Analysis Of Atm Premise Security Aspects On Preventing Cardholder's Pin Theft And Attack A Case Of Crdb Branches In Dar Es Salaam, Tanzania

Gervas Mgaya
Department of Computer Science
Ruaha Catholic University (RUCU)
Iringa, Tanzania
gervassandagila@yahoo.com

***Abstract*—Security in automatic teller machine (ATM) is one of the challenging subjects in security matters nowadays and particularly in Tanzania. Escalation of ATM thefts is overwhelming commercial banks in the country which are increasingly finding it difficult to cope with huge requests to compensate hundreds of victims of the electronic fraud. Tanzanian Banks are losing hundreds of millions of shillings in ATM card skimming and their customers are worried on the fate of their deposits. Securing PIN and preventing cardholders from attack at ATM site have gained a considerable attention during these recent years of advancement of science and technology. People have become victims of identity theft and assaults as a result of inadequate security measures at ATM premise. The aim of this study was to analyze the ATM premise security so as to identify security weaknesses and provide pertinent remedies. The study extremely involved CRDB bank in Dar es salaam City which has many ATMs installed in different locations like supermarket, fuel station/ bus stations and university campuses. 15 ATM premises were surveyed and observed. 100 cardholders and 10 ATM administrators/operators were randomly consulted. Data collected after surveys were analyzed using SPSS and then percentage analysis were done to find out the weaknesses of the security of ATM premise. The study revealed that, ATM premises do not have foreign device detection system, ground markings. Surveillance cameras and CCTV at the ATM premise are insufficient. ATMs are positioned in a way that paves a way to shoulder surfing and physical attack attempts.**

Keywords—Automated Teller Machine (ATM), ATM premise, cardholder, identity theft, skimming, attack, fraud, Social Engineering.

I. INTRODUCTION

In many countries, ATM has been aggressively promoted to become "the most visible face of e-banking". There is hardly a country in the world where the ATM has not been marketed as the most convenient form of retail banking in particular for cash withdrawal purpose [1].

The use of ATM has almost replaced the human teller (HT) method since its introduction in 1996 in Tanzania[2]. Its acceptance by the public has dramatically increased in these recent years. Now, at least every bank customer possesses an ATM card. However, there are challenges regardless of the remarkable development in e-banking field; one of the challenges is the PIN theft and attack at ATM premise resulting to money loss and injury to a victimized bank customer.

In Tanzania particularly in Dar es salaam city , different banks are now offering ATM cards to their valuable customers. However, no studies have been conducted by internal management of different banks or external company regarding the security of the ATM premise in preventing ATM card skimming and cardholder attack at the time of acquiring ATM services.

The main objective of this research paper was to critically analyze the ATM physical premise security aspects on preventing cardholder's PIN theft and attack in Dar es salaam , particularly at Cooperative Rural Development Bank (CRDB) branches. Three districts of Dar-es salaam region namely Temeke, Kinondoni and Ilala were visited from which a total of 15 ATM premise were surveyed and 100 cardholders, 10 ATM operators were interviewed regarding the security of the ATM premise

II.BACKGROUND AND LITERATURE SURVEY

The 21st Century has witnessed rapid and new innovative technologies with fundamental changes in the way banking process takes place. ATMs are now part and parcel of our lives. ATMs have made banking more convenient today than ever before: with the touch of a few buttons, cardholders can check account balance, withdraw cash, make deposits, top up air time, pay several bills and transfer funds. Banking services are now available 24 hours times 7 days. Performance or efficiency has been advocated. Queuing problems are less pronounced in ATM than in traditional HT of servicing the customers.

Transactions via ATM have gained a considerable attention during these recent years in each banking system and its customers as a whole. Along the same line however, physical security of ATM and protection of cardholder's PIN theft and attack from criminals have been and still a challenge to most of banks in Tanzania particularly, because security is often overlooked, it is not as important as availability, performance and efficiency. A banking institution may have purchased the best security technologies to protect ATM and trained their employees and customers so well that they lock up all their secrets before initiating any ATM transaction, and hired building guards from the best security firm in the business. However, if the environment in which the ATM is located is not well assessed from security viewpoint, that institution is still unsecured.

Simply assuming that fraud risk is low based on previous exposures is unwise security methodology. Social and organizational factors may stigmatize security risks and discourage clear identification of them [3]. Not surprisingly, crimes like identity theft, card jamming, swapping and skimming, shoulder surfing, diversion and physical attacks are spiraling out of control in Tanzania. As per [4], a thief can steal your password and steal what you have without much effort.

There are two approaches in practice with respect to security, sensitivity and secrecy of transactions through these machines. One approach is to authenticate a customer based on what he/she knows like password[4]. The second approach is what you have like an ATM card. Practically, these two approaches are combined together. Personal Identification Number (PIN) is one of the most important techniques to authenticate customers' identity in these machines [5]. However these approaches can be useless if the entire ATM premise does not support them in terms of security. Physical security is an area that is often overlooked when deciding where to locate and install an ATM. However, without physical security, there is no security [6].

It is argued that [7] some people are motivated to commit an ATM crime because of the existence of an easy opportunity, but if that opportunity was not there the crime would not have taken place.

Offenders can employ different techniques like card jamming, PIN card skimming and shoulder surfing via the use of sophisticated spy cameras and binoculars. Changes can be made to the face of the ATMs so that card details are captured, as well as by using various technologies or the involvement of dishonest bank staff. In addition to frauds, offences many also involve violence including robberies, for example where someone is attacked at the ATM premise itself, or by the use of force via threats and intimidation to withdraw and then hand over money.

The research done by [8] indicated various ways which can be used by offenders to carry out ATM crimes. These include; vandalism, shoulder surfing, ATM card skimming and muggings. However, it did not provide a way to enhance the security of the ATM premise in order to eliminate the opportunities for the above techniques to take place.

The study done by [9] on personal information privacy and found that most people have the assumption that they will not be deceived by others, based upon a belief that the probability of being deceived is very low. The attacker having understood this common belief makes his request sound so reasonable that it raises no suspicion, all the while exploiting the victim's trust. This has been attributed to due to the fact that majority of ATM cardholders do not have sufficient knowledge on social engineering attacks.

According to [10], card jamming, Insecurity, Machine breakdown, machine out of cash, and long time in cash dispensing to large extent are among the factors that cause challenges for bank customers when using ATMs in Tanzania.

As per [11] the latest victim of ATM theft is the community of the University of Dar es Salaam (UDSM), which has lost nearly Sh100 million to card skimming. 11 employees of the university comprising professors, senior lecturers and other staff who have each lost between Sh800,000 to Sh7 million in electronic theft from CRDB . Two professors, who wish to remain anonymous, have lost Sh6 million and Sh7.2 million each in ATM hacking. The fraudsters reportedly share bank information and personal identification numbers they have hacked from local banks with partners as far away as the United Kingdom and the United States of America. However

the source did not explain how the ATM site paved the way to ATM skimming.

Therefore it is explicitly empirical that banks that provide services via ATM should be aware of these security aspects of ATM premise.

The review of the literature helped the researcher to come up with the following methodology in order to achieve the objective of the study.

III. METHODOLOGY

Dar es salam region is a business city because it is a pathway to Malawi, DRC Congo, Zambia, Burundi, Rwanda via Dar es salaam port. It is one of the highly populated region with *4,364,541* millions of people as of the official 2012 census. AS a result, many banks have invested and some others are considering to invest in order to win customers. The CRDB and NBC are the most leading banks which have over 40 ATMs installed in different places at Dar es salaam. Thas is why CRDB has been selected for the purpose of this study. The primary data were obtained through survey and observation, interview and questionnaires. 15 ATM premises were surveyed and observed and 10 ATM administrators/operators were randomly interviewed. A well-structured questionnaire was prepared and distributed to 100 customers of CRDB in Dar es salaam at the ATM site and through emails.

Secondary information sources used for the present research included the journals, magazines and internet sources.

The data was collected based on convenience methodology. Customers having strong experience of ATM have been considered as respondents to collect information. The data collected were analyzed through percentages and frequencies in which the data were presented in table formats, pie charts and histograms which were obtained using SPSS (Statistical Package for Social Science). The study was conducted in January 2014 to February 2015.

IV. RESULTS AND DISCUSSIONS OF THE FINDINGS

The following are the results obtained from primary data which were collected through observation,questionnaires and interviews.

Results from observation

Table 1: shows the positioning of the ATM

	Evaluation level	Frequency	Percent
Valid	very unsatisfactory	1	3.3
	Unsatisfactory	2	6.7
	Somehow unsatisfactory	3	10.0
	Satisfactory	4	30.0
	very satisfactory	5	50.0
	Total	15	100.0

From the table above, 1 ATM site out of 15 was found to be very unsatisfactory due to the fact that it was not visible from public point of view and it was installed in are area which was not well-lit . 2 ATM sites were unsatisfactory, 3 ATM sites were somehow unsatisfactory as far as visibility and well-lit aspects are concerned especially during the night. The picture below is an evidence of the situation;

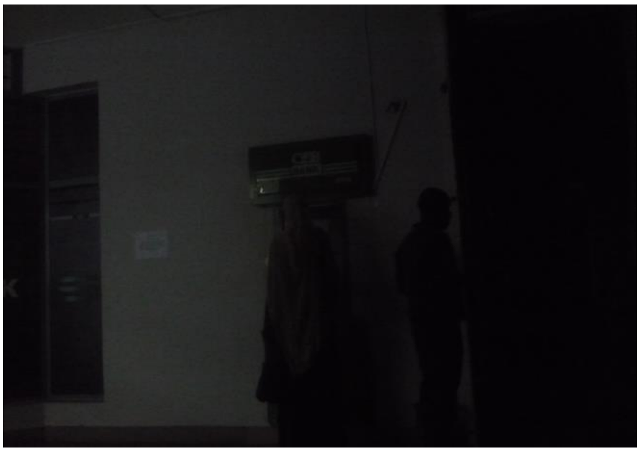


Table 2: Results of observation on building walls, floor and selling of ATM site

		Frequency	Percent
Valid	Worst	1	3.3
	Bad	2	6.7
	Good	1	3.3
	Excellent	26	86.7
	Total	30	100.0

From the table, one ATM site which is equivalent to 3.3 % was found to be the worst of all the 30 visited ATM sites as it had the poorest walls, floor and ceiling it terms of security. 2 ATM sites that are equivalent to 6.7% of all the 30 visited ATM sites were bad in terms of their walls, floor and ceiling that thieves could easily temper with. 1 ATM site (3.3%) was good enough to deter thieves and 26 ATM sites (86.7%) were so excellent that thieves could face difficult to penetrate through.

Table 3:Results of observation on possibility of cardholders' PIN spoofing

	Evaluation level	Frequency	Percent
Valid	very unsatisfactory	9	30.0
	Somehow unsatisfactory	4	13.3
	Unsatisfactory	14	46.7
	Satisfactory	1	3.3
	very satisfactory	2	6.7
	Total	30	100.0

From the table above, 9 (30%) ATM sites were very unsatisfactory, 4 (13.3%) were somehow unsatisfactory, 14 (46.7%) were unsatisfactory. This has been attributed to by the fact that most of the ATM are on open area where there is not obscured fence which can protect the customer in service from shoulder surfing and spoofing as evidenced by the below picture

Absence of glass fence that prevents PIN against spoofing at ATM premise

Table 4: Presence of criminal hiding areas around ATM premise

		Frequency	Percent
Valid	no hiding area	4	13.3
	Low possibility	8	26.7
	High possibility	18	60.0
	Total	30	100.0

4 ATM sites (13.3%) had no places around where criminals could hide themselves. 8 ATM sites (26.7%) had places where there was low possibility for criminals to hide themselves and 18 ATM sites (60%) had places where there was high possibility for criminals to hide themselves .The picture below shows how the ATM premise is in intact with other surroundings which are good hiding places for offenders especially during the night.

Table 5: Number of working cameras at ATM premise

	Number of camera	Frequency	Percent
Valid	0	4	13.35
	1	22	73.3
	2	4	13.35
	3 and above	0	0
	Total	30	100.0

Cameras collect images, which are transferred to a monitor- recording device of some sort, where they are available to be watched, reviewed and/or stored.

From above table, 13.35% of all the visited ATM premises had no cameras at all implying that a person could manage to commit an offence without being noticed.

73.3% were having only one camera, which is unhealthy in security perspective due to the fact that it could be easily tempered or subjected to a single point of failure problem as evidenced by the picture below;

Table 6: Existence of ground markings at ATM premise

		Frequency	Percent
Valid	did not have	30	100.0
	Have	0	0

Ground markings indicate the point where the next cardholder to enter the ATM chamber should stand so as to keep a security distance from him/her to another cardholder who is already in the ATM chamber being serviced by the ATM. From the table above, all 30 visited ATMs (100%) did not have ground markings at all. As a result ATM users have been subjected to the environment where their PIN could be spoofed by others in the queuing line.

Table 7: Presence of security guard

		Frequency	Percent
Valid	did not have	4	13.3
	Had	26	86.7
	Total	30	100.0

Human surveillance at ATM is very important aspect for ATM premise security. From the table above, 4 ATM premises (13.3%) had no security guard. This implicitly creates a loop hole for people to commit an ATM offence.

Results from questionnaire

Table 7: Cardholders' level of education

		Frequency	Percent
Valid	Non	4	4.0
	Primary	21	20.8
	secondary	26	25.7
	diploma	22	21.8
	degree	27	26.7
Total		100	99.0

The researcher posed this research question to CRDB cardholders to find out their educational status so as to justify the validity of respondents. Those respondents who did not attend any level of education were a bit hesitating in participating to the study as they knew little about security matters unlike other respondents of higher levels of education. Hence, the researcher had to provide little orientation to them as far as the study was concerned.

Table 8: Possibility of PIN being observed during the entry

		Frequency	Percent
Valid	NO	34	33.7
	YES	66	65.3
	Total	100	99.0
Missing	System	1	1.0
Total		101	100.0

From the table above, 65.3% of the respondents said that the ATMs from which they were serviced recently are so open that their PIN can be observed during the entry. This coincides with observation result in table 3 and is one of the reasons for massive ATM fraud.

Table 9.Cardholders' responses on whether they had been physically attacked at ATM premise

		Frequency	Percent
Valid	NO	96	95.0
	Yes	4	4.0
	Total	100	99.0

From the table above, 4% of the respondents asserted that they had been physically attacked by robbers once in time during the departure at ATM premise. This provides clues about inadequacy of security measures at ATM site more specifically on the presence of human security guard.

Table 10. Cross-tabulation of cardholders who had been assisted by a stranger and those who assisted others

Cardholder		Assisted Someone		Total
		NO	Yes	
Assisted By Stranger	NO	7	23	30
	YES	24	46	70
Total		31	69	100

From the table above, 7 respondents were not assisted by a stranger and did not assist any body to access the ATM, 23 respondents were not assisted by a stranger but dared to assist someone to access the ATM, 24 respondents were assisted by a stranger but they themselves did not assist someone to access the ATM and 46 respondents were assisted by a stranger and dared to assist someone to access the ATM. This indicates that majority of bank customers who are serviced via ATM have insufficient knowledge on how to use ATM and ATM premise security as a whole. This knowledge gap is a loop hole for fraudsters to commit ATM offences.

Resulst rom f the interview

Table 11: Provision of education to the first time - ATM card users

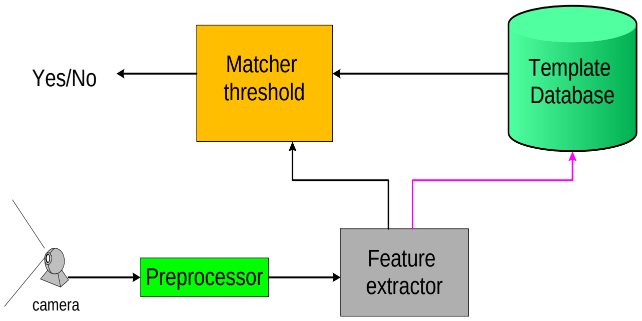
		Frequency	Percent	Valid Percent
Valid	YES	10	100.0	100.0

From the table above, all 10 interviewed ATM administrators did strongly and positively respond that their banks do provide preliminary education to their first time-ATM users. However, the results from table 10 suggest that this orientation knowledge provided to the first ATM customers is insufficient as evidenced by majority of them had to be assisted by someone during their first ATM transactions.

Table 12:Existence of a system to detect foreign devices at ATM premise .

		Frequency	Percent
Valid	NO	10	100.0
	YES	0	0

From the table above, 100% of all the interviewed ATM administrators acknowledged that there were no mechanisms for detecting foreign devices in the ATM premise. Having a mechanism to detect any foreign device in the ATM chamber is very crucial because bank staff can be notified of such device and react instantly on it before it has accomplished its mission. That is why also most of the ATM crimes in Dar es salaam have been successful and Banks have been being notified through customers who have been victimized with ATM frauds. This has made Banks remain so reactive rather than proactive to ATM crimes. The banks rely solely on the installed cameras and human surveillance available at ATM premise. However, these security measures are not able to detect sophisticated devices that can be installed by criminals to target cardholder's card, PIN, money and even the ATM itself. A mechanism to alert the banking ATM administrator that a certain malicious device has been installed in the ATM premise is very vital for security purpose. The following figure depicts the model for recognizing foreign device at the ATM premise



1. First, a live image of the ATM premise is acquired through surveillance camera (or CCTV) installed in the ATM premise. The image patterns are sent to the central control facility.

2. Second, software in the central control facility is employed to detect the location of any strange device in the acquired image. This task is difficult, and often generalized patterns of what a device looks like are employed to pick out the device.

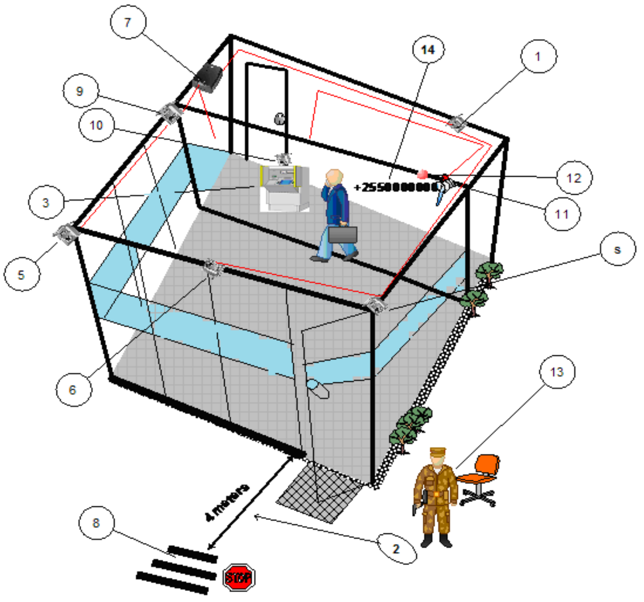
3. Once the device detection software has targeted a device, it can be analyzed by extracting the identified features of a device. The most popular method for feature extraction is called Principle Components Analysis (PCA), which is transform the identified features into a lower dimensional space but losing as little information as possible. Template generation is the result of the feature extraction process [12]. These templates are also referred to as training data set.

4. The fourth step, the template generated in step three is compared with those in a database of known devices for similarity. In an identification application, this process yields scores that indicate how closely the generated template matches each of those in the database. In a verification application, the generated template is only compared with one template in the database. In some cases (probably the most natural way), the similarity is given in terms of a rate varying from 0% for totally different patterns to 100% for perfectly similar patterns [13]. To compare two patterns, the system uses a metric that measures a kind of distance (the similarity or the dissimilarity) to assess how similar are two patterns. Some commonly used metrics are Minkowski distance, cosine distance, Hausdorff distance, Mahalanobis Distance [14] or city block distance and Euclidian distance that are particular Minkowski distances.

5. The final step is determining whether any scores produced in step four are high enough to declare a match. The rules governing the declaration of a match can be configured by the ATMA, so that he or she can determine how the foreign device recognition system should behave based on security and operational considerations. For instance when there is a match (Yes) the system should switch on the alarm system to alert the bank that there is a strange device maliciously installed in the ATM chamber. When there is mismatch the foreign device recognition should do nothing.

A model for enhancing security of ATM premise

This model aims at incorporating all the security aspects that the study has identified to miss or to be insufficient in ATM premise. These were ground markings, CCTV cameras, security guard, obscuring stripe to cover the ATM keyboard, emergency phone number, security alarm and foreign device recognition system.



The numbers on the figure above stands for the following:-

1. ATM servicing room CCTV camera for capturing the horizontal and vertical area
2. Security space distance
3. ATM
4. ATM site right CCTV camera for capturing right horizontal and vertical area
5. ATM site left CCTV camera for capturing left horizontal and vertical area
6. ATM site front CCTV camera for capturing front horizontal and vertical area
7. video recorder in service area
8. Ground markings for indication of starting point of free security space distance
9. ATM chamber CCT camera for capturing all area in the chamber
10. Cardholder's face and chest CCTV camera
11. Security alarm system terminal
12. Fire alarm system terminal
13. Security guard to monitor all the security measures and policies at ATM premise
14. Emergency phone number for cardholder to call the bank when a serious problem arises

15. Cardholder in the ATM chamber

16. Obscuring colour bar to cover ATM keyboard

17. Foreign device recognition system that starts with the CCTV camera

V.CONCLUSION

According to above discussion of the findings from primary source of data which were obtained through observation, questionnaires and interviews, it can be concluded that ATMs at Dar es salaam are still vulnerable to attack and the customers using these ATM may fall victims at any time. The present environment that surrounds an ATM machine has security loop holes (absence of obscuring fence, ground markings and foreign device detection mechanism) that has created a room for criminals to exercise should surfing, card jamming, card tapping and PIN recording.

VI.RECOMMENDATIONS AND FUTURE WORK

As far as the security of ATM premise is concerned, the banks should proactively make a thorough identification of all possible hiding localities and try to remove them if possible before the installation of ATM. This will reduce the possibility of cardholders' physical attack, injury by robbers and bank.

The CRDB bank in Dar es salaam should add more surveillance cameras and CCTV to the ATM premise in order to get rid of single point of failure problem which has been implicitly noted as evidenced by majority of ATMs having only one camera or CCTV. It should also incorporate foreign device detection system in the ATM premise to ensure that any malicious devices placed in ATM premises are detected as soon as possible.

Cardholder should be cautious at ATMs. Identity thieves targeting cardholder's PIN and card have been known to place sophisticated skimming devices over ATM slots to steal card account information. Hence, a cardholder should look for suspicious devices in the ATM chamber before the initiation of transaction, check for exposed wires, tape, or loose connections; look for hidden cameras on the sides of the ATM that criminals use to record ATM passwords. Cardholder should also be aware of those people who may have too much of an interest in his/her ATM transaction—the ones who are trying to look over his/her shoulder to see what he/she is doing. They may be shoulder surfers attempting to see cardholder's account balance or PIN.

The study has centered itself to CRDB branches in Dar es Salaam as far as ATM premise security is concerned. Considerable work needs to be done to other banking institutions that provide banking service via ATM meanwhile expanding the case of study to include other regions in Tanzania

The study has concentrated on the physical part of the ATM premise security. However, further research work is needed to include other aspects of security of ATM namely logical and social engineering parts which play a key role in security of any computerized system.

ACKNOWLEDGMENT

I would like to extend my appreciation to Charles Tarimo of University of Dar es salaam, Patrick Kihwele and Lusekelo Kibona of Ruaha Catholic University for their support during the preparation of this paper . This work could not bear honest fruits, without the inexpressible contribution and cooperation of the CRDB Staffs of Dar es Salaam branches for responding positively during the interview session. Thanks to CRDB Cardholders to whom I distributed my questionnaires, for showing me a great cooperation. Also I would like to thank wife Grace and my son Gratian for their patience during my absence.

REFERENCES

[1] Kulundu W. “Lesotho Law Journal, Dematerialisation of Banking instruments in Lesotho” in Eletronic Banking: An overview of system and operations 1998, vol.11 No 1.

[2] Ntagazwa R (2010) , Legal aspects of ATM in

Tanzania, Dissertation submitted at Ruaha University for award of L.L.B degree (2010).

[3] Hunter Magdalena (2000). The Centre for Gender and Development: Newsletter R.N. Charette (1996). Large-scale project management is risk management. IEEE Software

[4] Cornish, D and Clarke, R (2005) Opportunities, Precipitators and Criminal Decisions. In theory for practice in Situational Crime Prevention Studies, Vol 16. Monsey: Criminal Justice Press.

[5] Bruce Schneier: “Secrets and Lies”, *second edition*, Wiley, New York, 2004, available at http://www.schneier.com/book-sandl.html.

[6] James Michael Stewart (2004***), Security+™ Fast Pass***. SYBEX Inc.

[7] Felson, M. & Clarke, R.V. (1998), Opportunity Makes the Thief: Practical Theory for Crime Prevention. *Police Research Series 98*. London: Home Office.

[8] Global ATM Security Alliance (2003). ATM Security Manual for Customers. Retrieved from the World Wide Web April 23, 2010. http://www.atmgroup.net.au/files/file/Docs/ATM-Security-Manual-for-Customers.pdf

[9] Kelvin Mitnick (2003). The Art of Deception, Controlling the human element of security.

[10] E. J. Mwaikali, "Assessment of Challenges Facing Customers in Automated Teller Machines in the Banking Industry in Tanzania: A Case of Some Selected Banks in Tanzania," *International Journal of Research in Business and Technology,* vol. 4, pp. 480-488, 2014.

[11] Rise in ATM theft overwhelms bank. The Citizen online newspaper of December 27,2014 as retrieved on 23 January ,2015 from http://www.thecitizen.co.tz/News/national/Rise-in-ATM-theft-overwhelms-banks/-/1840392/2570136/-/83i5tmz/-/index.html

[12] Roberts, S. and Everson, R. (2001). *Independent Component Analysis- principles and practice*, Cambridge University Press, ISBN 0521792983

[13] Wilhelm Burger and Mark J. Burge."S Digital Image Processing.

[14] Veltkamp, R. C, & Hagedoorn, M. (2001). *State-of-the-art in shape matching*. In *Principles of Visual Information Retrieval*, M. Lew (editor), Springer, ISBN 185233-381-2