passwords and PIN can be illicitly acquired by direct covert observation.[5]

III. THE BASIC UNDERSTANDING OF ATM SKIMMING

The term ATM skimming describes the ways that the criminals use to capture the account info of someone on the rear of the bank's card once they used it at an ATM's purpose of sale terminals. What is more, the criminals use devices like "skimmers" to capture the small print of an ATM credit or revolving credit, this info is sometimes held on within the magnetic strip of the cardboard (Shaikh, 2012). The data on the magnetic strips of the cardboard will be browsed and deciphered by the appliance of a tiny low card reader, that is unbroken {close to|on the brink of|near to|about to|getting browser to|on the point of} the or on prime of the slot of the particular card reader to read and record the data that is gift on the magnetic track of the cardboard. Moreover, once removing this malicious device the recorded knowledge will be downloaded. To feature to it, skimming is that the method of capturing the personal and also the personal knowledge of the cardholder by compromising a card-reading device for a few monetary or alternative gains. ATM skimming will be thought of as an fraud for debit and credit cards. That's as a result of hidden physical science square measure employed by thieves to repeat the private knowledge of the cardholders from the magnetic stripes of a card (Singh, 2012). A PIN capturing device or camera is additionally used usually with a skimming device. Criminals then store the purloined info in counterfeit or faux cards. In alternative words, faux credit cards carry the purloined info of the ATM skimming victims. These victims typically carry their credit cards while not knowing that they may be thought of as a target of a stealing crime. These faux cards seem legitimate, with issuers, logos and magnetic strips. The skimmers typically use the faux eleven cards sometimes so abandon them before the victim realizes and reports this misuse to their issued bank (Singh, 2012). Moreover, additional cards square measure still being issued now; the merchants have to be compelled to still invest within the EMV terminals. Because of this delay, there square measure still several cards.[1][6]

IV. METHODOLOGY

The Research Philosophy According to Elliot, the research philosophy is about the manner in which research builds the source, the nature and the nurturing of the knowledge expected from the research (Elliot, 2005). The research philosophy adopted here would be interpretive in the nature where the responses of the respondents will be interpreted using interpretation research philosophy[9]

The Research Purpose A research must have a purpose to ensure that the research is being conducted and progressed in the right direction. The purpose of the research here would be to understand the existing awareness of youngsters regarding the security measures and effective usage of ATMs.[4][7]

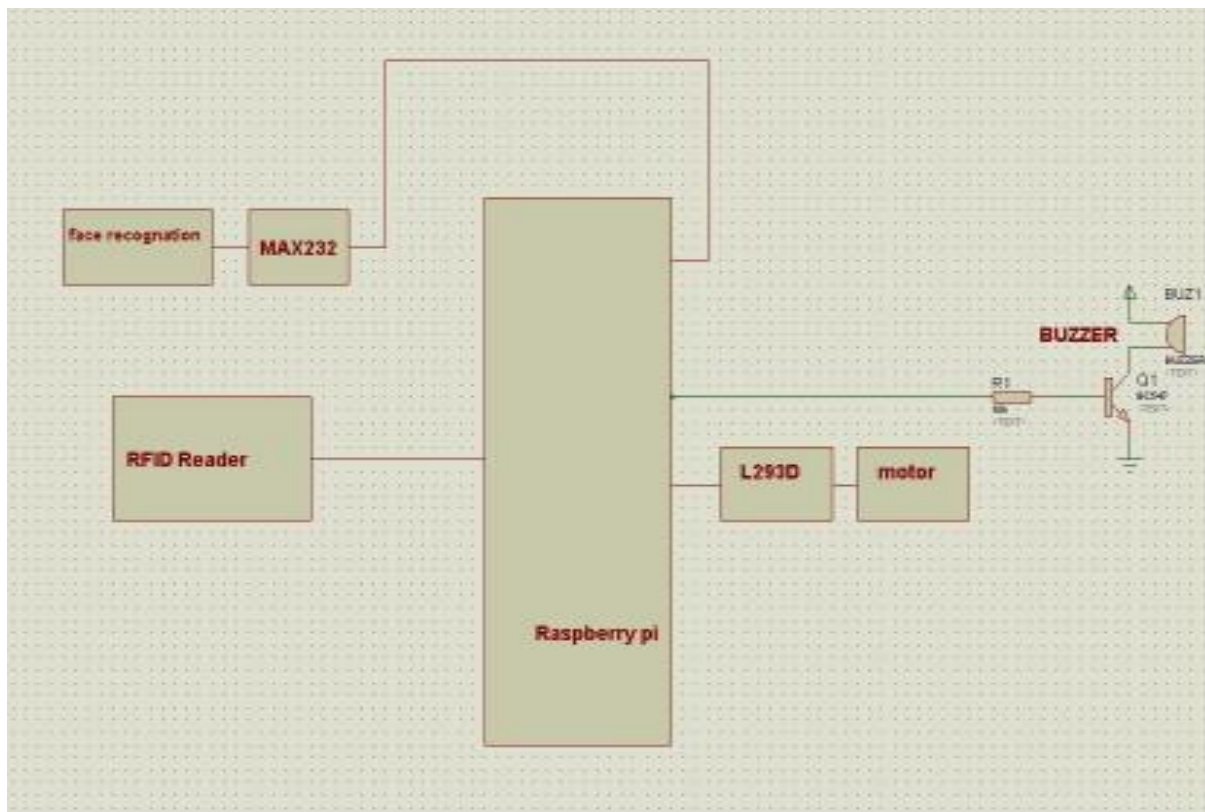
The Research Strategy According to Silverman, the research strategy is about the manner in which you conduct your strategy. It is about choosing whether the research is to be done using primary data or secondary data or even both. The Research Approach The choice of the research approach can be from the available three types, which are deductive, inductive and adductive. According to Denzin & Lincoln, deductive approach can be used to prove the correctness and applicability of an existing theory in the chosen scenario.

The Data Analysis The data analysis should be done effectively in order to achieve effective and applicable results. This research would be adopting thematic data analysis using qualitative analysis on the primary data collected from the surveys and the interviews.[11]

The Reliability The research conducted would be highly reliable as the data would be collected directly from the primary respondents and therefore, the authenticity of the research would be ensured. The respondent's' identity would be kept secret 0 **The Validity** The research results are expected to be highly valid for the analysis of the necessity of awareness about security measures and knowledge during using ATMs. The validity is expected to be high, as only primary data will be collected from respondents directly.[2][10]

V. PROPOSED SYSTEM

The process of ATM dealings starts once face recognized. MATLAB IDE used for face recognition purpose, then next step is RFID card, distinctive for every person, to the RFID reader for scanning. The account associated with the distinctive RFID range can access. Once this step match with keep RFID range than the dealings are allowed. Otherwise, the account data won't be displayed, and more activity are disabled. An analysis should have a purpose to make sure that the research is being conducted and progressed within the right direction. The aim of the analysis here would be to grasp the prevailing awareness of children concerning the safety measures and effective usage of ATMs. The aim of the analysis would be distinctive problems and loopholes within the existing awareness and areas of scope of improvement. Supported the identification of the weaknesses and loopholes within the existing information of the children concerning safe and effective use of ATMs, suggestions would be created concerning enhancing the cognitive content concerning ATM security. The feedback of a bank worker and also the expertise of a teen World Health Organization has long-faced security problems whereas victimization Associate in Nursing ATM square measure assessed as a section of the aim for this analysis paper.[12]



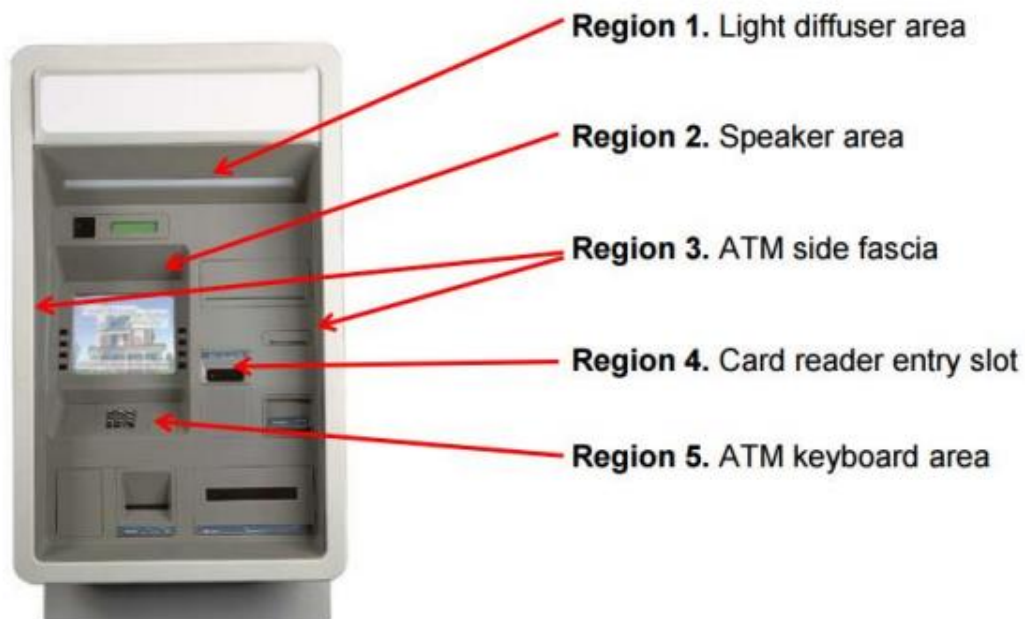


Figure: Where to spot the Card Skimming or the PIN Capturing devices on an ATM Machine (Wild, 2015).

VI. CONCLUSION

The results Face recognition might even be a awfully helpful and versatile technique. it's totally correct technique. this system has roaring applications. this system will increase each privacy and identity. the expansion in electronic transactions has resulted terribly} terribly larger demand for quick and correct user identification and authentication. Access codes for buildings, banks accounts and pc systems typically use PIN's for identification and security clearances. traditional methodology of identification supported possession of ID cards or exclusive knowledge kind of a welfare choice or a countersign don't seem to be all quickly reliable. once credit and ATM cards unit lost or taken, makings unauthorized user will typically return up with the right personal codes. Despite warning, many individuals still select simply guessed PIN's and passwords birthdays, phone numbers and welfare numbers. This paper might solve this flinch and helpful for detection a fraud . it's utilised in Bank sector and any ATM connected security. it's place along named as as bad person following system. As there's a scope for improvement and as a future implementation we'll add a following chip on ATM card for tracing the situation of card that's in a very position to facilitate in providing users facilitate. Face recognition technique finds associate large vary of applications in fields involving high security. it's advancement at intervals the arena of technology thereby giving a beautiful push to the technology trade. several comes associated with security and management unit typically enforced by this face recognition technique.[8]

A number of key themes emerge on the shape of conclusions from the findings and their analysis. The figure below illustrates the conclusions arrived at:

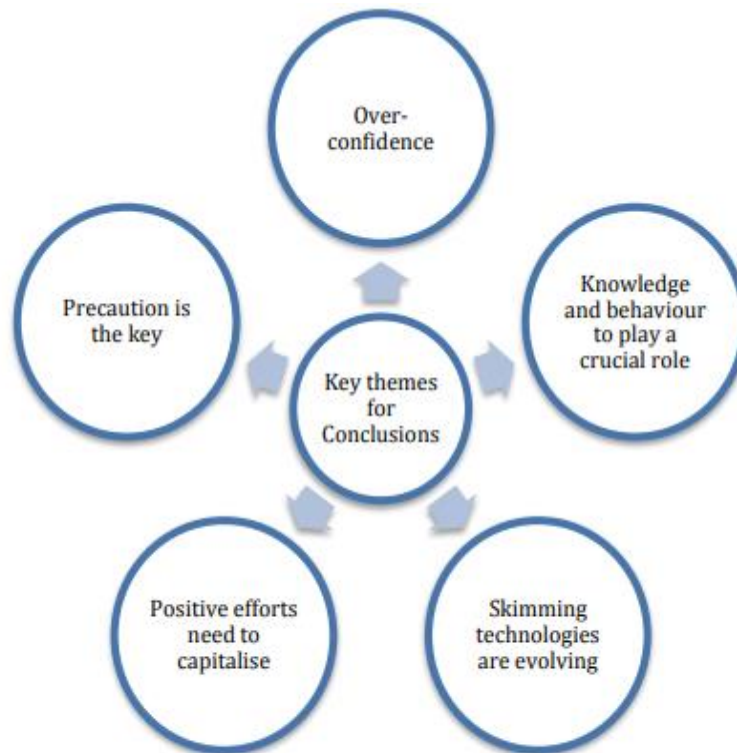


Figure: Key conclusions arrived from the results and analysis.

As can be seen in the figure above, an important theme to consider is the over-confidence, which is visible through student responses. It can be seen that most students do not feel threatened or do not see the seriousness of ATM security therefore they don't find it as an issue. Closed spaces and security guards in the form of physical security barriers seem to be sufficient for them. Similar overconfidence can be seen in their bank choosing behaviour, wherein they do not choose or consider security considerations to be an important parameter to finalize their bank choice. Secondly, both the knowledge and the behaviour of the customers have to play a crucial role in preventing them from self-harm. The interactions reveal a clear lack of knowledge to be easily evident among the respondents. Students show little understanding or knowledge towards skimming frauds and are highly unaware of the services which bank provides to prevent skimming frauds in the first place. Next with regard to the ATM visit and usage behaviour of the customers, it can be concluded and stated that although most students would like to visit ATM premises for conducting transactions, they have not paid attention to security guidelines, which banks provide through their websites.[3]

REFERENCES

- [1]Barker, K., & Sheridan, P. (2008). mastercard fraud: awareness and bar. *Journal of monetary Crime* , 15 (4), 398-410.
- [2]Dawson, C. (2009). *Introduction to analysis ways*. London: the way to Books,Ltd.
- [3]Degu, G., & Yigzaw, T. (2006). *analysis Methodology* . Ethiopia: University of Gondar.
- [4] Denzin, N. K., & Lincoln, Y. S. (2000). *reference book of qualitative analysis ((2nd disfunction.) ed.)*. Thousand Oaks, CA: Sage.
- [5][Ruane, J. M. (2008). *necessities of analysis Methods: A Guide to scientific discipline analysis*. London: Blackwell Publishers.
- [6]ARM7 primarily based sensible ATM Access & Security System exploitation Fingerprint Recognition & GSM Technology Khatmode Ranjit P1 , Kulkarni Ramchandra V2 , Ghodke Bharat S3 , Prof. P. P. Chitte4 , Prof. Anap S. D five one Student of B.E. physics, Pravara Rural engineering faculty, Ioni, geographic area,
- [7]An Improved technique for Extraction of Fingerprint options Jianwei rule, Lifeng Liu, and Tianzi Jiang*, Member, IEEE National Laboratory of Pattern Recognition, Institute of Automation, Chinese Academy of Sciences, Peking 100080, P. R. China.
- [8]Indian Journal of Science and Technology Supplementary Article ATM Terminal style exploitation Biological Technology by V. Khanaa and avatar Mohanta.
- [9]Volume three, No. 11, November 2012 *Journal of worldwide analysis in computing analysis PAPER HIGH PROTECTION HUMAN IRIS AUTHENTICATION IN NEW ATM TERMINAL style exploitation biometry MECHANISM*.
- [10]Neuman, W. L. (2000). *Social analysis methods: Qualitative and quantitative aproaches (4th disfunction.)*Boston: Allyn and Bacon.
- [11]Nwankwo, O. (2013). Implications of Fraud on business Banks Performance in Nigeria.*International Journal of Business and Management* , 8 (5), 119-125.
- [12]Ruane, J. M. (2008). *necessities of analysis Methods: A Guide to science analysis*. London:Blackwell Publishers.