International Journal of Engineering Technology and Management Sciences
Website: ijetms.in Issue: 2 Volume No.9 March - April – 2025
DOI:10.46647/ijetms.2025.v09i02.031 ISSN: 2581-4621

Design and Implementation of ATM Security Using IOT

S Monish, Department of ECE
Muthayammal Engineering College , Namakkal, India monishsella123@gmail.com
Dr.K.Radhika, Department of ECE
Muthayammal Engineering College , Namakkal, India radhika.k.ece@mec.edu.in
S Naveenkumar, Department of ECE
Muthayammal Engineering College , Namakkal, India ps.naveen135@gmail.com
R Ponkumar, Department of ECE
Muthayammal Engineering College , Namakkal, India ponkumar2005@gmail.com

ABSTRACT — This paper proposes a secured ATM (Automated Teller Machine) system that enhances traditional security protocols by incorporating a card scanning system along with a link-based authentication feature. Current ATM systems typically rely on a two-factor authentication model, where the user must have the ATM card and know the PIN. However, this method remains vulnerable to fraud if an attacker gains access to both the card and PIN. The proposed system addresses this issue by adding an extra layer of security: a link-based authentication process. In this system, after the user scans their ATM card and enters their PIN to authenticate, they can view their account details. However, when the user selects the "Money Withdrawal" option, the system generates and sends a unique, time-sensitive link to the user's registered mobile phone. The user must then enter this link into the ATM system in order to complete the withdrawal. This additional step ensures that even if an attacker gains access to the card and PIN, they cannot perform fraudulent transactions without access to the user's registered mobile phone. The proposed system thus provides a more secure method for ATM transactions by implementing a two level security structure, combining something the user knows (PIN) with something the user has (mobile phone). This enhances the protection of user accounts and reduces the risk of unauthorized ATM withdrawals.

Keywords : Link-based authentication , Secured ATM system , Two-factor authentication

I. INTRODUCTION

Automated Teller Machines (ATMs) play a crucial role in modern banking, allowing customers to perform financial transactions conveniently. However, ATMs are often vulnerable to security threats, including fraud, skimming, and physical attacks. To enhance security, the integration of Internet of Things (IOT) technology offers an innovative approach. This paper focuses on designing and implementing an IOT-based ATM security system to prevent unauthorized access and fraudulent activities. By utilizing biometric authentication, RFID technology, surveillance cameras, and real-time monitoring, the system can detect suspicious activities and alert authorities instantly. Features such as facial recognition, fingerprint scanning, GPS tracking, and OTP-based verification further strengthen ATM security. The implementation involves using microcontrollers (Arduino ATMEGA 328), sensors, and cloud-based data processing to create a smart, efficient, and secure ATM environment. This system ensures enhanced security, minimizes financial losses, and increases customer confidence in ATM transactions.

With the development of computer network technology and e-commerce, the self service banking system has got extensive popularization with the characteristic offering high-quality 24 hours service for customer. Nowadays, using the ATM (Automatic Teller Machine) which provides

International Journal of Engineering Technology and Management Sciences
Website: ijetms.in Issue: 2 Volume No.9 March - April – 2025
DOI:10.46647/ijetms.2025.v09i02.031 ISSN: 2581-4621

customers with the convenient banknote trading is very common. However, the financial crime case rises repeatedly in recent years; a lot of criminals tamper with the ATM terminal and steal user's credit card and password by illegal means. Once user's bank card is lost and the password is stolen, the criminal will draw all cash in the shortest time, which will bring enormous financial losses to customer. How to carry on the valid identity to the customer becomes the focus in current financial circle. Traditional ATM systems authenticate generally by using the credit card and the password, the method has some defects. Using credit card and password cannot verify the client's identity exactly. Anyone who knows the PIN and have the ATM card can easily access the user account. This paper describes a new method combining with the traditional method. Here RFID and GSM is used to improve the security of the transaction. To overcome the disadvantages of inserting the ATM card into the ATM machine, RFID card is used. It reads the user information by sensing and it also manages different banks accounts in a single RFID card. The GSM is used to improve the security by providing OTP and also informs the user by an SMS in case the entered password is wrong.

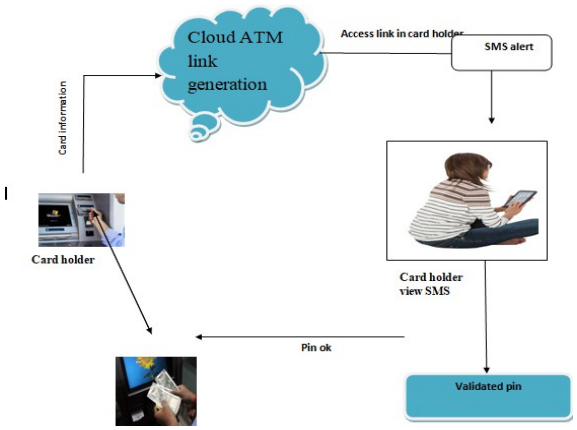
The Internet of Things (IOT) is a system of interrelated computing devices, mechanical and digital machines, objects, animals or people that are provided with unique identifiers and the ability to transfer data over a network without requiring human-to human or human-to-computer interaction. The IoT is a giant network of connected things and people – all of which collect and share data about the way they are used and about the environment around them. That includes an extraordinary number of objects of all shapes 3 and sizes – from smart microwaves, which automatically cook your food for the right length of time, to self-driving cars, whose complex sensors detect objects in their path, to wearable fitness devices that measure your heart rate and the number of steps you've taken that day, then use that information to suggest exercise plans tailored to you. There are even connected footballs that can track how far and fast they are thrown and record those statistics via an app for future training purposes.

II. SYSTEM ARCHITECTURE

A. System Overview

The design and implementation of ATM security using IoT (Internet of Things) aim to address these challenges by enhancing real-time monitoring, alert systems, and user authentication processes. This IoT-based system integrates various technologies to create a comprehensive security mechanism for ATMs. Biometric authentication, such as fingerprint or facial recognition, is used to ensure that only authorized users can access the ATM. Sensors, including motion, vibration, and temperature detectors, are installed to monitor the ATM's physical condition and detect suspicious activities like forced entry or tampering.

B. Architecture Diagram



International Journal of Engineering Technology and Management Sciences
Website: ijetms.in Issue: 2 Volume No.9 March - April – 2025
DOI:10.46647/ijetms.2025.v09i02.031 ISSN: 2581-4621

Fig 1. Architecture Diagram of ATM Simulation MODULES

- Cloud ATM web UI
- Link generation
- SMS Alert
- Money loading

MODULES DESCRIPTION

1. Cloud ATM web UI

In this module To be able to use an ATM a customer must first register an account number and a The ATM user interface consists of a keypad, a display window, 14 a selection of Check Balance. Use cases describe the main sequence scenario and lists. And this module to used for card holder with secondary person.

2. Link generation

In this modules released a new module the ATM cloud Linker. This module is an easy access for cardholder and provides a complete solution for generating the Link Element in a cloud website. It makes for a serious alternative to limited solutions that either use the requested url (therefore not eliminating duplicates) or that use a static html head inclusion (therefore eliminating content displayed via query strings) this module access for card holder only.

3. SMS Alert

SMS alert module sends out alerts to industrial automation, building automation, cloud based link access in cardholder and similar applications, where the timely alert to cardholder are important Based on the link, it sends pre configured SMS text to pre-configured mobile numbers.

4. Money loading

In this module to provide for in an attempt to provide cash-handling solutions in the field of banking automation, a new ATM (automated teller machine) with cash currency can be customized by simply uploading validation software. In this modules used in card holder secondary person.

C. Data Flow Diagram

Symbol	Description
	An **entity**. A source of data or a destination for data.
	A **process** or task that is performed by the system.
	A **data store**, a place where data is held between processes.
	A **data flow**.

Fig 2. Data Flow Symbols

A two-dimensional diagram that explains how data is processed and transferred in a system. The graphical depiction identifies each source of data and how it interacts with other data sources to

International Journal of Engineering Technology and Management Sciences
Website: ijetms.in Issue: 2 Volume No.9 March - April – 2025
DOI:10.46647/ijetms.2025.v09i02.031 ISSN: 2581-4621

reach a common output.

International Journal of Engineering Technology and Management Sciences
Website: ijetms.in Issue: 2 Volume No.9 March - April – 2025
DOI:10.46647/ijetms.2025.v09i02.031 ISSN: 2581-4621

Individuals seeking to draft a data flow diagram must (1) identify external inputs and outputs, (2) determine how the inputs and outputs relate to each other, and (3) explain with graphics how these connections relate and what they result in. This type of diagram helps business development and design teams visualize how data is processed and identify or improve certain aspects.
Level 1:

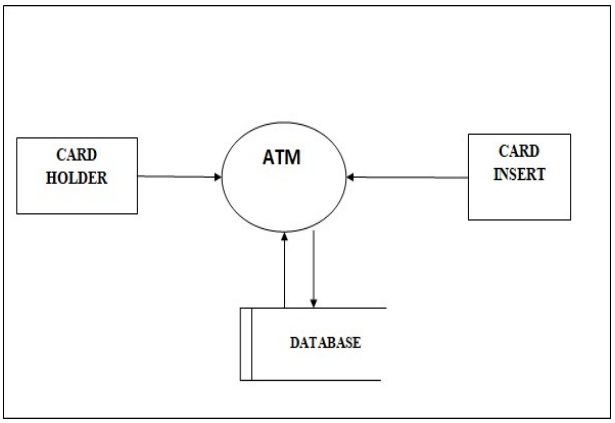


Fig 3. Basic Flow Diagram of an ATM System

The image represents a basic flow diagram of an ATM system that outlines the interaction between a cardholder, the ATM, and the database. In this system, the cardholder initiates a transaction by inserting their card into the ATM. The ATM reads the card details, such as the account number, and verifies the information. To process the transaction, the ATM communicates with the database, which stores all relevant user information, including account balance, transaction history, and authentication details like a PIN or biometric data. If the credentials and request are valid, the database approves the transaction and sends the required data back to the ATM. The ATM then allows the cardholder to proceed with operations such as cash withdrawal, balance inquiry, or fund transfer. Finally, the updated account details are stored back in the database.
Level 2:

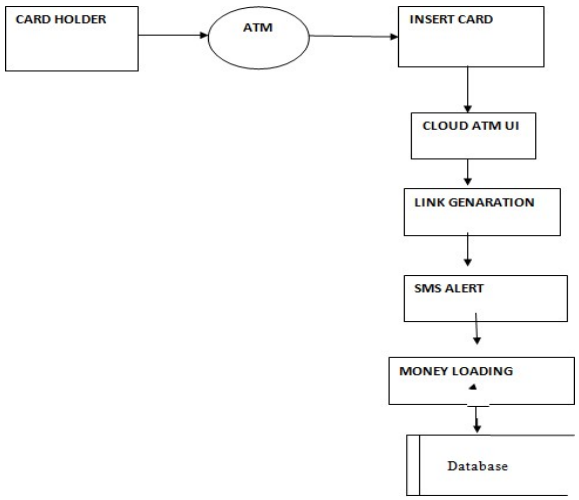


Fig 4. Database Diagram of ATM System

The diagram represents a secure ATM transaction process using cloud integration and real-time notifications. The process starts with the cardholder inserting their card into the ATM, which connects to a cloud-based ATM web interface for authentication and transaction management. A

International Journal of Engineering Technology and Management Sciences
Website: ijetms.in Issue: 2 Volume No.9 March - April – 2025
DOI:10.46647/ijetms.2025.v09i02.031 ISSN: 2581-4621

unique link is generated by the system and sent to the cardholder, ensuring an additional layer of security. Simultaneously, an SMS alert is sent to notify the cardholder of the transaction in progress. The cardholder then validates their identity by entering their PIN, which is verified by the system. If the PIN is correct, the transaction proceeds to completion, such as money withdrawal or loading. This system emphasizes security by leveraging cloud technology, SMS alerts, and multi-step authentication to protect against unauthorized access and enhance the overall user experience.

III. HARDWARE IMPLEMENTATION

The implementation of an IoT-based ATM security system requires various hardware components to enhance security, monitor real-time activities, and prevent fraudulent transactions. These components work together to detect unauthorized access, verify users, and alert authorities in case of suspicious activities.

A. Hardware Components :

- ATM module
- Micro Controller- Atmega328
- Web Api
- Motors
- Mobile Phones / Personal Computer
- Wi-Fi Module –ESP8266/Node MCU E12
- LCD Display

B. Block Diagram

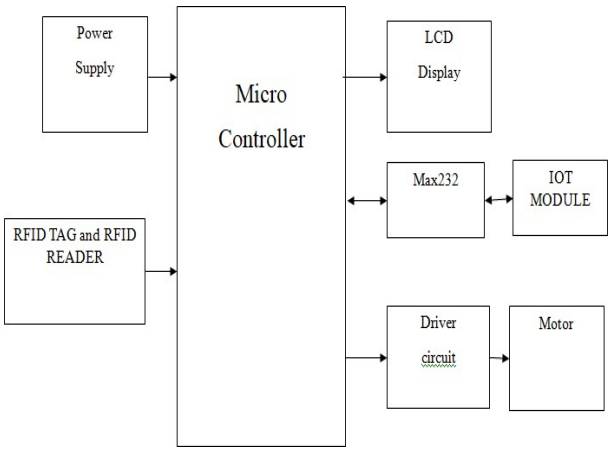


Fig 5. Block Diagram of ATM Simulation

1. Atmega328 Microcontroller

Arduino is a tool for making computers that can sense and control more of the physical world than your desktop computer. It's an open-source physical computing platform based on a simple microcontroller board, and a development environment for writing software for the board. Arduino can be used to develop interactive objects, taking inputs from a variety of switches or sensors, and controlling a variety of lights, motors, and other physical outputs. Arduino projects can be stand-alone, or they can be communicate with software running on your computer (e.g. Flash, Processing.) The boards can be assembled by hand or purchased preassembled; the open-source IDE can be

International Journal of Engineering Technology and Management Sciences
Website: ijetms.in Issue: 2 Volume No.9 March - April – 2025
DOI:10.46647/ijetms.2025.v09i02.031 ISSN: 2581-4621

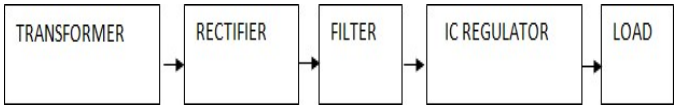
downloaded for free. The Arduino programming language is an implementation of Wiring, a similar physical computing platform, which is based on the Processing multimedia programming environment.

- Inexpensive - Arduino boards are relatively inexpensive compared to other microcontroller platforms. The least expensive version of the Arduino module can be assembled by hand, and even the pre-assembled Arduino modules cost less than $50.
- Cross-platform - The Arduino software runs on Windows, Macintosh OSX, and Linux operating systems. Most microcontroller systems are limited to Windows.
- Simple, clear programming environment - The Arduino programming environment is easy-to-use for beginners, yet flexible enough for advanced users to take advantage of as well. For teachers, it's conveniently based on the Processing programming environment, so students learning to program in that environment will be familiar with the look and feel of Arduino.
- Open source and extensible software- The Arduino software is published as open source tools, available for extension by experienced programmers. The language can be expanded through C++ libraries, and people wanting to understand the technical details can make the leap from Arduino to the AVR C programming language on which it's based. Similarly, you can add AVR-C code directly into your Arduino programs if you want to.
- Open source and extensible hardware - The Arduino is based on Atmel's ATMEGA8 and ATMEGA168microcontrollers. The plans for the modules are published under a Creative Commons license, so experienced circuit designers can make their own version of the module, extending it and improving it. Even relatively inexperienced users can build the breadboard version of the module in order to understand how it works and save money.

Fig 6. ATMEGA328 Microcontroller

2. Power Supply

The ac voltage, typically 220V rms, is connected to a transformer, which steps that ac voltage down to the level of the desired dc output. A diode rectifier then provides a full-wave rectified voltage that is initially filtered by a simple capacitor filter to produce a dc voltage. This resulting dc voltage usually has some ripple or ac voltage variation. A regulator circuit removes the ripples and also remains the same dc value even if the input dc voltage varies, or the load connected to the output dc voltage changes. This voltage regulation is usually obtained using one of the popular voltage regulator IC units.



Fi g 7. Block Diagram of Power Supply

International Journal of Engineering Technology and Management Sciences
Website: ijetms.in Issue: 2 Volume No.9 March - April – 2025
DOI:10.46647/ijetms.2025.v09i02.031 ISSN: 2581-4621

3. Relay

A relay is an electrically operated switch. Many relays use an electromagnet to operate a switching mechanism mechanically, but other operating principles are also used. Relays are used where it is necessary to control a circuit by a low-power signal (with complete electrical isolation between control and controlled circuits), or where several circuits must be controlled by one signal. The first relays were used in long distance telegraph circuits, repeating the signal coming in from one circuit and re-transmitting it to another. Relays were used extensively in telephone exchanges and early computers to perform logical operations. A type of relay that can handle the high power required to directly control an electric motor or other loads is called a contactor. Relays with calibrated operating characteristics and sometimes multiple operating coils are used to protect electrical circuits from overload or faults; in modern electric power systems these functions are performed by digital instruments still called protective relays.

4. LCD Display

A Liquid Crystal Display (LCD) is a flat panel display, electronic visual display, or video display that uses the light modulating properties of liquid crystals. Liquid crystals do not emit light directly. LCDs are available to display arbitrary images (as in a general-purpose computer display) or fixed images which can be displayed or hidden, such as preset words, digits, and 7-segment displays as in a digital clock. They use the same basic technology, except that arbitrary images are made up of a large number of small pixels, while other displays have larger elements. LCDs are used in a wide range of applications including computer monitors, televisions, instrument panels, aircraft cockpit displays, and signage. They are common in consumer devices such as video players, gaming devices, clocks, watches, calculators, and telephones, and have replaced 26 Cathode Ray Tube (CRT) displays in most applications. They are available in a wider range of screen sizes than CRT and plasma displays, and since they do not use phosphors, they do not suffer image burn-in. LCDs are, however, susceptible to image persistence. The LCD screen is more energy efficient and can be disposed of more safely than a CRT. Its low electrical power consumption enables it to be used in battery powered electronic equipment. It is an electronically modulated optical device made up of any number of segments filled with liquid crystals and arrayed in front of a light source (backlight) or reflector to produce images in color or monochrome. Liquid crystals were first discovered in 1888. By 2008, worldwide sales of televisions with LCD screens exceeded annual sales of CRT units; the CRT became obsolete for most purposes.

Fig 8. LCD display

5. GSM Technology

GSM refers to second-generation wireless telecommunications standard for digital cellular services. First deployed in Europe, it is based on TDMA (Time Division Multiple Access) technology. GSM uses three frequency bands: 900 MHz, 1800 MHz and 1900 MHZ. Dual-band phones operate on two out of three of these frequencies, while tri-band phones operate on all three frequencies.

GSM (Global System for Mobile Communications, originally Group Special Mobile)

It is a standard set developed by the European Telecommunications Standards Institute (ETSI) to describe protocols for second generation (2G) digital cellular networks used by mobile phones. The GSM standard was developed as a replacement for first generation (1G) analog cellular networks,

DOI:10.46647/ijetms.2025.v09i02.031 ISSN: 2581-4621

and originally described a digital, circuit switched network optimized for full duplex voice telephony. This was expanded over time to include data communications, first by circuit switched transport, then packet data transport via GPRS (General Packet Radio Services) and EDGE (Enhanced Data rates for GSM Evolution or EGPRS). Further improvements were made when the 3GPP developed third generation (3G) UMTS standards followed by 27 fourth generation (4G) LTE Advanced standards."GSM" is a trademark owned by the GSM Association.

IV. SOFTWARE IMPLEMENTATION

A. Embedded Programming

Embedded systems programming is different from developing applications on a desktop computers. Key characteristics of an embedded system, when compared to PCs, are as follows:

· Embedded devices have resource constraints(limited ROM, limited RAM, limited stack space, less processing power)

Components used in embedded system and PCs are different; embedded systems typically uses smaller, less power consuming components. Embedded systems are more tied to the hardware.

Two salient features of Embedded Programming are code speed and code size. Code speed is governed by the processing power, timing constraints, whereas code size is governed by available program memory and use of programming language. Goal of embedded system programming is to get maximum features in minimum space and minimum time.

B. Biometric Authentication Software

One of the primary security features of this system is biometric authentication, which eliminates the need for traditional PIN-based security. The ATM software is programmed to recognize users through fingerprint scanning **or** facial recognition**.** Using OpenCV and deep learning algorithms**,** the system matches the user's biometric data against a pre-stored database. If a match is found, the user is granted access to perform transactions. Otherwise, the system records the attempt and, if multiple failed attempts occur, alerts the bank's security team.

C. IoT Communication and Alert System

The ATM security system relies on IoT communication protocols to send security alerts in real-time. The software uses GSM, MQTT, or HTTP protocols to deliver instant alerts via SMS, email, or push notifications to bank authorities and law enforcement. For instance, in case of a security breach, an SMS gateway or Firebase Cloud Messaging (FCM) is used to notify relevant stakeholders immediately. This ensures a rapid response to any suspicious activity occurring at the ATM.

The software implementation of an IoT-based ATM security system significantly enhances ATM safety by integrating biometric authentication, AI-based surveillance, cloud computing, and IoT-enabled alert mechanisms**.** This system provides an efficient and automated approach to preventing fraud, unauthorized access, and ATM-related crimes. By leveraging real-time monitoring, encrypted data storage, and mobile connectivity, the system ensures that ATM security is both proactive and reliable. As banking technology advances, the integration of artificial intelligence and blockchain can further strengthen ATM security systems, making transactions safer and more efficient for users.

V. APPLICATIONS

A. . Enhanced ATM Security in Banking

The primary application of this system is in banking institutions to prevent ATM fraud, card skimming, and unauthorized access**.** By integrating biometric authentication (fingerprint, facial recognition) and real-time monitoring**,** banks can ensure that only authorized users access the ATM. Additionally, GPS tracking and IoT-based alerts help banks respond quickly to security breaches.

DOI:10.46647/ijetms.2025.v09i02.031 ISSN: 2581-4621

B. Remote ATM Monitoring for Banks

Banks and financial institutions can monitor ATMs remotely through a cloud-based dashboard or mobile app**.** This allows them to track ATM activity, detect security threats, and take preventive actions without needing physical security personnel at every location. The web and mobile-based monitoring system helps banks manage ATM networks more efficiently.

C. Integration with Law Enforcement Agencies

In case of theft, fraud, or physical attacks on ATMs, the system can send instant alerts to law enforcement agencies**.** The GPS tracking system helps authorities locate stolen or tampered ATMs, while real-time CCTV footage aids in identifying criminals and preventing further crimes.

D. Emergency Alert System for ATM Users

In case a user feels threatened during an ATM transaction (such as a robbery attempt), an emergency alert button can be integrated into the system. This button will trigger a silent alarm that notifies security personnel or the nearest police station.

E. Improved Customer Safety and User Experience

Customers benefit from increased ATM security through biometric authentication, OTP-based transactions, and AI-powered surveillance**.** This reduces risks associated with card theft, PIN hacking, and ATM fraud, creating a safer and more reliable banking experience.

F. Area Monitoring

Area monitoring is a typical application of WSNs. In area monitoring, the WSN is deployed over a region where some phenomenon is to be monitored. As an example, a large quantity of sensor nodes could be deployed over a battlefield to detect enemy intrusion instead of using landmines. When the sensors detect the event being monitored (heat, pressure, sound, light, electro-magnetic field, vibration, etc), the event needs to be reported to one of the base stations, which can take appropriate action (e.g., send a message on the internet or to a satellite). Depending on the exact application, different objective functions will require different data-propagation strategies, depending on things such as need for real-time response, redundancy of the data (which can be tackled via data aggregation techniques), need for security, etc.

VI. CONCLUSION

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.Udaya Sree, M.Vinusha " Real Time SMS-Based Hashing Scheme for Securing Financial Transactions on ATM Terminal" ,IJSETR, ISSN 2319-8885 Vol.02,Issue.12,
September-2013, Pages:1223-1227.

[2] Khatmode Ranjit P, Kulkarni Ramchandra V, "ARM7 Based Smart ATM Access & Security System Using Fingerprint Recognition & GSM Technology", ISSN 2250- 2459, ISO 9001:2008 Certified Journal, Volume 4, Issue 2,
February 2014.

[3] M.R.Dineshkumar,M.S.Geethanjali,"Protected Cash Withdrawal in ATM Using Mobile Phone", International Journal Of Engineering And Computer Science ISSN:2319- 7242 Volume 2

DOI:10.46647/ijetms.2025.v09i02.031 ISSN: 2581-4621

Issue 4 April, 2013 Page No. 1346-1350.
[4] Zaid Imran,Rafay Nizaami ,"Advance Secure Login", International Journal For Science and Research Publications, Volume 1,Issue 1,December 2011.
[5] M. Ajaykumar and N. Bharath Kumar," Anti-Theft ATM Machine Using Vibration Detection Sensor", IJARCSSC Volume 3, Issue 12, December 2013 ISSN: 2277 128X.
[6] SURAJ B S and Dr. R GIRISHA, " ARM7 based Smart ATM Access System", International Journal on Recent and Innovation Trends in Computing and Communication ISSN: 2321-8169 Volume: 3 Issue: 5.
[7] Kannan K, "Microcontroller Based Secure Pin 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.
[9] Taha Ayesha ,Pallavi B V Dr. BaswarajGadgay "Securing ATM Transactions using Raspberry PI Processor", International Journal for Research in Applied Science & Engineering Technology (IJRASET) , Vol.
[10] No. VII, 2018.. [6] Narmada, D., and J. V. Priyadarsini. "Design and implementation of security based ATM using ARM11." In 2016 International Conference on Inventive Computation Technologies (ICICT), vol. 3, pp. 1-4. 2016.
[11] Ravichandran, S. "Cloud connected smart gas cylinder platform senses LPG gas leakage using IOT application." International Journal of MC Square Scientific Research, Vol. 9, no. 1,pp. 324-330, 2017.