To Improve the ATM Security by using (RFID Reader) IOT

M. Umapathy[1] K. Soundarya[2] S. Parimala[3] C. Kowsalya[4]
[1]Assistant Professor
[1,2,3,4]Department of Computer Science and Engineering
[1,2,3,4]The Kavery Engineering College, Salem, TamilNadu, India

Abstract— Internet of things(IOT) is a basically Connecting machines without help of humans. Currently we using many methods for money transaction through online like G-pay, Xenpay, patym, etc. but we have to with draw money only from bank or ATM but smartly through ATM. Transaction from ATM using mobile banking apart from using ATM is proposed in order to reduce time of transaction but there might be security problems. In this paper, ATM service as remote access, security measures, prevention of hacking and duplicate cards and scope in futures will be discussed.

Keywords: Internet of things, money withdrawal, ATM security, remote access

I. Introduction

Banking has adopted technology for its fast growth and adoptions of current technology like cloud computing, data mining and data analytics. Now a day we use ATM for both transaction and withdrawal. In this service every account holder, have individual unique ATM card that contains unique pin provide by bank. In India ATM was implemented in the year of 1967, while it comes to cashless travel. According to ATM industry association (ATMIA), there are above 3 million ATM's in-stalled worldwide. Some useful services apart from cash withdrawal and account balance checking from an ATM

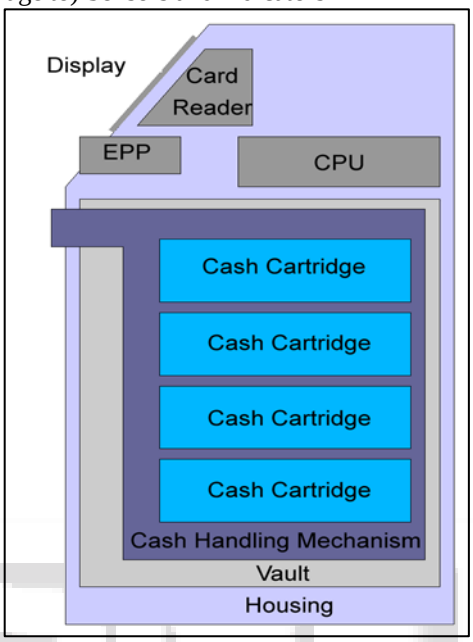
- recharge your mobile
- pay income tax
- transfer cash
- book railway tickets
- withdraw a fixed deposit
- apply for personal loan

More and more people are being globally digitalized and also it faced lot of security issues like developing of spam ATM card , skimming (copies the content of the magnetic stripes from ATM card) and PIN capturing technique by spy a camera or curb keypad every since. If a person want to withdraw money he/she must be present in ATM machine or unable to travel should have be sharing their PIN to third person. Normal users facing problems like misbehaving of other users and also CCTV camera observe the Pin detail. To overcome above activity we using remote access to improve ATM security.

II. Infrastructure of ATM

An ATM is made up of the following devices:

- CPU (to control the transaction devices)
- Magnetic chip card (to identify the user)
- PIN pad for accepting the user pin and encrypting personal identification number EPP4 (similar in layout to a touch tone or calculator keypad).
- Display (show the transaction details)
- Function key buttons or a touchscreen Record printer (to provide the a retransaction) Vault (to store the parts of the machinery re-stricted access) Housing (to attach signage to) Sensors and indicators



In early 2014, 95% of ATMs were running in Windows XP. A limited number of disposal may still be race older versions of the Windows OS, such as Windows NT, Windows 2000.ATM ap-plications are commonly referred to as pro-grammable applications it allows new host ap-plications and ATM terminal do more communicate with the switch.

III. Existing System

Original concept of regional private banks was built the existing ATM Simulation Sys-tem .ATM facilities are used to security, energy efficiency, time efficiency and performances are play a vital role in determine the Key Performance Indicators (KPI). IOT Helps Banks for enhance and secure their ATMs. Modern trend in banking system is very easy to handled by user like simpler and signature less features like IMPS (Immediate Payment Service), RTGS (Real Time Gross Settlement), NEFT (National Electronic Funds Transfer), Online Banking, and Tele-banking. If increasing the operational cost of ATM is reduce by IOT based devices.

A. Use Cases

1) Web-based Graphical User Interface with graphical reports, maps, and inventory; analysis the trend To check reason for slower and failure customer transaction and service issues are reduced in a cost-efficient manner.
2) monitoring failures & alerts on crossing a door-step.

3) ATM. Security attacks –damage to an ATM's customer panel, Intruder detection and alerts, Preventing cash-trapping, the attachment of skimming devices.
4) IOT allows a bank to track its ATM network cash shortages or maintenance issues.
5) It help to refilling the cash and maintenance.
6) Optimizes cash stocking of ATM and planning in the bank.
7) frequency of ATM usage can be analyzed in specific area and targeting zones for ATM in-stallation.

B. Customer's perspective:

1) A person cannot withdraw a money but re-ceiveda message of withdrawing money then they will complained to bank then authorized persons taking actions to refund the amount.
2) Track the history of money Withdrawals for every month.
3) Persons who have mobile number inked with bank account he want change the number or if it is lost by that user
4) will allowed to change the number every times .
5) Notify account balance on ATM entry and save receipt printing cost.
6) Transfer cash to your unbanked family/friend at local

Country	Banking in ATM	Banking in person	Banking online	banking via mobile
India	94%	94%	56%	76%
China	65%	22%	70%	85%
US	47%	43%	79%	63%

Table 1: Bank Domain

Based on the data with reference to the table 1 online banking service is used to more then the person banking. Mobile ATM is used to comparatively mobile banking.

Challenges in existing sys-tem: unauthorized person can easily access the account, when card is stolen and the pin number ascertained. Basic transactions are performed easy used to ATM. In this sense, the ATM Is rather like the express line in a supermarket--swift for some, but untouchable to others. ATM performance is generally brisk than that at a human teller. Although, user can instruction by that human teller and this can result struggling to complete a transaction of longer wait times in that currently using the machine.

Offenders can use skimming methods and small spy cameras to ATMs to cover the pin number also. By using skimming devices cost of more than $300,000 per day as per the U.S. banking system each year. As per the result of director of product management for Fiserv's Financial Crimes division ,In Jan 2012, ATM skimming had reached "epidemic "levels .ATMs give, but they can also take. It also have some malfunction and simply not available for sometimes. Customers will also make damage in cards, or any card owner fails to enter a correct PIN after three attempts. It have easy chance to accessing another account by this above methods and no safety barriers for the customers while enter he pin number, others who nearer to that person can see the pin number. Illiterate or the aged ones cannot using this current system without disclosing their PIN numbers. Otherwise they taking amount with the help of others in ATM new person for all every times. Now a days they are many methods for money transactions but withdrawing money from anywhere is by ATM .Suppose that person who are helped he/she will forget the password after three tries that card will be locked. In this system person must be present in the ATM and no chance to withdrawing money without dis-closing their PIN number and amount details, he can also have chance to check the balance or transfer the amount to their own account or something else.

To providing the solution for this ,it is possible without travelling without disclosing PIN number and amount details we can withdraw money by a third person.

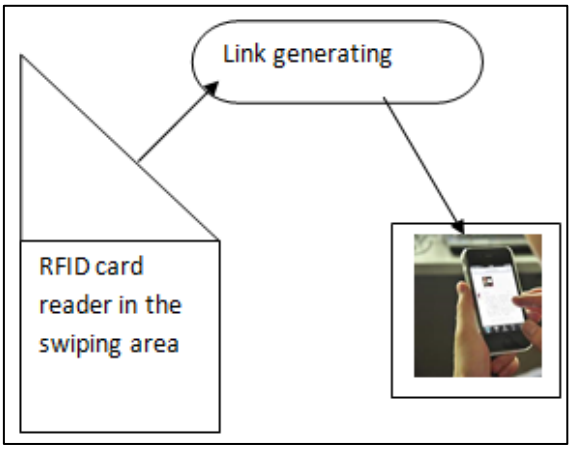
IV. PROPOSING SYSTEM

In this project we can provide one new method for the person who are not able to travel the ATM and normal users without sharing the PIN number, amount details to third person. If we enter our PIN number in ATM it provide chance to saw by nearer person and other users. In our project no need enter a PIN number ATM center so it prevent the customer details and provide security services.

Using IOT we connecting ATM and mobile for wireless connection. IOT is one of best way to connect two devices without wire. We can collect the database of Users name, mobile number. It is basic thing normal details can be submitted like what the customer will submit when applying for a new ATM card, it is not more difficult because now era all are having android mobiles. Coming to ATM center we can modify the swiping area we can fix the RFID (RADIOFREQUENCY IDENTIFIER) reader. The user swipe card then the RFID reader in the swiping area generating a link through the cloud source in the form of notification the link send to the user mobile. Then the user received the notification or message in the form of link, then they will press link it directed into the web page contains the virtual image of ATM's display. The customer can view web page of screen to the ATM, then the user enter the PIN number and amount details. After verifying the user details the money can be loaded and ready to withdrawing.

Because of this process we could improve the security in the way of avoid skimming, Some fake keypads in the control of cameras to capture PIN numbers. Just like the skimmers can lift over the ATM's original card slot, skimming keypads are designed to same as normal keypad's design and it like a glove. we cannot notice that the keypad on your ATM seems to original or a setup one or if you spy different color change between the key pad and anyone can put something like printable dust on the keypad and know what are the keys can be pressed in white collar theft manner and criminals can hide a small pinhole camera in a brochure holder near the ATM in order to extract the dupe pin numbers. In this process first thing we provide the security and then avoid the mon-ey hacking.

Normal android users can make this process very easily to safety and security it can avoid the unauthorized persons can access their ac-count in this process.



Dig. 3.1: IOT connecting through wireless

V. WORKING

In this project the working process divided into four modules they are Cloud web User Identification, Link generation, Notification, Money loading.

A. *Cloud web UI:*

This is the first module, the process is we insert the RFID reader in the card swiping area of ATM, then the link was generated using the data base of customer .The working RFID is an Automatic Identification and Data Capture (AIDC) methods of automatically identifying objects which is scanned, collected data about that, and enter those data directly into system .RFID methods usage of radio waves to accomplish the process. Ordinary level, RFID systems contains of three components: a tag of RFID or smart label, an RFID reader, and an antenna. RFID tags contain an IC (integrated circuit)integrated circuit and an antenna, with usage this it transmit data to the RFID reader (also known as interrogator).in this process radio waves are converted into data format .The tags contains Information is thentransform via communications interface to a host system, where database contains storage of data and it will analyzed later.

B. *Link Generation:*

The link will generated in the cloud it is link of website that contains virtual image of ATM display ,the website having front end of PHP language and back end of My SQL. Cloud is generally involves storage of data on physical location, it can be accessed from any device through the internet. Normally cloud is used to store the huge amount of data and it can be retrieve any time if we want. That SQL (Standard Query Language) data base contains user details of name, mobile number which is linked with bank account.

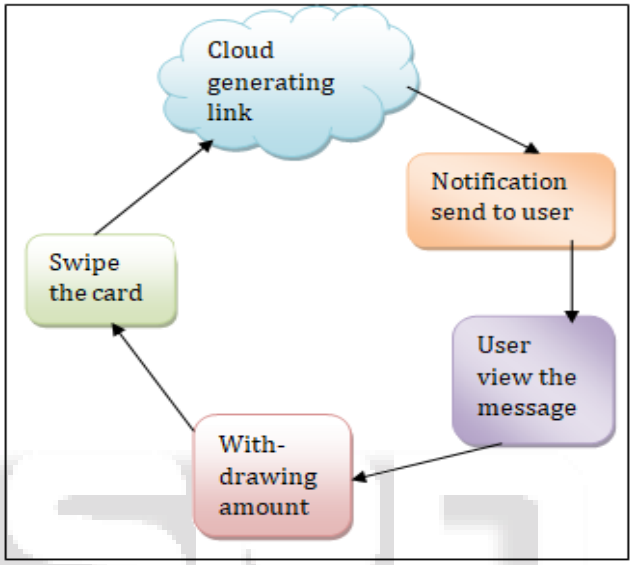
C. *Notification:*

The link is send to the user mobile in the form of notification, is working behind the principle of authentication request and response vice versa, it requires the multiple step of iterations, that notification is normal message format contain link when user press the link it will go to the webpage (which is already we created),it is a virtual image of ATM display , then the customer can enter the Personal Identification Number (PIN)and amount, after verify the authorized person details then it moves to next step.

D. *Money Loading:*

This is a final stage process, after completed above three stages, the money will be loaded which is stored in the ATM, inside the ATM, amount is stored in a session of trays, it allow the bills to be made available to the discharge opening and control mechanism. A gear inside the complex system it push tray of amount at one time. Then an optical sensor checks the amount and also verifying that, then money can be withdrawal.

dig: Architecture Diagram



Dig. 5.1: Architecture Diagram

VI. CONCLUSION

In this process ATM security will be improved using IOT mechanism and it provides the security service avoid skimming and development of duplicated cards. In any situation the PIN number only enter by authorized user. So it avoid the all misbehaving activities in ATM center. It is very useful to both normal user and people are not able to travel to ATM center.

REFERENCE

[1] Hariharan Ramalingam, Dr.V. Prasanna Venka-tesan, “Analysis of current trends in Internet of Things Gateway and edge data processing Characteristics”, International Journal of Engi-neering Research and Technology (IJERT), July 2019.
[2] Christiawan, B. A. Sahar, A. F. Rahardian, and E. Muchtar, “Fingershield ATM – ATM Security System using Fingerprint Authentication,” Int. Symposium Electronics and Smart Devices (ISESD) Indonesia, January 2019.
[3] Hariharan Ramalingam, Dr.V. Prasanna Venka-tesan, “Survey of Bio inspired algorithms in Edge computing”, Journal of Emerging Technologies and Innovation Research (JETIR), Dec 2018.
[4] Charlotte O'Donnelly, "A Guide to digital bank-ing in the IoT economy - How APIs enable an omnichannel,

mobile-first trategy for next generation banking experience", Au-gust 2018.
[5] Product specification – "NCR Self Serv 80 Series ATM family", NCR, 2018.
[6] White paper-"IoT-Enabled Banking Services", Infosys, 2018.
[7] E book - "Tech-enabled transformation - the trillion dollar opportunity for industrials", Mckinsey, 2018.
[8] S.Geetha, R.Hariharan, V.Prasanna Venkatesan, "Secured Indexing and tagging of IoT based device nodes for service based licensing and secured access", IEEE, Oct 2017.
[9] Ethan Wang, "IoT in Banking - Enabling Bank's Digital Fu-ture",Edgeverve.https://www.edgeverve.
[10] S. Sridharan and K. Malladi, "New generation ATM terminal services," Int. Conf. Computer Communication and Inform. (ICCCI) India, pp. 1-6, January 2016.

