RESEARCH
O&G Forum 2024; 34 – 2s: 130 - 134

VARIED PIN ENTRY SYSTEM USING DYNAMIC PASSWORD

Shailesh M.[1], Varunsevvel M[2], Srivarsan S.[3], Suriya Prakash N.[4]
[1] Student, Computer Science and Engineering, Sri Krishna College of Technology, Coimbatore, India.
20tucs216@skct.edu.in
[2] Student, Computer Science and Engineering, Sri Krishna College of Technology, Coimbatore, India.
20tucs247@skct.edu.in
[3] Student, Computer Science and Engineering, Sri Krishna College of Technology, Coimbatore, India.
21tucs801@skct.edu.in
[4] Student, Computer Science and Engineering, Sri Krishna College of Technology, Coimbatore, India.
21tucs802@skct.edu.in

Abstract
The current technological enhancements are consistently paving the way towards the ease of approach to the information, things or people via the combination of technology, gadgets and their regular updates. The motivating factor in this research work is the need and search for an optimized and effective security enhancement mechanism and system for duress cash withdrawals cases at ATM. Every time a client enters an ATM and inserts a card, an automated four-digit code, similar to an OTP, is created and sent as a message to the authorized consumer's mobile device via the GSM modem connected to the microcontroller. The user can then proceed with the transaction after entering the combination of PIN and OTP they got by hitting the keys on the screen of the system or on a web application.
Keyword: ATM, OTP, IoT, Sensors, GSM, Security.

INTRODUCTION

The requirement of safe and secure transaction is one of the foremost needs of every any organization, group or an individual. In current era, people expect a hassle free and least time consuming system for such activities. With the increasing demands of fast, secure and reliable monetary transaction systems by public, the government and private organization has made several efforts to fulfill the public needs. Many tools and programmes have been developed and put into use to meet the need for quick and safe automated financial transactions. In addition, various modes of performing monetary transactions are made available to enable a prompt mobilization of cash physically or electronically. The Automated Teller Machine is one among them.

In ATMs, the clients are recognized and authorized to access their accounts through a special plastic card issued from organizations to them. Some unique identifiers like magnetic stripe or chip carrying client's unique card number or information, issue date, expiry date and Card Verification Value (CVV) are added to this card to make it secure and protected from unauthorized access to anyone's account [1][2]. In addition to the security measures through ATM card, a secret code known as Personal Identification Number (PIN) is also required for accessing account by a customer to perform his financial transactions or enquiries [3]. An authorised ATM user enters their Personal Identification Number (PIN), which is provided by the ATM and banking authorities, to begin a transaction using the ATM's user interface. Through the communication network between the ATM and the banking financial network, the customer's input PIN is then compared, validated, and confirmed in accordance with the bank's recorded PIN of reference.

ATMs, like other technical innovations, have two sides: they are convenient, but they also raise security risks. The duress cash withdrawal is a kind of indirect bank robbery and physical attack on ATM, but done through an ATM card holder on a gunpoint or life threatening physical pressure. The ATM card holder withdraws cash from ATM and bears the financial loss. The victim is left with no option other than simply reporting the attack to security officials when he comes out from the grip of the attackers. Nowadays, the cases of duress cash withdrawal are hiking, may be reported or may be left unreported many times due to security issues faced by the victim. The physical and financial insecurity of the customer is a serious problem of real world which could happen with any ATM user. Thus, there is a need of enhancement of the security system of ATM to deal with such physical attacks.

RELATED WORKS

Jaiswal A. M., Bartere M., [14], an ATM application system, specifically for security concern is proposed. As part of the plan, bankers were required to get the mobile number and finger prints of new customers when they opened accounts. Every time a client enters an ATM and inserts a card, he must place his finger on the finger print module. After that, an automated four-digit code, similar to an OTP, is created and sent as a message to the authorised consumer's mobile device via the GSM modem connected to the microcontroller. The user can then proceed with the transaction after entering the OTP they got by hitting the keys on the screen of the system.

No single security technique, algorithm, key, or procedure is said to be completely safe in the work by Lasisi H. et al. [21]; rather, a combination of many security complements is required to provide a high degree of protection against threats and scams.

The idea combined two security implementations: fingerprint recognition for one and magnetic stripe cards for the other. The vulnerabilities of PINs, passwords used for ATMs, and magnetic-stripe card verification were examined. In contrast to the PIN and magnetic stripe card authentication approach, the paper suggested a framework for user identification and authentication in ATMs utilizing fingerprints and magnetic stripe cards.

The creation and use of a low-cost ATM with currency exchange capabilities known as a Hybrid ATM (H-ATM), which combines currency exchanging capabilities with standard money transaction facilities, is described in a paper presented by Iqbal A., Shabnam F., et al. [23]. It is suggested that H-ATM, which can perform common tasks, be equipped with a more sophisticated system that combines an embedded microcontroller system with a computer. This cutting-edge technology has demonstrated notable gains in cost-effectiveness, performance, and troubleshooting while maintaining a greater degree of security and consistency.
A Real Time Instructive SMS-Based scheme dubbed MophTem system, which encourages all customers to subscribe to SMS alerts as a source for starting transactions on their account, is introduced in the article presented by Onwudebelu, U., et al. [27]. Using the customer's contact information and Personal Identification number, the bank generates a hash code. The information requested for transactions from the customer is decrypted using this hash key. The goal is to strengthen current PIN access and add another layer of protection to protect client accounts and account information.

In a paper given by Zajac P. et. al. [31], the performance estimation measure for multicore processors is discussed. The researchers analyzed major trends to increase the computing performance in current processors and found that the computing performance is based on adding more and more cores on chip. The researcher investigated the impact of faults on multicore processor performance, under the assumption, that a faulty core or router on chip is detected and either repaired, replaced or disabled, according to suitable fault-tolerant mechanism. Diverse fault-tolerant techniques are also analyzed. A, 4×4 mesh multicore processor to measure the performance penalty is simulated. The study will help us in directing and finding the nano-chip performance factor for the proposed security system.
The patent of Susann M. K., et. al. [46], introduced the system which involves in the controlling of electronic withdrawals by a drawee by introducing a special withdrawal request originated from withdrawee. It is suggested and has an identification for the withdrawal device, a drawer, and a withdrawal amount. The maximum withdrawal amount, withdrawal duration, and withdrawal type are the only restrictions on electronic withdrawals; the drawer location is not included in the system. The researcher suggested common implementations, such as restricting the position of drawers to a region that includes one or more withdrawal device sites. This study gives insight into an interesting way to enhance monetary security of ATM's customers.

SYSTEM ARCHITECTURE

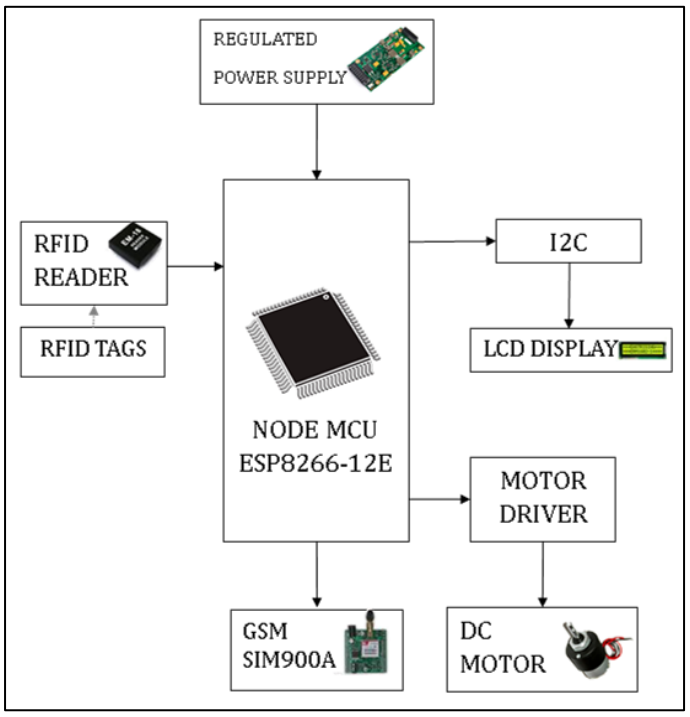

Figure 1 System Architecture

a. NodeMCU Esp8266
NodeMCU [5] Esp8266 is an low-cost open source IoT platform. Its original hardware components were ESP-12 modules and firmware based on the ESP8266 Wi-Fi SoC [6]. The NodeMCU Dev Kit/Board includes the ESP8266 WiFi chip. The TCP/IP protocol is used by Espressif Systems' low-cost ESP8266 Wi-Fi chip. To learn more about the ESP8266, use the WiFi Module. The NodeMCU microcontroller and development board are designed primarily for Internet of Things-related purposes.

b. RFID Tag
A location tracking system uses RFID, or radio frequency identification, to follow the object, and cloud computing speeds up calculations while lowering hardware costs. A transponder or tag is attached to the luggage so that it may be tracked within the museum. When the tag comes into close proximity with the reader or integrator, it activates. An RFID passive tag consists of an antenna coil, nonvolatile memory, basic modulation circuitry, and an integrated semiconductor chip. A transponder or tag is affixed to the luggage in order to track it within the museum. When the tag is near the reader or integrator, it becomes active. An RFID passive tag consists of an integrated electronic chip and an antenna coil that includes non-volatile memory and basic modulation circuitry. Furthermore, the impact of various offset angles on tag read rates was investigated. The findings indicate that the reading rate reduces as the offset angle rises. The effective recognition angle is around 60 degrees, and the impact is optimal at 45 cents. When the reading rate reaches 75 cents, it dramatically drops. To ensure their authenticity, there are consequently precise rules regarding the positioning of cultural artefacts and reading perspectives.

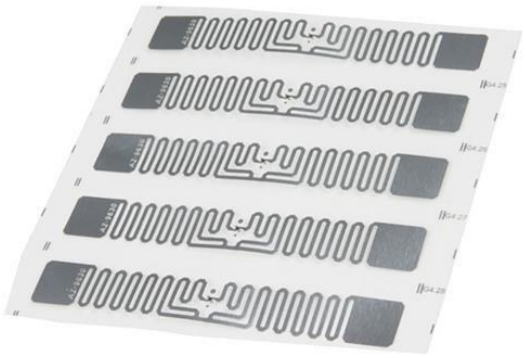

Figure 2 RFID Tag

c. EM18 RFID Reader
It is an RFID reader that operates at a 125 kHz frequency to read tags. After reading tags, it connects to the appropriate pins on the PC or microcontroller using Wiegand format or UART to send a serial unique ID. The EM18 RFID reader can read data from RFID tags with stored IDs that are 12 bytes long. The EM18 RFID reader does not require line-of-sight to operate. Additionally, it only has a few centimeters of identification range.

Figure 3 EM18 RFID Reader

d. GSM
The primary global mobile standard and the communications technology with the highest rate of growth is GSM. From the perspective of the mobile operator, a GSM modem is similar to a cell phone. A computer may use the mobile network for communication when a GSM modem is attached. Although many of these GSM modems can also send and receive SMS and MMS messages, they are frequently used for mobile internet access. A mobile phone with GSM modem functionality can also function as a standalone modem via USB, Bluetooth, or serial connection.

Figure 4 GSM Module

e. DC Motor
A DC motor is an electrical device that uses direct current's magnetic field to transform electrical energy into mechanical energy. Turning on a direct current motor produces a magnetic field in the stator. Due to the magnets on it being attracted to and repelled by the magnetic field, the rotor rotates. To maintain the rotor rotating continuously, the motor's wire windings get power from the commutator, which is linked to brushes attached to the power supply. Next, NodeMCU utilizes the signal to drive the little servo motor, which opens and closes the door based on distance measurement. NodeMCU code is used for the same.

Figure 5 DC Motor

f. 12V Power Supplies
The 12V (or 12VDC) supply is one of the most widely utilised power sources available today. To convert a 120VAC or 240VAC input into a 12VDC output, a transformer, diode, and transistor combination is frequently used. The two different forms of 12V power sources are regulated and uncontrolled power supplies. Furthermore, in an acopian switching regulated power supply, substantial EMI filtering and shielding are employed to minimise noise transmitted to the line and load in both common and differential modes. The system's power source, represented by the power supply block in the diagram, steps down the voltage from 230V to 5V in order to provide the system with the vital power it needs. The voltage is then further passed to the remaining system blocks after being stepped down to 5V.

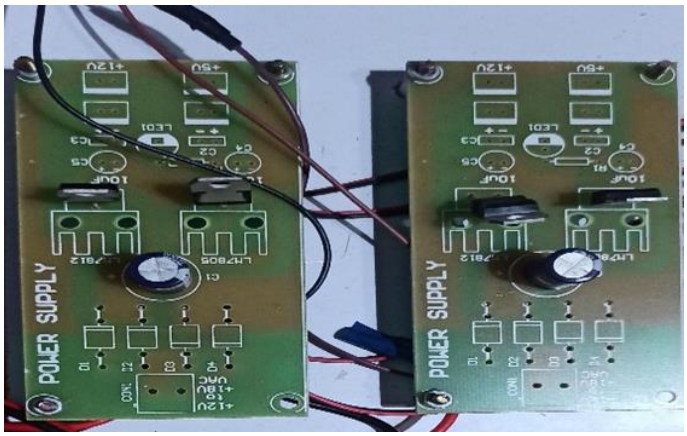

Figure 6 Power Supply

g. LCD
LCD module at 40% relative humidity and 40% temperature, respectively. Higher temperatures can cause the display's overall colour to alter, while lower temperatures can delay the rate at which the display blinks. When the temperature drops within the designated range, the display will normalize. Polarizer peel-off, bubble formation, and polarization deterioration can all be brought on by heat and humidity.

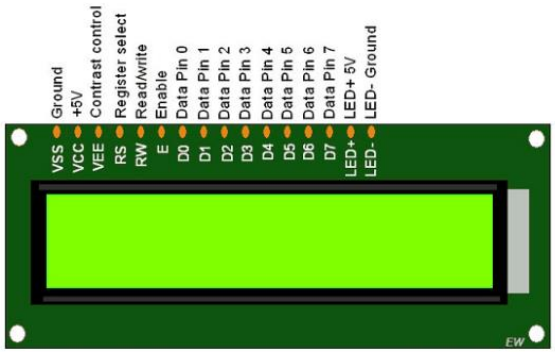

Figure 7 LCD Display

Proposed System

The components of the current system include issues with modern ATMs, such as solder surfing attacks and pin stealing via pinhole cameras. Additionally, there's a chance that kids will use money to purchase undesired items.

In order to overcome them, the pin and OTPP combing procedures, which alter the real pin value each time a withdrawal or deposit is made, hence lowering the likelihood of pin theft. Additionally, by connecting a parental account and sending a request to that account each time an ATM is used, parents may limit their children's access to money by utilizing the remote pin entering technique with the assistance web app. Moreover, solder surfing and pinhole monitoring are less likely with this remote pin insertion.

SHA-1 algorithm for OTP Generation

A cryptographic hash function in the field of cryptography is called SHA-1; SHA stands for Secure Hash Algorithm. SHA-1 is the most widely used hash algorithm currently in use, and it may be found in many well-known security applications and protocols. With a more conservative design, SHA-1 creates a 160-bit message digest using concepts that are comparable to those used by Ronald L. Rivest of MIT to create the MD4 and MD5 message digest algorithms. Many widely used security programmes and protocols make use of SHA-1. The SHA 1 method was used in this endeavour to produce the OTP. To generate the OTP code, it needs two inputs: a moving factor and a seed. When you register for a new account on the authentication server, a static value (secret key) known as the seed is produced. To protect OTP creation, the SHA 1 algorithm employs a variety of encryption mechanisms such as position exchange and bit shifting, as well as keys and weights applied over several rounds.

EXPERIMENTAL RESULTS

This work used HTML, CSS and PHP, mySQL for creating the web page.

Figure 8 RFID Tag

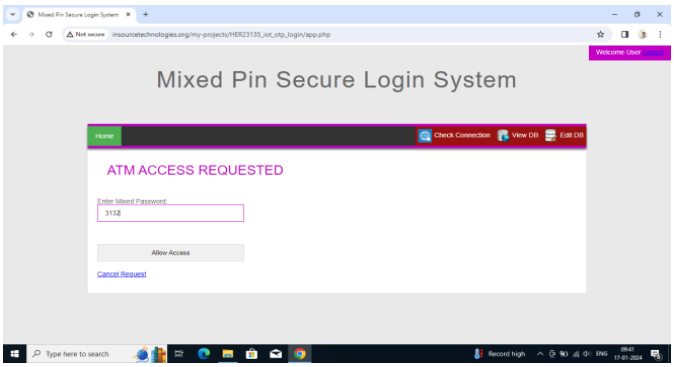

Figure 9 Mixed Pin Secure Login System

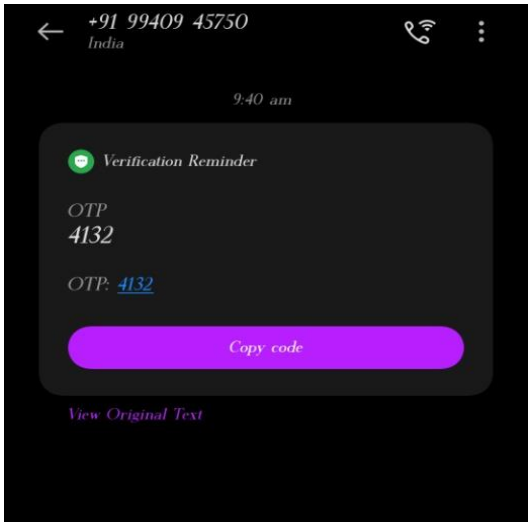

Figure 10 OTP Received to the User Registered Mobile Number

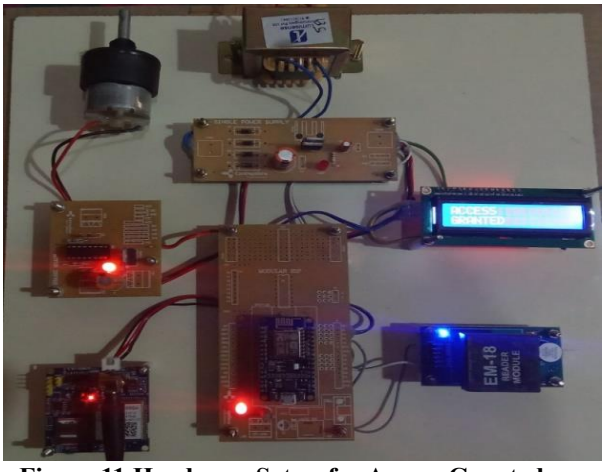

Figure 11 Hardware Setup for Access Granted

CONCLUSION

ATMs are placed in public areas, and both the user's and the banking system's security must be very strong. Although research on a variety of security measures has been put into practice, more effort is still needed to find solutions for issues like forced or duress cash withdrawals. The anticipated Internet of Things (IoT)-based automated teller machine (ATM) system is anticipated to offer a practical and cost-effective means of compensating users for their financial losses, alleviate anxiety in high-stress situations, and enable the tracking of cash and perpetrators even after they have managed to flee the scene of the crime.

References

1. *ApurvaTaralekar, GopalsinghChouhan, RutujaTangade, NikhilkumarShardoor, "One Touch Multi-banking Transaction ATM System using Biometric and GSM Authentication", International Conference on Big Data, IoT and Data Science (BID) ,Vishwakarma Institute of Technology, Pune, pp.61-68, Dec 20-22,2017*
2. *D. Venkatesh and M. Rakhra, "Agile adoption issues in large scale organizations: A review," Mater. Today Proc., no. xxxx, 2020, doi: 10.1016/j.matpr.2020.11.308.*
3. *G. B. Iwasokun, Development of a Hybrid Platform for the Pattern Recognition and Matching of Thumbprints, PhD Thesis , Department of Computer Science, Federal University of Technology, Akure, Nigeria, 2012*
4. *G. S. Panesar, D. Venkatesh, M. Rakhra, K. Jairath, and M. Shabaz, "Agile software and business development using artificial intelligence," Ann. Rom. Soc. Cell Biol., vol. 25, no. 2, pp. 1851–1857, 2021.*
5. *Jong-Hoon Kim, Gokarna Sharma, Irvin Steve Cardenas, Do Yeon Kim, NagarajanPrabakar, S.S.Iyengar, "DynamicPIN: A Novel Approach towards Secure ATM Authentication", International Conference on Computational Science and Computational Intelligence, pp. 69- 73,2017.*
6. *Jong-Hoon Kim, Gokarna Sharma, Irvin Steve Cardenas, Do Yeon Kim, NagarajanPrabakar, S.S. Iyengar,"DynamicPIN: A Novel Approach towards Secure ATM Authentication", International Conference on Computational Science and Computational Intelligence, pp. 69-73,2017*
7. *Karovaliya, M., Karedia, S., Oza, S., & Kalbande, D. R. (2015). Enhanced security for ATM machine with OTP and Facial, Procedia - Procedia Comput. Sci., 45, (pp. 390-396).*
8. *Kavitha V, Dr.G.UmaraniSrikanth, "Moving ATM Applications to Smartphones with a Secured Pin-Entry Methods", IOSR Journal of Computer Engineering (IOSR-JCE), Volume s17, Issue 1, pp. 58- 65, Ver. II (Jan–Feb.2015).*
9. *Kavitha V, Dr.G.UmaraniSrikanth, "Moving ATM Applications to Smartphones with a Secured Pin-Entry Methods", IOSR Journal of Computer Engineering (IOSR-JCE), Volume 17, Issue 1, pp. 58-65, Ver. II (Jan– Feb.2015)*
10. *M. Arora et al., "Agile Umbrella Methodologies and its Global Impact Introduction to Scrum," vol. 25, no. 4, pp. 2990–3003, 2021.*
11. *M. Rakhra and R. Singh, "Materials Today : Proceedings A study of machinery and equipment used by farmers to develop an uberized model for renting and sharing," Mater. Today Proc., no. xxxx, 2020, doi: 10.1016/j.matpr.2020.11.784.*
12. *M. Rakhra and R. Singh, "Materials Today : Proceedings Smart data in innovative farming," Mater. Today Proc., no. xxxx, 2021, doi: 10.1016/j.matpr.2021.01.237.*
13. *M. Rakhra et al., "Materials Today : Proceedings Crop Price Prediction Using Random Forest and Decision Tree Regression : -A Review," Mater. Today Proc., no. xxxx, 2021, doi: 10.1016/j.matpr.2021.03.261.*
14. *M. Rakhra, R. Singh, T. K. Lohani, and M. Shabaz, "Metaheuristic and Machine Learning-Based Smart Engine for Renting and Sharing of Agriculture Equipment," vol. 2021, 2021.*
15. *M.Hindusree, Dr.R.Sasikumar, "Preventing Shoulder Surfing in Secure Transactions", International Conference on Computing and Communications Technologies (ICCCT'15), pp. 160 -`163,2015*
16. *Mr.YogeshKisanMali, Ms. ArtiMohanpurkar, "Advanced Pin Entry Method By Resisting Shoulder Surfing Attacks", International Conference on Information Processing (ICIP) Vishwakarma Institute of Technology, pp, 37-42, Dec 16-19,2015*
17. *Ms.Ojaswi K. Kasat, Dr.Umesh S. Bhadade, "Revolving Flywheel PIN Entry Method to Prevent Shoulder Surfing Attacks", 3rd International Conference for Convergence in Technology (I2CT), pp.1-5, Apr 06-08, 2018*
18. *Mun-Kyu Lee, "Security Notions and Advanced Method for Human Shoulder-Surfing Resistant PIN-Entry", IEEE transactions on information forensics and security, vol. 9, no.4, pp. 695 -708, April 2014.*
19. *Mun-Kyu Lee, "Security Notions and Advanced Method for Human Shoulder-Surfing Resistant PIN-Entry", IEEE transactions on information forensics and security, vol. 9, no.4, pp. 695 -708, April2014*
20. *Nilesh Chakraborty, Smart Mondal, "Color Pass: An Intelligent User Interface to Resist Shoulder Surfing Attack", Proceeding of the 2014 IEEE Students' Technology Symposium, pp. 13 – 18, 2014.*
21. *NileshChakraborty, SamratMondal,"Color Pass: An Intelligent User Interface to Resist Shoulder Surfing Attack", Proceeding of the 2014 IEEE Students' Technology Symposium, pp. 13 – 18,2014*
22. *Rasib Khan, RagibHasan, and JinfangXu, "SEPIA: Secure-PINAuthentication-as-a-Service for ATM using Mobile and Wearable Devices", 3rd IEEE International Conference on Mobile Cloud Computing, Services, and Engineering, pp. 41-50,2015*
23. *S.Priyadharshini, Mrs.R.Kurinjimalar, "security enhancement in automated teller machine", International Conference on Intelligent Computing and Control (I2C2) 2017.*
24. *ShwetaSankhwar, "A Safeguard Against ATM Fraud", IEEE 6th International Conference on Advanced Computing, pp. 23-27, May 2016.*
25. *Sweta Singh, Akhilesh Singh, Rakesh Kumar "A Constraint-based Biometric Scheme onATM and Swiping Machine", In International Conference on Computational Techniques in Information andCommunication Technologies (ICCTICT), pp. 45-49, September 2016.*
26. *T. Kwon and S. Na, "SwitchPIN: Securing smartphone PIN entry with switchable keypads," in Proc. IEEE Int. Conf. Consumer Electron, pp. 27–28,2014*
27. *T. Kwon, S. Shin, and S. Na, "Covert attentional shoulder surfing: Human adversaries are more powerful than expected," IEEE Trans. Syst., Man,Cybern., Syst., vol. 44, no. 6, pp. 716–727,Jun.2014.*
28. *Taekyoung Kwon, Member, IEEE, and Jin Hong, "Analysis and Improvement of a PIN-Entry Method Resilient to Shoulder-Surfing and RecordingAttacks", IEEE transactions on information forensics and security, vol. 10, no. 2, pp. 278-292, February 2015*
29. *Taekyoung Kwon, Sarang Na, "SteganoPIN: Two-Faced HumanMachine Interface for Practical Enforcement of PIN Entry Security", IEEE Transactions On Human Machine Systems, vol. 46, pp. 314-317, September 2016.*