Indonesian Journal of Electrical Engineering and Computer Science
Vol. 17, No. 3, March 2020, pp. 1224~1231
ISSN: 2502-4752, DOI: 10.11591/ijeecs.v17.i3.pp1224-1231

Design and development for detection and prevention of ATM skimming frauds

Sultan Saleem Khalaf Al Hattali, Shaik Mazhar Hussain, Anilloy Frank
Department of Electriconics and Communication Engineering, Middle East College, Oman

Article Info

Article history:

Received May 28, 2019
Revised Jul 30, 2019
Accepted Aug 14, 2019

Keywords:

ATM skimming
FSR sensors
GPS
GSM
OTP

ABSTRACT

ATM Skimming is a major concern that needs to be addressed with a specific solution. ATM Skimming is done in two steps. One is stealing the Personal Information that is stored on the Debit card / Credit card using Rain cover connected to the card reader slot (ATM's real card slot). The second is installing a Fake keypad that can capture the pin code when the card holder enters pin details. Few researchers have proposed solutions to address the issue using Image Processing techniques. However, it does not provide a complete solution in a long term. Hence it is of paramount importance to provide ATM with high security features. In order to solve the issue of ATM Skimming, An Embedded System design is proposed. The research is carried out in two phases. One is detection phase and the second is Prevention Phase. In the detection phase, Hardware components such as Arduino Mega, Force Sensing Resistor (FSR), GPS, GSM and Buzzer are used. Arduino Mega acts as a Central Processor that processes the information received from Force sensing resistor (FSR) and send SMS Messages to ROP and Bank Officials using GSM and informing them about the ATM Location using GPS where the Fraud is taking place. Buzzer can be used at the ATM Locations to alert nearby people. In the prevention Phase, as a preventive measure a Onetime password (OTP) technique is used. If a fraudster somehow succeeds in Fixing fake key pad and Rain Cover at ATM's real card slot, When he tries to insert debit card, An OTP will be generated and is sent to the Card Holder which in turn he can know someone is trying to make Transactions and quickly he can ask bank officials to Block his account and inform ROP about the same. Expected findings of the proposed work is to detect Fake keypads and Fake card readers using FSR placed at the edges of Original Keypad and card reader slot. Sending messages to ROP, BANK OFFICIALS and CARD HOLDER using GSM. ATM locations are identified using GPS. Buzzers are used to alert nearby people.

Corresponding Author:

Shaik Mazhar Hussain,
Department of Electronics and Communication Engineering,
Middle East College (MEC), Muscat, Oman.
Email: mazhar@mec.edu.om

1. INTRODUCTION

ATM skimming is a type of fraud which occurs when ATM machines are deployed with skimming devices such as Rain cover and fake keypad. These devices looks like part of ATM machines.When a user slides through ATM card reader, he is swiping his card through rain cover attached to the card reader slot and when the user types his ATM pin, his finger prints are scanned and used later for misuse. According to the United States federal trade commission the rate of identity theft has been increased to 21 percent in 2008 [1]. ATM Frauds have become a major issue that needs to be addressed to ensure Safe Living in the society. Miscreants and Fraudsters are spread across the world to steal Public Money. Recent Years, Several Cases

have come into existence where the Fraudsters have stolen huge amount of money from ATM Machines through skimming devices. On June 24, 2015 A Fraud activity is published in Times of Oman where Three Europeans were caught stealing money from ATM machines using Forged Debit cards [2]. On May 10, 2013 A Crime gang from US were involved in ATM frauds had stolen US dollar 45 million from RAK bank and bank Muscat [3]. In the same year, another incident On October 31, 2013 took place where three foreigners were caught in ATM Frauds [4, 5] On April 16, 2017 A news was published "Cybercrime on the rise in Oman" in an Article "The National" where a police spokesman has stated Cybercrime frauds have been increased as compared to earlier years mainly in Debit card and credit card frauds [6]. Therefore, it is desperately needed to develop effective and efficient security solutions to avoid ATM Skimming. Security in [7, 8] is defined as measures taken to be safe or protected and hence it is equally important [9, 10]. The development of Advanced Security Systems for ATM machines in Oman can reduce the percentage of ATM Frauds and can increase trust with the banks [11, 12]. Integrating advanced security mechanisms to ATM machines could substantially improve Confidentiality, Authenticity, and Non – Repudiation, Data Integrity and decreases Vulnerability [13, 14]. Several solutions to avoid ATM skimming is proposed using Image Processing Techniques. However, such methods are past and unreliable, since there is a possibility of frauds. Solution to such problem is given by using embedded system devices and OTP methods. Below Figure 1 shows ATM skimming frauds and how the skimmer succeeds in installing fake devices. The proposed research work is organised as follows: Section 2 discusses the existing solutions to avoid ATM Skimming, Section 3 briefly explains research method, expected outputs and design methods, Section 4 will show case the simulation and implementation, Section 5 discusses conclusions and references.

Figure 1. Installation of Rain Cover and Fake Keypad [15]

2. LITERATURE REVIEW

Several research articles have proposed solutions to mitigate ATM Skimming issues [16]. One approach is using Image processing technique to detect the skimming devices captured through surveillance cameras and does processing. However, this method does not provide adequate solution to security as advanced technologies could be used to manipulate cameras [17-20]. Additionally, In real time implementations, sophisticated and advanced surveillance cameras needs to be installed to capture clear details of skimming devices which could be cost effective. In another paper, Monitoring and controlling of ATM machines is proposed using ARM 11 processor and Raspberry pi [21]. However, this method is more confined to Authentication and does not guarantee data integrity and confidentiality [22, 23]. In another article, Anomaly detection on ATM's is proposed using Image processing technique called "Complex Quad-Tree Wavelet Packet transform ". In this work, Occuring Vibrations are captured using piezoelectric sensors. The signals captured is applied to the Complex quad tree wavelet packet transform technique where motifs are detected from where the patterns are extracted for detecting anamolies. However, the approach is more related with ATM machines and does not guarantee Data Integrity and Confidentiality. Additionally, the approach is not transparent to the account holders where they were unaware of the ATM's attacks [24] [25]. The research identifies the level of ATM frauds across the world and proposes a solution to reduce it to the barest minimum. The proposed research is mainly focused on detecting ATM skimming at the initial stages and preventing the frauds to happen at its best. In [26], the research is mainly focussed on providing security to ATM keypads as skimmers can uncover the sequence easily. The authors have showed one of the techniques to attack ATM keypads called acoustic transfer function (ATF). The data is collected using spectrum based techbique. The work proposed is to showcase the recognition possibilities of ATM key pads.

However, the method does not provide any solutions to such problems. In another paper [27, 28], biometric based user recognition is proposed. Basically the work is based on finger print mechanism. The paper does not ensure any security mechanism. The proposed research aims to achieve an efficient way to secure ATM machines from unauthorized transactions to happen. The proposed research is sustainable since the hardware used is cheap, easy to install and transparent to the customers.

3. RESEARCH METHOD

ATM's are the access points for the bank customers to perform transactions from anywhere in the world. The deployment of more ATM terminals could improve the performance of the bank. However, less security could adversely effect the Banks. Adding more security layers to ATM terminals can positively drag the customers to open accounts with a bank that provides High security. The proposed research can contribute immensely to promote marketing banking services in and outside Oman. This research work will improve the ATM service quality towards the Customer Satisfaction in Oman Banking sector. Banks that provide high security features for their ATM machines will attract customers and increases trust towards them. Highly secure banking transactions could directly influence on Customer satisfaction level. The proposed research could subvert the tricks of ATM skimmers. The proposed research will give awareness to young Omani nationals and expatriates on the usage of ATM cards. Development of Intelligent Security System for ATM machines could become an important source of Economy for Financial Institutions like Banks.

The Expected output of the research activity are as follows:

a) Detecting Fake Keypad and Card Readers using Fixed FSR Sensors and sending SMS and ATM locations to the Concerned Bank Officials and nearby Royal Oman Police (ROP) Using GSM and GPS. Buzzer Alarm to alert nearby people
b) Generating One Time Passwords (OTP) when accessing Victim Card Holders account. This will send an SMS Message to Card Holders Registered Mobile Number.
c) Automatically Locking card holder account for 1 Minute if the person fails to enter OTP in 30 Seconds. "This will alert the Card Holder about misuse of his account and can Inform Bank Officials and ROP".

The Proposed Research is intended to develop a Prototype that demonstrates the Design as follows:

a) A sample of three card holder details A, B, C are set up by the bank. There accounts will be initialized by the bank. In our design we use Bank, ATM machine and a Router for communication between them. The bank is a data base created using server programming languages where the details of three sample card holders will be stored. The hardware setup is fixed in ATM machine. Router is the communication medium between ATM machine and Bank.
b) Force Sensitive Resistors (FSR) are fixed at each corner of ATM Keypad and Card reader slot. When the fraudster tries to fix Fake keypad/card reader, FSR could be able to detect and send signals to Arduino.
c) GSM module interfaced to "Arduino" sends SMS Messages to predefined Contacts like Card Holder, nearby ROP and Bank Officials to take necessary steps.
d) GPS Module to detect ATM locations
e) Buzzer is interfaced to alarm in case of detecting Theft.
f) When the fraudster tries to access using Fake card reader, An OTP is generated and sent to Card Holder.
g) The user has to enter OTP pin in 30seconds otherwise the Card holder Account is automatically locked for 1 minute. This is repeated till 3 attempts and then the card holder account is locked for the complete day.

4. RESULTS AND DISCUSSIONS

This section briefs on simulation results and hardware implementation. The proposed work is based on providing security for ATM users by sending OTP messages, location details and alerting account holder and bank. Force sensitive sensors are placed beneath the ATM keypads. The prototype developed shows different cases when a skimmer tries to steal owners account details. The results obtained has shown different outputs. One is if the skimmer tries to install fake keypads, the FSR will identify its pressure and communicates to owner using GSM and GPS. In the second scenario, even if skimmer was succeeded in installing fake keypads and rain cover, the skimmer when tries to access owners account an OTP is sent to the account holder through which he can know someone is trying to access his account and inform the bank officials immediately. The third scenario is the user has to enter OTP pin in 30seconds otherwise the Card holder Account is automatically locked for 1 minute. This is repeated till 3 attempts and then the card holder account is locked for the complete day. These three different scenarios are integrated and simualted in our

proposed work and proves to be the best possible solutions to avoid ATM skimming as compared to the existing techniques where the researchers have used image processing techniques to capture the images of additional devices attached to the ATM machine. However, Image processing techniques might not be an accurate solution as the the software has to know the exact pattern and sizes of skimming devices which in other case the cameras could not capture correctly.

4.1. Simulation Results

The project work is simulated in PROTEUS ISIS 8. The figure shows simulation results for different cases as listed below.

1) Figure 2 shows welcome message
2) Figure 3 shows the message to swipe debit card
3) Figure 4 shows the person swiped the debit card and password entered
4) Figure 5 shows that the password is correct
5) Figure 6 GSM, GPS and IR sensor is interfaced. GPS gives location details, GSM sends messages to registered mobile number incase of misuse and IR sensors to detect when skimme tries to insert rain cover / fake keypad. IR sensor is used only in simulation whereas Force sensitive resistor (FSR) is used in real implementation.
6) Figure 7 Virtual terminal displays location, messages.

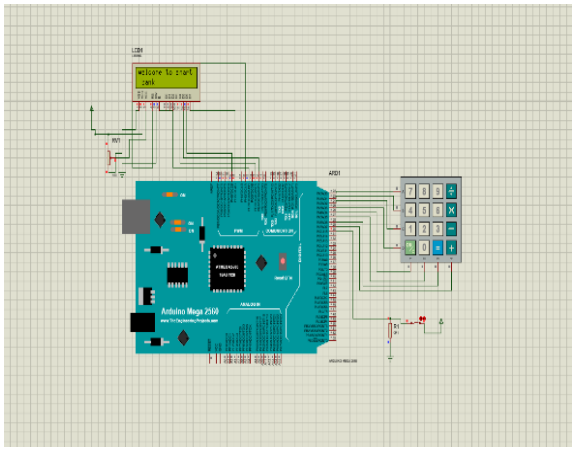

Figure 2. Welcome message

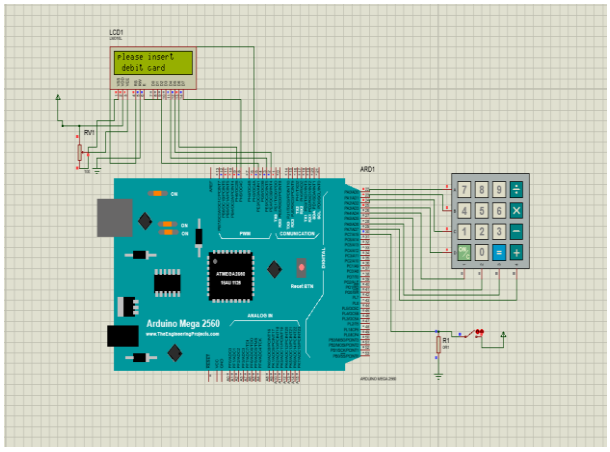

Figure 3. Swipe debit card

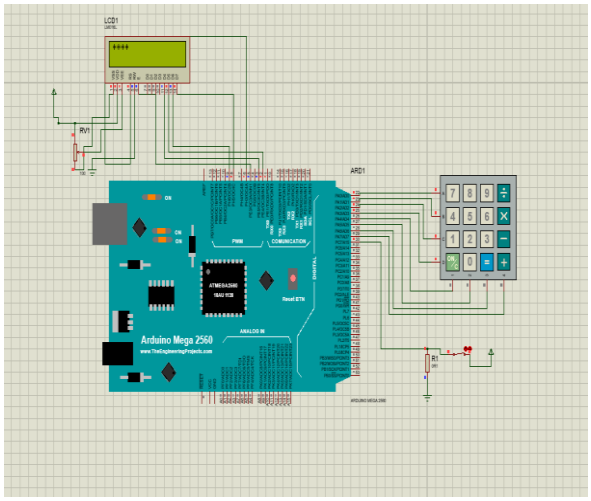

Figure 4. Person swiped the debit card and the password is entered

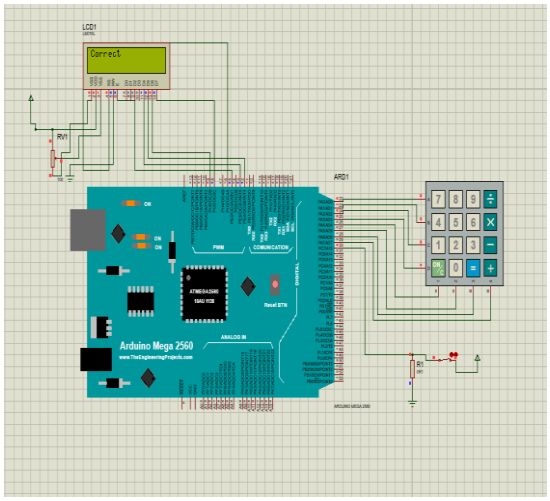

Figure 5. Password is correct

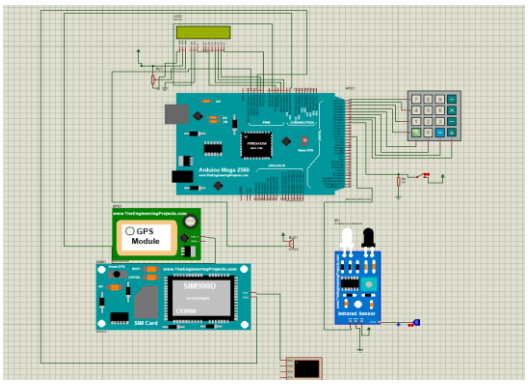

Figure 6. GSM, GPS and IR sensor is interfaced

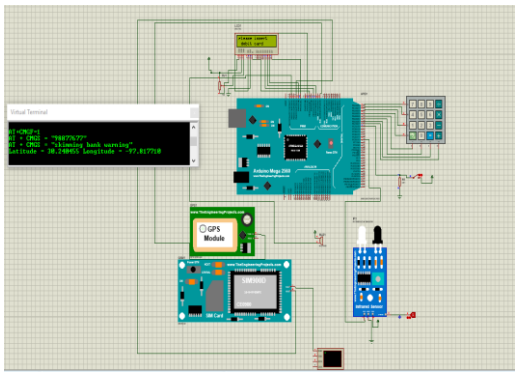

Figure 7. Virtual terminal displays location, messages

4.2. Hardware Implementation

The project work is implemented using basic bread boards and other components. The components/devices that are used for the design are listed:

a) Arduino Mega
b) Force Sensitive Resistor (FSR)
c) GPS
d) GSM
e) Keypad
f) LCD

The programming is done using C. The below figure shows different cases of the project

1) Figure 8 shows welcome message
2) Figure 9 shows enter password message
3) Figure 10 shows blocked message when password entered is incorrect
4) Figure 11 shows account bloked status
5) Figure 12 shows location and OTP is sent to owners mobile when correct password is entered

Figure 13 shows the final prototype called SMART BANK system.

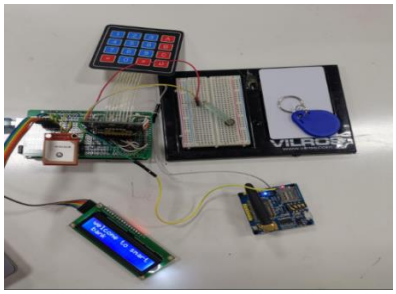

Figure 8. “Welcome to smart bank”

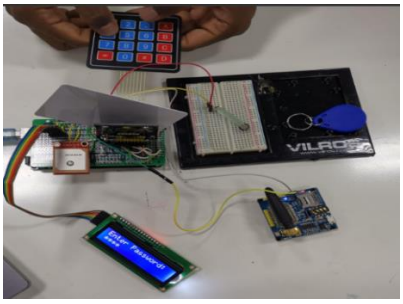

Figure 9. Enter password

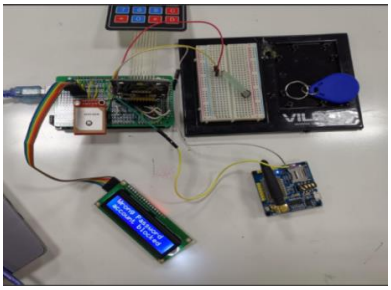

Figure 10. Wrong password for 3 attempts

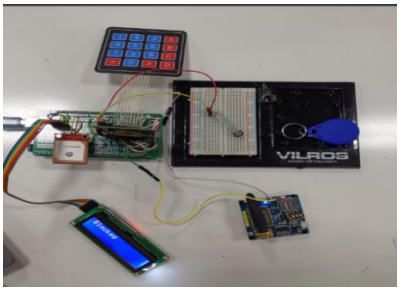

Figure 11. Blocked in case of

- Account blocked entering wrong password

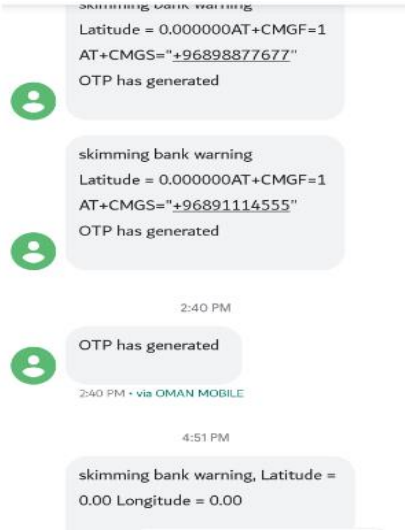

Figure 12. Location and OTP is sent to card holders account. When correct password is entered

Figure 13. SMART BANK to avoid ATM Skimming

The above figure shown is displayed in owners mobile. This is the case when skimmer tries to access owner's account by entering ATM pin. In this case, an OTP is generated and the location details is sent to owners registered mobile number.

5. CONCLUSION

In this work, a prototype is designed for detecting and preventing ATM skimming. The proposed system will avoid skimmers from misusing card holders account.The system uses ARDUINO MEGA as a processor which controls all other devices and processes the input data and generates output.The device works in a more sophisticated way to resolve the issue of ATM skimming in real time which has proven to be the major concern across the world. The system uses Force Sensitive Resistor (FSR) placed beneath the keypad which converts pressure in to electrical quantities that will be processed by ARDUINO MEGA and sends SMS and location information using GSM and GPS to card holders and bank officials. The proposed system can be used as a commercial tool for ATM monitoring, detecting and preventing from skimming.

ACKNOWLEDGMENT

I would like to thank Middle East College (MEC) for all time support in encouraging to research on hot issues of these days.

REFERENCES

[1] "Federal Trade Commision," February 2009. [Online]. Available: https://www.ftc.gov/sites/default/files/documents/reports_annual/sentinel-cy-2008/sentinel-cy2008.pdf. [Acesso em 13 5 2019].
[2] T. o. Oman, "Oman jails four over credit card fraud," Times of Oman, 13 march 2014. [Online]. Available: https://timesofoman.com/article/31587. [Acesso em 12 05 2019].
[3] C. Prabhu, "Got scammed? It can be ages before your bank reimburses you!," Oman Observer, 4 4 2018. [Online]. Available: Got scammed? It can be ages before your bank reimburses you!. [Acesso em 12 5 2019].
[4] H. Y. K. G. S. Faria, "Identification of Pressed Keys From Mechanical Vibrations," *IEEE T. Information Forensics and Security*, vol. 8, nº 7, pp. 1221-1229, 2013.
[5] B. Omar, "Times of Oman," Times of Oman, 2 july 2016. [Online]. Available: https://timesofoman.com/article/87279. [Acesso em 12 5 2019].
[6] K. Yusof, "ROP warns against fake messages on ATM cards," Oman Observer, 12 May 2019. [Online]. Available: http://www.omanobserver.om/rop-warns-against-fake-messages-on-atm-cards/. [Acesso em 12 5 2019].
[7] A. Khanum e Rekha, "An enhanced security alert system for smart home using IOT," *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 13, nº 1, pp. 27-34, 2019.

[8] S. F. A. S. F. M. Y. F. Trio Adiono, "Curtain Control Systems Development on Mesh Wireless Network of the Smart Home," *Bulletin of Electrical Engineering and Informatics,* vol. 7, nº 4, pp. 615-625, 2018.
[9] G. d. S. Faria e H. Y. Kim, "Identification of Pressed Keys by Acoustic Transfer Function," em *2015 IEEE International Conference on Systems, Man, and Cybernetics*, Kowloon,China, 2015.
[10] R. o. M. B. I. U. H. F. a. Face, "Sampada A Dhole, V H Patil," *Buletin Teknik Elektro dan Informatika,* vol. 1, nº 3, pp. 179-184, 2012.
[11] A. W. A. Y. Y. Berger, "Dictionary attacks using keyboard acoustic emanations," em *Proc. 13th ACM Conf. Computer and Communications Security*, 2006.
[12] M. M. E. Raj e A. Julian, "*Design and implementation of anti-theft ATM machine using embedded systems*," em 2015 International Conference on Circuits, Power and Computing Technologies [ICCPCT-2015], Nagercoil, India, 2015.
[13] T. K. M. Wax, "*Detection of signals by information theoretic criteria*," IEEE T. Acoustics Speech and Signal Processing, vol. 33, nº 2, pp. 387-392, 1985.
[14] P. P.Borade, R. b. e V. salunkhe, "Design and Implementation of Security Based Atm Theft Monitoring System," *JETIR,* vol. 4, nº 3, pp. 166-168, 2017.
[15] B. Starzee, "staying ahead of the theives," [Online]. Available: https://libn.com/2018/01/15/staying-ahead-of-the-thieves/. [Acesso em 16 7 2019].
[16] S. M. H. K. M. Y. S. A. H. A. V. S. Naji Taaib Said Al Wadhahi, "*Accidents Detection and Prevention System to reduce Traffic Hazards using IR Sensors*," em 2018 7th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions)(ICRITO), New Delhi ; India, 2018.
[17] C. R. R. A. S. A. N. R. V. Shaik Mazhar Hussain, "*An RFID based smart EVM system for reducing electoral frauds,*" em 2016 5th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions)(*ICRITO),* New Delhi ; India, 2016.
[18] B. Deshpande e D. Jayaswal, "*Fast and Reliable Biometric Verification System Using Iris,*" em *2018 Second* International Conference on Inventive Communication and Computational Technologies (ICICCT), Coimbatore;India, 2018.
[19] S. J. M. R. A. S. Drimer, "Thinking inside the box: system-level failures of tamper proofing," *Proc. IEEE Symp. on Security and Privacy*, pp. 281-295, 2008.
[20] M. M. K. A. Rawahi e S. S. K. Nair, "*Detecting Skimming Devices in ATM Through Image Processing,"* em *2015* IEEE/ACS 12th International Conference of Computer Systems and Applications (AICCSA), Marrakech, Morocco, 2015.
[21] S. M. H. K. M. Y. S. A. H. A. V. S. Zahir bin Sulaiman Al Brashdi, "*IoT based Health Monitoring System for Critical Patients and Communication through Think Speak Cloud Platform*," em 2018 7th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions)(ICRITO), New Delhi ; India, 2018.
[22] S. I. Manzoor e A. Selwal, "*An Analysis of Biometric Based Security Systems*," em 2018 Fifth International Conference on Parallel, Distributed and Grid Computing (PDGC), Solan Himachal Pradesh, India, India, 2019.
[23] D. Narmada e J. V. Priyadarsini, "*Design and implementation of security based ATM using ARM11*," em 2016 International Conference on Inventive Computation Technologies (ICICT), Coimbatore, India, 2016.
[24] A. V. H. C. P. T. P. Marquardt, *"(sp)iPhone: decoding vibrations from nearby keyboards using mobile phone accelerometers,*" em Proc. 18th ACM Conf. on Computer and Communications Security, 2011.
[25] S. Torkamani, A. Dicks e V. Lohweg, "*Anomaly detection on ATMs via time series motif discovery*," em 2016 IEEE 21st International Conference on Emerging Technologies and Factory Automation (ETFA), BERLIN, GERMANY, 2016.
[26] G. d. S. Faria e H. Y. Kim, "*Identification of Pressed Keys by Acoustic Transfer Function*," em 2015 IEEE International Conference on Systems, Man, and Cybernetics, Kowloon, China, 2015.
[27] E. P. Kukula, M. J. Sutton e S. J. Elliott, "The Human–Biometric-Sensor Interaction Evaluation Method: Biometric Performance and Usability Measurements," em *IEEE Transactions on Instrumentation and Measurement*, 2010.
[28] E. D. Dimaunahan, A. H. Ballado, F. R. G. Cruz e J. C. D. Cruz, "*MFCC and VQ voice recognition based ATM security for the visually disabled*," em 2017IEEE 9th International Conference on Humanoid, Nanotechnology, Information Technology, Communication and Control, Environment and Management (HNICEM), Manila, Philippines, 2017.

BIOGRAPHIES OF AUTHORS

Mr.Sultan Al Hattali, Department of Electronics and Communication Engineering. He is a Graduate student at Middle East College(MEC). His research areas include IOT.

Mr. Shaik Mazhar Hussain, Department of Electronics and Communications Engineering received his Master's degree in Embedded System from India in 2012 and received PGCert from Coventry University, UK in December 2017, Certified in Digital Circuits and Systems from IIT Madras. He is currently a Ph.D candidate at the Universiti Teknology Malaysia (UTM), Johor Bahru, Malaysia. His Research areas of interest include Wireless Communications and intelligent transportation system (ITS)

Dr.Anilloy Frank, Department of Electronics and Communication Engineering received his Ph.D from Graz University of technology, Austria. He is a Co-Founder and System Architect at Frank Vision Computer Technologies Pvt.Ltd. He has 30 years of teaching experience. He is life member of Indian Society for technical education (ISTE) and ECQA certifed Functional Safety Manager. His Research areas of Interest include Embedded Systems and IOT.