International Journal of Innovations in Engineering and Technology (IJIET)
http://dx.doi.org/10.21172/ijiet.102.13

Implementation of ATM security using IOT

Mahalakshmi.T.K[1], J.Kumudha[2], M.Ranjitha[3], Mr.J.Gurumurthy[4], Dr.D.Sivakumar[5]

[1,2,3]*Department of electronics and communication engineering, Easwari engineering college, Ramapuram, Tamil Nadu, India*

[4]*Assistant Professor, Department of electronics and communication engineering, Easwari engineering college, Ramapuram, Tamil Nadu, India*

[5]*Professor, Department of electronics and communication engineering, Easwari engineering college, Ramapuram, Tamil Nadu, India*

Abstract- Automated Teller Machine(ATM) are well known systems typically used to carry out a variety of personal and business financial transactions. The existing ones provide instructions on the display screen for operation and a user is able to operate. In the proposed system if an unauthorized person accesses the user account knowingly or unknowingly an image of the person is captured. It is then compared with the account user database present in the cloud using image recognition and OpenCV . The image is sent to the user and also a message is dropped. If the user acknowledges the third person as known person then the display screen opens where the pin can be entered and the cash is withdrawn. It possesses an enhanced security and prevents spoofing.

Keywords- Automated Teller Machine (ATM), Authentication, Databases, Spoofing, Security.

I. INTRODUCTION

Automated Teller Machines (ATM) terminals are designed to facilitate easier withdrawal of money for bank customers. The number of bank transactions happening through ATM terminals nowadays is numerous which establishes the stability of the infrastructure in a great deal. There has been a research to offer several non-financial services along with the regular financial service offerings through ATM terminals but has never got implemented because of the challenges like the increased load on servers, security. The aim of this paper is to propose an architecture which enables the provisioning of several financial services through ATM terminals which proves to improve the security in case of unauthorized access.

IPv6 has been a great revolution in the area of computer networking. The adoption of IPv6 from IPv4 has been quite beneficial. IPv6 allows the flexibility of assigning the logical addresses to all the nodes in the internet which facilitates the communication between every node. The architecture proposed in this paper uses the IPv6 setting. Service offerings like online mobile recharge, online bill payment etc, Require a lot of infrastructure and robust security mechanisms. While these are being offered currently through various online services, there is a very good scope of making the use of existing technology with little changes to accomplish in a better way such that the offerings reach out to the general public.

II. EXISTING SYSTEM

Automated Teller Machine is the system which has been designed to give money instantly to the customers. The existing ATM's typically provide instructions on the display screen that are read by the user for an interactive operation. Having read the instructions the user is able to operate the ATM via the data and information entered in the keypad. Customers need to insert their ATM card provided by their financial institutions into the ATM terminals. To enable an authentication mechanism, a Personal Identification Number (PIN) is present against all the ATM card numbers. When their authentication is complete, the customer is allowed to select the type of transaction to be made by them - either balance enquiry or instant cash withdrawal. All these transactions now happen in a private network of the bank servers. The ATM Terminals could be extended to numerous other financial related services which could reach the end users at very fast and thus utilize these systems for instant cash withdrawal. This increases the efficiency of utilization of the installed Automated Teller Machines around the world and makes it more accessible to the end users. This makes the entire system usage robust. The main problem involved is in security issue.

III. SPECIFICATION

3.1 Web Camera

A webcam is a video camera that feeds or streams its image in real time to or through a computer to a computer network. When "captured" by the computer, the video stream may be saved, viewed or sent on to other networks via

systems such as the internet, and emailed as an attachment. When sent to a remote location, the video stream may be saved, viewed or on sent there. Unlike an IP camera this is connected using Ethernet or Wi-Fi. A webcam is generally connected by a USB cable, or similar cable, or built into computer hardware, such as laptops. The web camera is connected to the Web continuously for an indefinite time and generally supplies a view for anyone who visits its web page over the Internet. Some of them, for example such as online traffic cameras etc. In this implementation it plays a major role rather than used in ATM now a days.

Fig 1: A Web Camera

3.2. Image Sensor

An image sensor or imaging sensor is a sensor that detects and conveys the information that constitutes an image. It does so by converting the variable attenuation of light waves as they pass through or reflect off objects into signals, small bursts of current that convey the information. The waves can be light or other electromagnetic radiation. Image sensors are used in electronic imaging devices of both analog and digital types, which include digital camera, camera modules, medical imaging equipment, night vision equipment such as thermal imaging devices. Digital sensors include flat panel detectors. In this system an image sensor is integrated within the web camera.

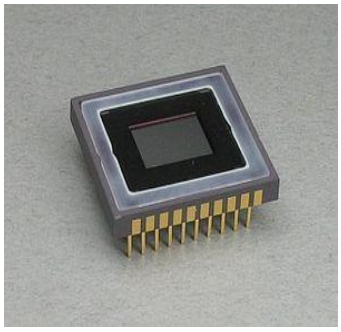

Fig 2: An Image Sensor

3.3 Raspberry Pi Controller

Raspberry Pi board is a miniature marvel, packing considerable computing power into a footprint no larger than a credit card. The Raspberry Pi is a credit card sized single-board computer with an open-source platform that has a thriving community of its own, similar to that of the audio. It can be used in various types of projects for designing home automation systems. There are a few versions of the Raspberry Pi, but the latest version, has improved upon its predecessor in terms of both form and functionality. The processor at the heart of the Raspberry Pi system is a Broadcom BCM2835 system on-chip multimedia processor. This means that the vast majority of the system's components, including its central and graphics processing units along with the audio and communication hardware are built onto that single component hidden beneath the 256MB memory chip at the center of the board. It also uses a different instruction set architecture (ISA) known as ARM.

The ARM-based BCM2835 is the secret of how the raspberry Pi is able to operate on just the 5V, 1A power supply provide by the onboard micro-USB port. It is also the reason why we will not be able to find any heat-sink on the device: the chip's low power draws directly and translates into a very little waste heat even during the complicated

processing task. It includes a Quad-core cortex-A7 CPU running at 900MHz and 1GB RAM. It is 4-6 times more powerful than the predecessor. The Raspberry Pi does not have an in-built real time clock. It consists of a SD card to store the operating system and program memory in either SDHC or Micro SDHC sizes. Most of them have between one to four USB ports, HDMI and composite video output and 3.5mm audio jack. It has a Wi-Fi onboard. It also has a CSI camera port for connecting Raspberry pi camera. The DSI display port is used for connecting the display.

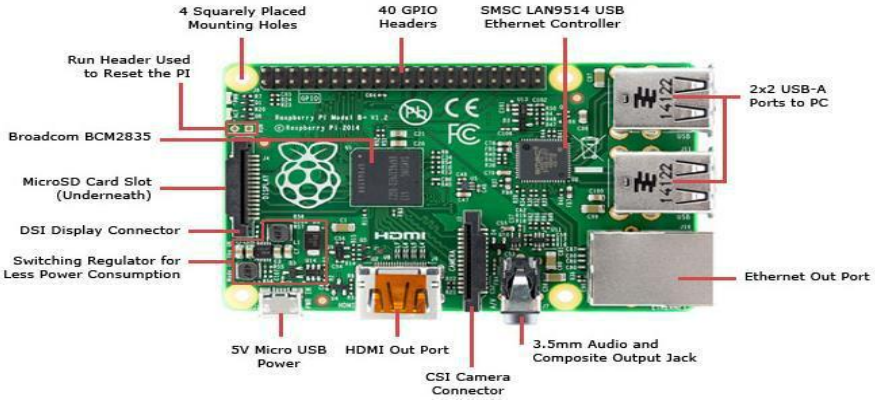

Fig 3: A Raspberry Pi Controller

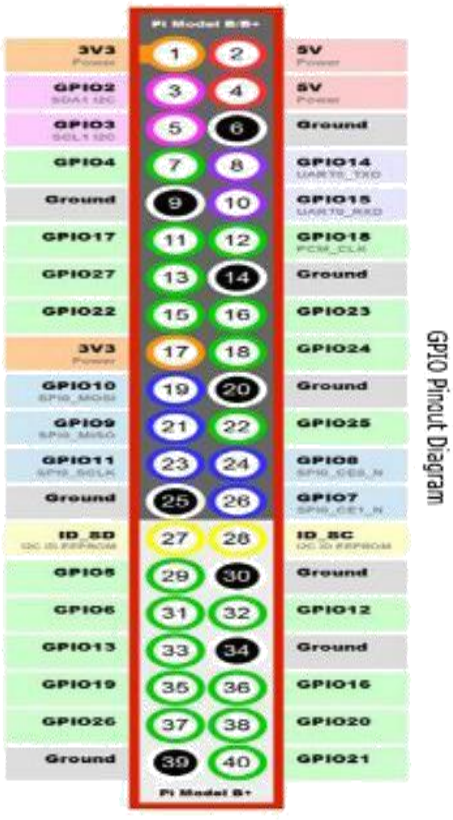

Fig 4: The Pin Configuration

The pin configuration of the raspberry pi controller is shown in the fig 4.2. It has 40 GPIO pins and some inbuilt pins such as UART pins. These pins are the interface between the system and external world. The raspberry pi is powered by 5V DC. Each pin is programmed to communicate to the external world. If pin is said to be logic 1 when input is 3.3V otherwise it is logic 0. It can act as both GPIO and I2C.

http://dx.doi.org/10.21172/ijiet.102.13

IV. SESSION ESTABLISHMENT

In order to have a communication to the user we establish a trusted third party application. All the implementations are made assuming the fact that there is a trusted third party application. At any cost it does not compromise the confidentiality of the card details. The application is said to posses only the ATM Card number and the mobile number of the corresponding account holder. The main assumption that is being made is that the ATM Card holder is always has a mobile phone with them. We have used an application called way2sms to ensure that the SMS reaches the account user in case of an unauthorized access.

V. OPERATION

In this proposed system we have created the new generation ATM machine which can be operator without the ATM card. By using this system ATM machine can be operated by using our mobile phone and IOT. We can also prevent the use of unauthorized person without our knowledge. We use image recognition and original image compared to the database in our server. In server we can collect the related information of the Image (i.e.) the users account details, their photo etc. the camera presented near the ATM machine will capture the users image and compare it with the user image in the server using OpenCV.

The session can be established only if the user acknowledges the third person as known person. Here the display has an option of either user or third user. If person who has come for withdrawn is the user then he can directly click on user option and can enter the PIN for withdrawal. If the person is a third user then the image of the person is captured using web camera. Then the image is compared with the database in the of the account user. Then the image is mailed to the account user and also a message is dropped. If the user acknowledges that the person is a known person sent by him then a window opens where he can enter the PIN number and the cash can be withdrawn.

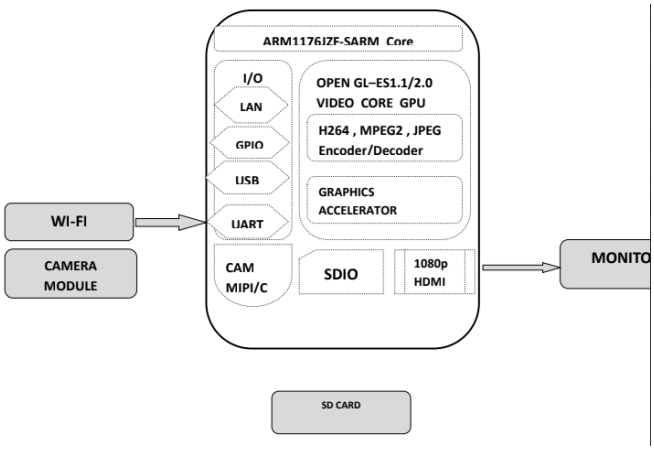

Fig 5: Proposed Block diagram

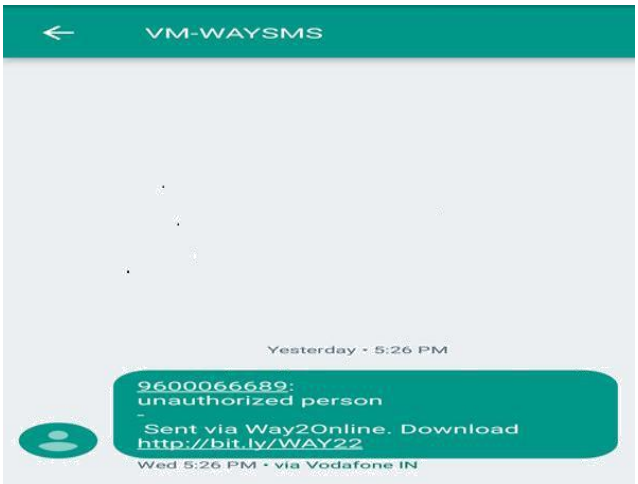

Fig 6: Message received by the account user

The fig 5 shows the output of the coding using the trusted third party application and the message received by the account user in case of an unauthorized access.

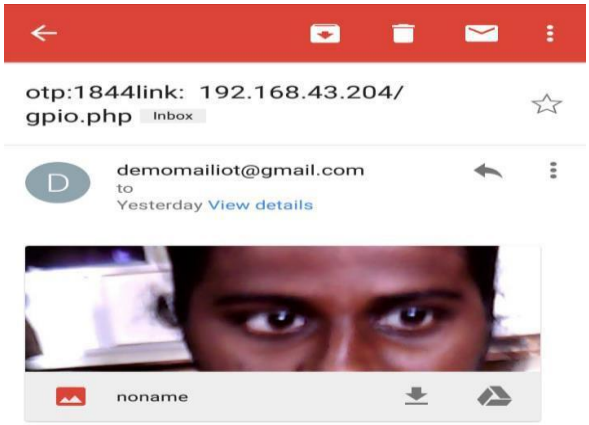

Fig 6: Mail of an image of the unauthorized person

VI. CONCLUSION

The ATM machine should have a very robust infrastructure in order to withstand all the transactions to take place. It must also be able to withstand from any attacks as it may collapse the entire transactions. A lot more services are being included in order to increase the efficiency of the system. The security and the authentication are the two main issues in money transfers over online networking. This proposed system ensures that the transactions are being encrypted. This increases security by providing the session key which increases the encryption. The system is robust, secure and easily implementable for several issues. It is made more usable as well as convenient for both the end users. Their feature which includes verification of Identities, Controlled Access, Authorization and prevent spoofing (Third party access).The proposed system ensures that the infrastructure available is made more usable and also convenient to the end users. In future the system can be implemented with a secure way of accessing an ATM by authorized persons using face recognition module, eliminates the drawback of previous system like manual controlling camera modules and doors, the system is cost effective as compare to existing manual technique and the real time video of the ATM centre can be monitored through web server which make ATM better safe from thefts.

VII. REFERENCES

[1] T. Kohno, A. Stubblefield, A. D. Rubin, and D. S. Wallach, "Analysis of an electronic voting system," in Security and Privacy, 2004 IEEE Symposium

[2] Gujarat State Election Commission, "e-voting system,"2010.[Online]Available: http://sec.gujarat.gov.inle-voting-system.html.

[3] Mujtaba.G, "Adaptive Automated Teller Machine Part-II," in ICICT, July 2011.

[4] K. Malladi, S. Sridharan, "Contemplate for Online Plebiscite Capturing ATM Terminals," in international Journal of Advanced Research in Computer Science and Software Engineering, vol. 3, issue 4, April 2013.

[5] K. Malladi and S. Sridharan, "Online Franchise Capturing using IPv6 through Automated Teller Machines," in the Proceedings of International Conference on Recent Trends in Information Technology (iCRTlT), IEEE,2013, pp. 562 – 568.