

INTEGRATION OF TRIANGULAR LOCATION DETECTION, IOT, OPEN CV - USER AUTHENTICATION FOR SECURED ATM.

Gomathi.D¹,Hameetha Banu.K²,Mahalakshmi.M³,S.Panimalar⁴

⁴S.Panimalar ,Assistant Professor, Dept. of Computer Science & Engineering, Panimalar Institute Of Technology, Chennai,Tamilnadu, India

Abstract-The Open CV for Utilizer Signature like pattern Apperception is implemented. The implementation is deployed for ATM Loading Conveyance.It is deployed with 3 Zigbees, one is affixed with Conveyance, another is with the Mobile phone of the Ascendancy and the last one is with the ATM Machine. Once all the Zigbees meet together, which denotes conveyance is at the ATM, and then OTP is engendered and Verified by ATM Zigbee via Conveyance Zigbee.Apart from OTP, Utilizer Signature is verified utilizing Open CV after loading cash into the ATM Machine.

Keywords—Automated Teller Machine (ATM), Zigbee,One Time Password (OTP),Utilizer Signature,open CV.

1. INTRODUCTION

Automated Teller Machines (ATM) today have become areas of target due to their facile and yarely available cash at everyone's accommodation. The assailments on ATM's are steadily elevating and this is an earnest quandary for law enforcement and banking sectors. So there has to be a system developed and put into place that will ascertain the ATM is safeguarded and additionally gives customers the confidence when utilizing the ATM. Currently to provide bulwark to the ATM and to the customers utilizing it, there are CCTV security cameras and emergency sirens. Other measures that are being researched includes a system that implements a low cost standalone embedded web server, Machine to Machine (M2M) and RFID to implement an anti-larceny system, in case there is an intruder in the ATM kiosk a system with image processing capabilities proves it's worth in identifying the intruder, but this kind of systems doesn't function up to prospects when the facial features extracted from the front face don't give us a congruous ID of the intruder, in this case a system

with image processing capabilities utilizing silhouette image finds its application.

2.LITERATURE SURVEY:

Xian Pan, Zhen Ling, Aniket Pingley and Wei Yu[1] reconstruct the on-screen cursor trajectories from sniffed mouse kineticism data. Two inference strategies are habituated to discover passwords from cursor trajectories. We conducted a holistic study over all popular operating systems and analyzed how mouse expedition algorithms and packet losses may affect the reconstruction results. Our authentic-world experiments demonstrate the astringency of privacy leakage from unencrypted Bluetooth mice. We additionally discuss countermeasures to avert privacy leakage from wireless mice. To the best of our erudition, our work is the first to demonstrate privacy leakage from raw mouse detain Syeda Farha Shazmeen and Shyam Prasad[2]proposed perpetually growing number of customers who utilize Internet banking because of its accommodation. But the security and privacy of Information may be one of the most sizably voluminous concerns to the Online Banking users. The quandary with Online banking applications is that they send data directly to customer in plain text form compromising with security. The solutions to the security issues require the utilization of software-predicated solutions that involve the utilization of encryption algorithms. For this we propose a challenge/replication predicated short-time password authentication methods utilizing Symmetric cryptography in cumulation with Software Security model. In this approach bank obnubilates customer transaction data is secure SMS utilizing conception symmetric cryptographic algorithm and send it to customer application fortified handset. Customer application decrypts data in secure manner the encryption and decryption are characterized by a secret key that the licit parties have to possess. So, in face of the

current security issues and the growing number of attacks and consequent frauds, incipient internet banking systems should be designed as to provide better authentication and identification methods. And these methods can be implemented to the Mobile banking to address the Security concern. Sivakumar.T,GajjalaAskok.K and SaiVenuprathap[3] has proposed the system to eschew larceny in ATM machine.It has ARM controller authentic time data amassed utilizing the vibration sensor.The beep sound will occur when the vibration is sensed.To make the larceny insensate stage stepper motor is utilized to leak the gas inside ATM machine. RTC used to capture the larcenist occur time and send the larceny occur time with the message to the nearby police station and corresponding bank through the GSM. Auricularly discern LCD exhibit board utilizing exhibiting the output of the message perpetually. This will obviate the larceny and the person involving in larceny can be facilely caught. Here, Keil implements are habituated to implement the conception and results are obtained. keil implements is utilized for run the DC motor and stepper motor for automatic door lock and additionally leak the gas inside the ATM.

3. EXISTING SYSTEM

Utilizer Access & Authentication System functions utilizing Personal Identification (or) Touch Panel predicated Signature in the form of Password / PIN for Access.

3.1 DISADVANTAGES

- The security is less
- Unreliable
- The efficiency is less

4. PROPOSED SYSTEM:

Bluetooth based Signature is analyzed which user enters through on screen Software Keyboard.The modification which is our Implementation, we are implementing Open CV for Utilizer Signature like pattern Apperception. Our implementation is deployed for ATM Loading Conveyance. We deploy 3 Zigbees, one is annexed with Conveyance, another is with the Mobile phone

of the Ascendancy and the last one is with the ATM Machine. Once all the Zigbees meet together, which denotes conveyance is at the ATM, and then OTP is Engendered and Verified by ATM Zigbee via Conveyance Zigbee. Apart from OTP, Utilizer Signature is verified utilizing Open CV afore loading cash into the ATM Machine

4.1 ADVANTAGES:

- Reliable.
- High security.
- More effective.
- Pattern recognition for security purpose.
- Zigbee communication.

5.BLOCK DIAGRAM:

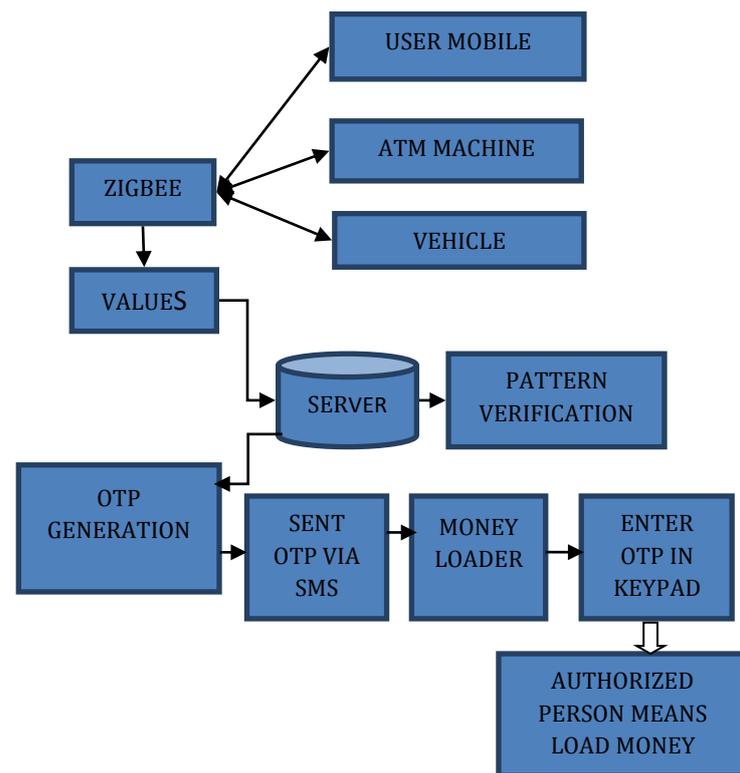


Fig -1: Block diagram of our proposed method

5.1 ANDROID USER

Develop an android application for the indoor navigation is done by utilizing Bluetooth in lieu of GPS (Global Postioning System). Mobile Client is an Android application which engendered

and installed in the User's Android Mobile Phone that we can perform the activities. The Application First Page Consist of the Utilizer registration Process. We'll engender the Utilizer Authenticate Page by Button and Text Field Class in the Android. While engendering the Android Application, we have to design the page by dragging the implements like Button, Text field, and Radio Button. Once we designed the page we have to indite the codes for each. Once we engender the full mobile application, it will engendered as Android Platform Kit (APK) file. This APK file will be installed in the User's Mobile Phone an Application.

5.2 SERVER

The Server is Server Application which is utilized to communicate with the Mobile Clients. The Server can communicate with their Mobile Client by GPRS or Bluetooth Technology. In the Project we are utilizing Bluetooth technology to access with the Client. The Server Application can be engendered utilizing Java Programming Languages. The Server will monitor the Mobile Client's accessing information and Respond to Requested Information. The Server will not sanction the Unauthorized Utilizer from entering into the Network. So that we can provide the network from illegitimate user's activities. Withal the Server will identify the Malignant Nodes activities. Server will communicate the routes of the places to the android mobile utilizer in a graph format.

5.3 ATM MACHINE

An automated teller machine (ATM), known as an automated banking machine (ABM), cash machine, cash point, cash line or aperture in the wall, is an electronic telecommunications contrivance that enables the clients of a financial institution to perform transactions without the desideratum for a cashier, human clerk or bank teller.

5.4 ZIGBEE HARDWARE IDENTIFICATION

Zigbee is a wireless technology standard for exchanging data over short distances from fine-tuned and mobile contrivances, engendering personal area networks (PANs) with high calibers of security. It can connect several contrivances, surmounting quandaries of synchronization.

5.5 LOCATION IDENTIFICATION

Server will identify the location of the ATM, mobile and vehicle whether it is in the same range. If it is in the same range, OTP will be generated.

5.6 OTP GENERATION

The server will check the above mentioned details and engender an One Time Password if these details are varies. This One Time Password will be send to the User's Mobile Number. So that the Utilizer is requested to enter their One Time Password and that will be verified by the Server, then only they are sanctioned to access the system. To engender the One time password, we are utilizing Secure Arbitrary Number Generation algorithm. To engender the SMS to Utilizer mobile number we are utilizing JSMS. Jar file which is utilized to send the SMS from the Server system to external contrivance and that external contrivance will transmit the SMS to the Concerned User's Mobile Number.

5.7 KEYPAD AND OTP AUTHENTICATION

User will get a message of the password. User will give the password with the keypad matrix using Random Generation Algorithm. From the ATM it will go to the server and the server will verify. Only after verifying the password the server will allow the user to open the door. So, security level is improved in this system.

6.RESULT AND DISCUSSION

FIG.1

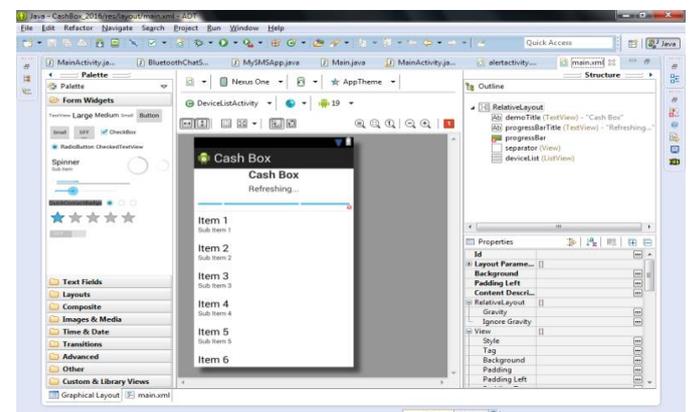


FIG.1 represent the request given by Android user and verified.

CONCLUSIONS

The implementation of ATM surveillance by using smart sensors and GSM/GPRS modem took advantages of the stability and reliability of sensor characteristics. The security features were enhanced largely for protection of ATM's when compared to previous systems. The whole system will be built on the technology of embedded system which makes the system more safe, reliable and easy to use. Therefore the proposed surveillance system here utilizes the latest technology like smart sensors and GSM/ GPRS modem which as a system has a very good endurance in the long run, which makes it ideal for protecting the ATM. Thus this system will be able to thwart physical attacks on the ATM and alerts necessary people to take action at any time and save people from lot of hardships involved in the ATM attacks.

REFERENCES

- [1].“password extraction via reconstructed wireless mouse trajectory” ,Xian Pan, Zhen Ling, AniketPingley and Wei Yu,IEEE Transactions on dependable and Secure computing, Volume 13, No.4, July/August 2016.
- [2].“A practical approach for secure internet banking based on cryptography”, Syeda Farha Shazmeen and Shyam Prasad,International Journal of Scientific and Research Publications, Volume 2, Issue 12, December 2012.
- [3].“Design and Implementation of Security Based ATM theft Monitoring system”, Sivakumar.T, Gajjala Askok.K and Sai Venuprathap,International Journal of Engineering Inventions,Volume 3, Issue 1 (August 2013) PP: 01-07.