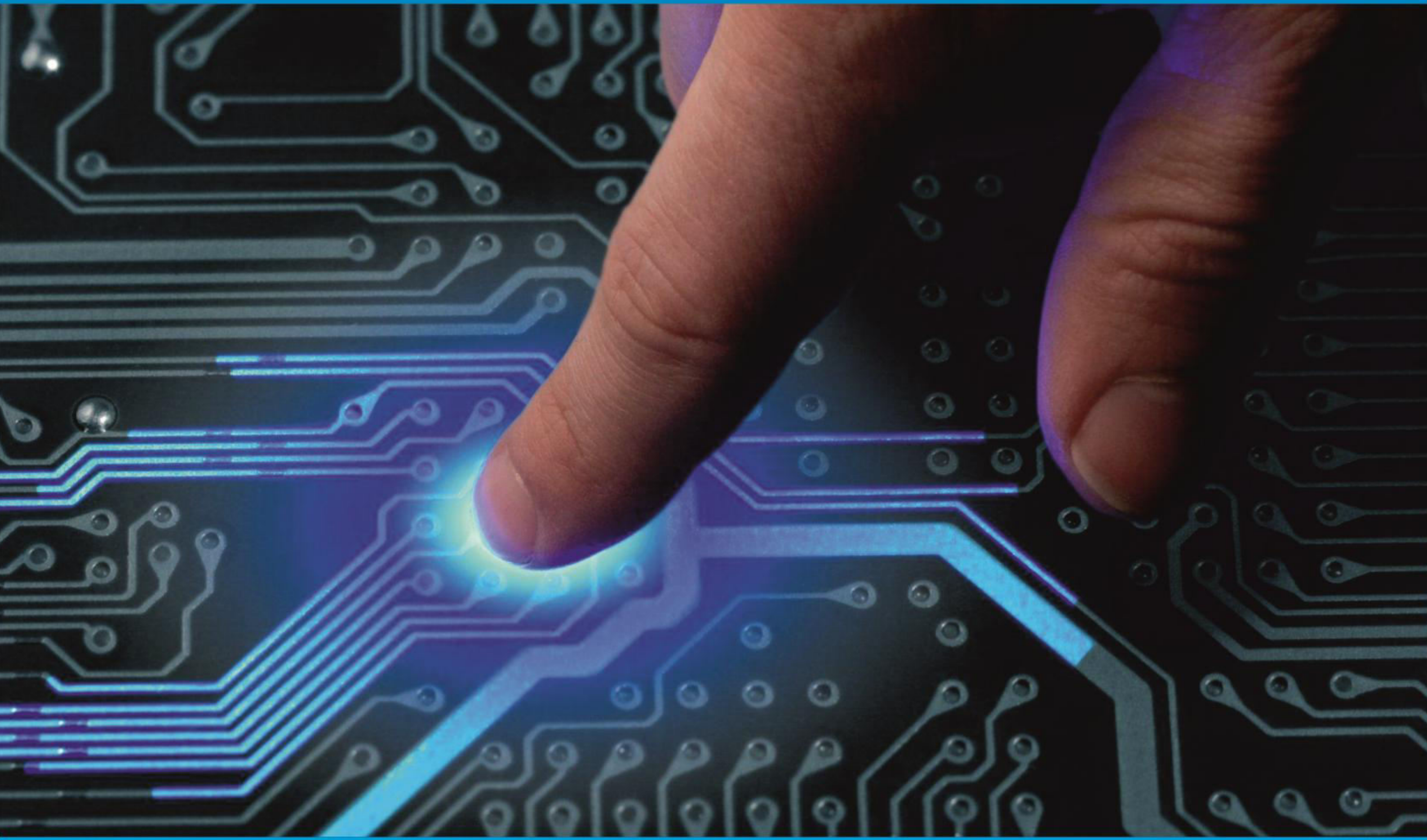
IJIRCCE

e-ISSN: 2320-9801 | p-ISSN: 2320-9798



INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

Volume 9, Issue 4, April 2021

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 7.488

International Journal of Innovative Research in Computer and Communication Engineering

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.488 |

|| Volume 9, Issue 4, April 2021 ||

| DOI: 10.15680/IJIRCCE.2021.0904069 |

Remote Access to Improve ATM Security by Using IOT

S.Vijayakumar, N.Abi, M.Arunkumar, G.Janani Aravind

Assistant Professor, Dept. of ECE, Paavai Engineering College, Namakkal, India

UG Students, Dept of ECE, Paavai Engineering College, Namakkal, India

ABSTRACT: Our project proposes a secured ATM (Automated Teller Machine) system using a card scanning system along with link system for improved security. Usual ATM systems do not contain the link feature form one withdrawal. If an attacker manages to get hold of ATM card and the pin number, he may easily use it to withdraw money fraudulent. So, our proposed system supports the ATM card scanning system along with a link system. This user may scan his card and login to the system. But after user is through with this authentication ,he may view details but it asked to enter link as soon as he clicks money withdrawal option. At this stage the system generates and sends a link to the registered mobile number to that particular user. The password is generated ad sent to the user mobile phone. He now needs to enter the link in the system in order to withdraw money .Thus, our system provides a totally secure way to perform ATM transactions with two level securitystructure.

KEYWORDS: Money fraudulent; Manets; authentication; security structure; link feature

I. INTRODUCTION

An embedded system is some combination of computer hardware and software, either fixed in capability or programmable, that is designed for a specific function or for specific functions within a larger system. Industrial machines, agricultural and process industry devices, automobiles, medical equipment, cameras, household appliances, airplanes ,vending machines and to as well as mobile devices are all possible locations for an embedded system .Embedded systems are computing systems ,but can range from having no user interface (UI) for example, on devices in which the embedded system is designed to perform a single task to complex graphical user interfaces (GUI), such as in mobile devices. User interfaces can include buttons, LEDs, touchscreen sensing and more. Some systems use remote user interfaces as well. Embedded systems can be microprocessor or microcontroller based. In either case, there is an integrated circuit (IC) at the heart of the product that is generally designed to carry out computation for real-time operations. Microprocessors are visually indistinguishable from microcontrollers, but whereas the microprocessor only implements a central processing unit (CPU) and thus requires the addition of other components such as memory chips, microcontrollers are designed as self- contained systems. Embedded systems can be microprocessor or microcontroller based. In either case, there is an integrated circuit (IC) at the heart of the product that is generally designed to carry out computation for real-time operations. Microprocessors are visually indistinguishable from microcontrollers, but whereas the microprocessor only implements a central processing unit (CPU) and thus requires the addition of other components such as memory chips, microcontrollers are designed as self-contained systems.

II. RELATED WORK

In[2]Therearemanythingsthatare,,wellknow‟‟aboutpasswords;suchasthatusercan’tremember strong password and that the passwords they can remember are easy to guess a password authentication system should encourage strong and less predictable passwords while maintaining memorability and security. This password authentication system allows user choice while influencing users towards stronger passwords.In [3] Graphical password systems are a type of knowledge-based authentication that attempts to leverage the human memory for visual information. A complete review of graphical passwords is available elsewhere. Of interest herein are cued-recall click-based graphical passwords (also known as loci metric). In such systems, users identify and target previously selected locations within one or more images. The images act as memory cues to aid recall. Example systems include Pass Points and Cued Click-Points (CCP).In [4] Classical PIN entry mechanism is broadly used for authenticating a user. It is a popular scheme because it properly balances the usability and safety aspects of a organism .However, if this scheme is to be used ina public system then the design might endure since accept surfing attack. In this attack, an unauthorized user can completely or partially watch the login session .Even the activities of the login gathering can be recorded which the attacker can use it soon after to get the actual PIN. In this paper, we suggest an intelligent user interface, known as Color Pass to oppose the accept surfing attack so that any authentic user can enter the session PIN without disclosing the authentic PIN. The Color Pass is based on a partially noticeable attacker model. The experimental analysis shows that the Color Pass interface is secure and simple to use even for novice users. In [5] Biometric system is the most secure and convenient authentication tool. Biometric systems are automated by hardware and software, allowing for fast, real-time decision making in identification situations. Biometric technology gives the potential for automatic personal verification. The two patterns of the biometric are the biological and behavioral. For verification of personal identity, the biological characteristics such as face, fingerprints, iris is used. Where as in behavioral characteristics such as voice, keystroke, signature is used. Handwritten signature is a common type to declares the accepts and take responsibility for a signed document. Signature verification is a behavioral biometric that is developed over the course of a person‘s lifetime. A biometric system is essentially a pattern recognition system which makes a personal identification by determining the authenticity of a specific physiological or behavioral characteristic possessed by the user. These characteristics are measurable and unique. These characteristics should not be duplicable. Many people are very accustomed to the process of signing their name and having it matched for authentication. Depending on data acquisition process signature verification system are divided into two types first is the Off- line and second is the On-line signature verification. In [6] Over the last decade, mobile devices such as smart phones have dominated the PC world, becoming undetectable part of people lives. The ever growing use of these devices in business areas has led to policies that allow employees to bring their own devices to work and access corporate assets and network. Smartphones as a latest technology break through provided with an all in one‖convenience, as spending a daywithout them is considered impossible for most of us. With all the personal and corporate sensitive data, there is a strong need for effective security methods. The current solutions to this problem are password-based authentication, PIN authentication, and password pattern authentication that allows user to draw shapes on screen. Despite their manifold advantages, passwords and PINs have major security drawbacks. They are very easy to spy on, which makes shoulder surfing a common attack specifically in public areas. In addition, pattern authentication is prone to the infamous ―smudge attack‖ in which finger traces left on the screen are used to extract the password. Moreover, users may forget their devices in office or public areas and unlocked, which allows others to take a peek without being noticed. Due to their weak security properties, these authentication approaches do not fully meet the requirement of adequately protecting the user‘s data stored on the device.In [7] Biometric authentication can be decent replacement for common traditional authentication schemes such as PINs, passwords, or pattern locks. There are two types of biometric identification schemes: physiological and behavioral. The physiological biometric methods such as fingerprint, iris, and hand geometry are become popular with traditional authentication methods, which provide additional security level due to their uniqueness and low error rate.

III. PROPOSED ALGORITHM

A. *Design Considerations:*

- ATMEGA 328P Microcontroller is used for this Proposed System
- It helps to save the Database of theuser.
- This System helps to Avoid the Malfunctionary Activities.
- IOT helps to save the database and link generation.
- Mobile is used as a remote for user friendly.

B. *Description of the Proposed Algorithm:*

system aims to solve all this by constant updating of bank records. The Java based construction of the system will enable transactions at any bank or ATM to be registered within a matter of seconds. Security of these details is also a top priority in this system. This central hub will be accessed by an ATM for secure customer transactions. In our project we are going to place an extra button in ATM machines. When that button got pressed the control window will be telecasted to accountant cellular phone. Then the accountant can enter the pin and amount manually in his

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.488 |

|| Volume 9, Issue 4, April 2021 ||

| DOI: 10.15680/IJIRCCE.2021.0904069 |

mobiles telecasted pop-up window. By this control system accountant can keep his pin number with him and he can vend the amount by his own control by the desired person.

Step 1: Wireless Sensor Network:
A wireless sensor network (WSN) is a computer network consisting of spatially distributed autonomous devices using sensors to cooperatively monitor physical or environmental conditions, such as temperature ,sound, vibration, pressure, motion or pollutants, at different locations. The development of wireless sensor networks was originally motivated by military applications such as battlefield surveillance. However, wireless sensor networks are now used in many civilian application areas, including environment and habitat monitoring, healthcare applications, home automation, and traffic control. In addition to one or more sensors, each node in a sensor network is typically equipped with a radio transceiver or other wireless communications device, a small microcontroller, and an energy source, usually a battery. The size a single sensor node can vary from shoebox-sized nodes down to devices the size of grain of dust. The cost of sensor nodes is similarly variable, ranging from hundreds of dollars to a few cents, depending on the size of the sensor network and the complexity required of individual sensor nodes.

Step 2: Internet of Things:
The Internet of Things (IOT) refers to the ever-growing network of physical objects that feature an IP address for internet connectivity, and the communication that occurs between these objects and other Internet-enabled devices and system. The Internet of Things extends internet connectivity beyond traditional devices like desktop and laptop computers ,smartphones and tablets to a diverse range of devices and everyday things that utilize embedded technology to communicate and interact with the external environment, all via the Internet. Examples of objects that can fall into the scope of Internet of Things include connected security systems, thermostats, cars, electronic appliances, and lights in household and commercial environments, alarm clocks, speaker systems, vending machines and more.The Internet of Things (IOT) is the network of physical objects—devices, vehicles, buildings and other items embedded with electronics, software, sensors, and network connectivity—that enables these objects to collect and exchangedata.

Step 3: MAX 232 Pin:
The MAX232 is an integrated circuit, first created by Maxim Integrated Products, that converts signals from an RS-232 serial port to signals suitable for use in TTL compatible digital logic circuits. The MAX232 is a dual driver/receiver and typically converts the RX, TX, CTS and RTS signals. The drivers provide RS-232 voltage leveloutputs (approx. ± 7.5 V) from a single + 5 V supply via on-chip charge pumps and external capacitors. This makes it useful for implementing RS-232 in devices that otherwise do not need any voltages outside the 0 V to + 5 V range, as power supply design does not need to be made more complicated just for driving the RS-232 in this case. The receivers reduce RS-232 inputs (which may be as high as ± 25 V), to standard 5VTTLlevels.These receiver shave a typical threshold of 1.3V, and a typical hysteresis of 0.5V.

IV. **PSEUDO CODE**

```
Step 1: Generate all the possible Links.
Step 2: Collect the all Server Database on Node MCU
Step 3: By Using IOT and Wi-fi Module Link will be generated Make the node into sleep mode.
else end Select all the routes which have active nodes

Step 4: Calculate the total Generated links
Step 5: Select the energy efficient route on the basis of minimum total transmission energy of the route. Step 6:
Calculate the RBE for each node of the selected route
Step 7: go to step 3.
Step 8: End.
```

V. SIMULATION RESULTS

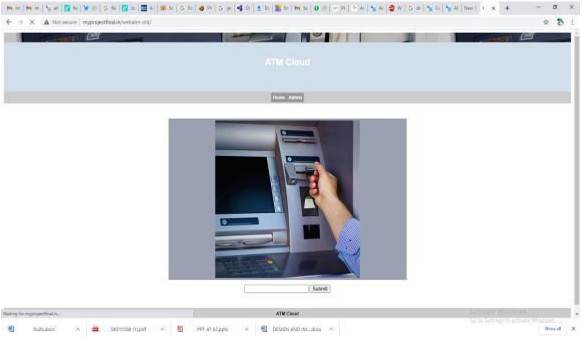
The simulation studies involve the deterministic small network topology. The ATM machine should have a very robust infrastructure in order to withstand all the transactions to take place. It must also be able to withstand from any attacks as it may collapse the entire transactions. A lot more services 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

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.488 |

|| Volume 9, Issue 4, April 2021 ||

| DOI: 10.15680/IJIRCCE.2021.0904069 |

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.



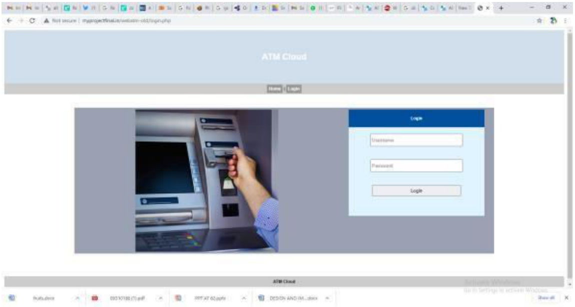
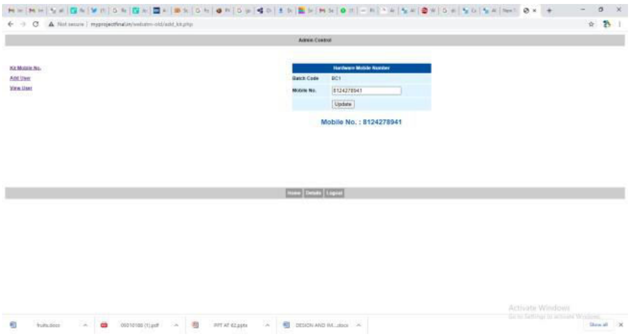


Fig.1. ATM Cardinsert

Fig. 2. Linkgeneration



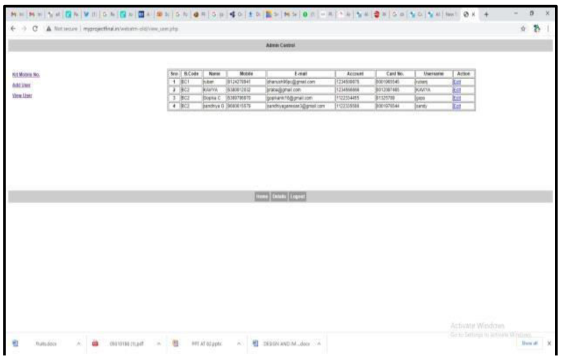
Hardware Mobile Number

Batch Code BC1

Mobile No. 8124278941

Update

Mobile No. : 8124278941



Sno	B.Code	Name	Mobile	E-mail	Account	Card No.	Username	Action
1	BC1	ruban	8124278941	dhanush96pc@gmail.com	1234509876	8001065546	rubanj	Edit
2	BC2	KAVIYA	6380812832	prabaa@gmail.com	1234566666	8012087465	KAVIYA	Edit
3	BC2	Gopika C	6369796870	gopikanki16@gmail.com	1122334455	81325789	gops	Edit
4	BC3	sandhya G	9688615576	sandhyaganesan3@gmail.com	1122335566	8001976544	sandy	Edit

Fig.3.RemoteAccess

Fig.4. User's Detail

VI. CONCLUSION AND FUTUREWORK

This whole implementation ensures us a secured and authenticated transaction through RFID and GSM technique with lowest cost and minimum maintenance. Mankind will utilize new and secured type of money transactions. The only thing is that initial cost of RFID conversion of the entire system is the required one time investment. The value added service that this system provides increases the credibility of the financial institutions, the banks improves the convenience to its customer. Hence as the world progresses through the inevitable and an indomitable quest for knowledge, the aspect of security bound systems are bound to concede with the growing innovations and obviously more vulnerabilities. Hence our application might well solve the aspect of transaction security to a precise and great extent.

REFERENCES

1. G.UdayaSree, M.Vinusha — Real Time SMS-Based Hashing Scheme for Securing Financial Transactions onATMTerminal‖,IJSETR,ISSN 2319-8885 Vol.02,Issue.12,September-2013,Pages:1223-1227.
2. KhatmodeRanjit.P, KulkarniRamchandra.V,-ARM7 Based Smart ATM Access
3. M.R.Dineshkumar, M.S.Geethanjali,-Protected Cash Withdrawing ATM Using Mobile Phone, International Journal Of Engineering And Computer Science ISSN:2319-7242 Volume 2 Issue 4 April, 2013 PageNo.1346-

1350.

4. ZaidImran,Rafay Nizaami-Advance Secure Login, International Journal For Science
5. M. Ajay Kumar and N. Bharath Kumar- Anti-Theft ATM Machine Using Vibration Detection Sensor, IJARCSSC Volume3,Issue12,December 2013 ISSN:2277128X.
6. SURAJ.B.S and Dr. R GIRISHA, ― ARM7 based Smart ATM Access System‖,InternationalJournalonRecentandInnovationTrendsinComputing and Communication ISSN: 2321-8169 Volume: 3Issue:5.
7. Kannan.K,―Microcontroller Based SecurePin Entry Method For ATM ,International Journal of Scientific & Engineering Research, Volume 4, Issue 8, August-2013 ISSN 2229-5518.
8. Hyung-Woo Lee,―Security in Wireless Sensor Networks: Issues and Challenges", ICACT, ISBN 89-5519-129-4, Feb.20-22,2006.

BIOGRAPHY

Mr.S.VIJAYAKUMAR M.E.,is Woking as an Assistant Professor in the Department of Electronics and Communication Engineering, Paavai Engineering College, Namakkal. He Completed his degree in 2002 in Master of Engineering and he Received Award for best Project Coordinator

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

9940 572 462 6381 907 438 ijircce@gmail.com

www.ijircce.com

Scan to save the contact details