SMART ATM SURVEILLANCE SYSTEM

A PROJECT REPORT

Submitted by:

POOJA ANIL

LMC17MCA004

to

The APJ Abdul Kalam Technological University

in partial fulfillment of the requirements for the award of the Degree

of

Master of Computer Applications

Department of Computer Applications

LOURDES MATHA COLLEGE OF SCIENCE AND TECHNOLOGY

KUTTICHAL, THIRUVANANTHAPURAM 695574

JULY 2020

SMART ATM SURVEILLANCE SYSTEM

A PROJECT REPORT

Submitted by:

POOJA ANIL

LMC17MCA004

to

The APJ Abdul Kalam Technological University

in partial fulfillment of the requirements for the award of the Degree

of

Master of Computer Applications

Department of Computer Applications

LOURDES MATHA COLLEGE OF SCIENCE AND TECHNOLOGY

KUTTICHAL, THIRUVANANTHAPURAM 695574

JULY 2020

DEPARTMENT OF COMPUTER APPLICATIONS
LOURDES MATHA COLLEGE OF SCIENCE AND TECHNOLOGY
KUTICHAL, THIRUVANANTHAPURAM

CERTIFICATE

This is to certify that the report entitled **SMART ATM SURVEILLANCE SYSTEM** submitted by **POOJA ANIL** to the APJ Abdul Kalam Technological University in partial fulfillment of the requirements for the award of the Degree of Master of Computer Applications is a bonafide record of the project work carried out by her under my guidance and supervision.

Prof. Sherin Joseph
(Internal Supervisor)

Date:

(External Supervisor)

Prof.Justin G Russel
(Project Co-ordinator)

Prof. Selma Joseph
(Head of the Dept.)

DECLARATION

I undersigned hereby declare that the project report “SMART ATM SURVEILLANCE SYSTEM”, submitted for partial fulfillment of the requirements for the award of degree of Master of Computer Application of the APJ Abdul Kalam Technological University, Kerala is a bonafide work done by me under supervision of Prof.Sherin Joseph. This submission represents my ideas in my own words and, I have adequately and accurately cited and referenced the original sources. I also declare that I have adhered to ethics of academic honesty and integrity and have not misrepresented or fabricated any data or idea or fact or source in my submission. I understand that any violation of the above will be a cause for disciplinary action by the institute and/or the University.

Thiruvananthapuram

16/05/20 POOJA ANIL

CONTENTS

ACKNOWLEDGEMENT

An endeavor over a long can be successful only with advice and support of many well wishers. I wish to place on record my profound indebtedness and gratitude to all those who have contributed directly or indirectly to make this project work a success. At the very onset, I express my gratitude to God Almighty, who sheltered me under his protective wings and showered on innumerable blessings throughout the period of this Master of Computer Application Course.

It is a great pleasure to express my sincere gratitude to **Rev. Dr.Tomy Joseph Padinjareveettil;** Director and **Prof. Dr. P.P Mohanlal**, Principal, Lourdes Matha College of Science and Technology for permitting to do this project with the fullest spirit. I am highly obliged to **Ms. Selma Joseph,** Head of the Department of Computer Applications, Lourdes Matha College of Science and Technology, for being the source of inspiration throughout the course and for her valuable guidance.

With heart full of thanks, I would like to take up this opportunity to wish my internal guide **Ms. Sherin Joseph**, Assistant Professor and all staffs of department of computer applications for their endless support, encouragements and suggestions in various stages of the development of this project.

I thank my parents and friends for their moral support and encouragement for the successful completion of this project.

ABSTRACT

The Idea of Designing and Implementation of Smart ATM surveillance project is born with the observation in our real life ATM physical attacks happening around us and lack of proper surveillance system for ATM and nearby components like AC,CCTV as well as to check power supply inside the ATM . This project deals with prevention of physical attack and provide accurate mointering system with proper data history using latest IOT platforms.Here our main motive is to overcome the drawback found in existing technology where in traditional methodology many operators sit infront of the mointers and watch each CCTV visuals if they found anything unusual they have to inform nearby police station and bank authority.This is a time consuming and difficult task. We here overcome this drawback using two open source platform known as ThingSpeak and Blynk. ThingSpeak which is an open source IOT application and API to store and retrieve data using HTTP and MQTT protocol over internet or via a Local Area Network. It enable the creation of senser logging applications, location tracking applications and a social network of things with status updates whereas blynk ia an open source interface that can be used with IOS and Android apps to control Arduino over the Internet. It can display sensor data, store data and can vizualize . Whenever robbery occurs,the attacker attack the ATM machine,vibration sensor that placed inside the ATM is used here to senses the vibration produced from the machine. This system uses Node MCU to process real time data which are collected using the vibration sensor and other sensers Once the vibration is sensed, the beep sound will occur from the buzzer and NodeMCU which has a in-built Wi-Fi that is used to send the robbery occur time with the message to the nearby police station and corresponding centralized atm control room. We use the LDR sensor for CCTV mointering ,temperature and humidity sensor(DHT11) for monitoring the AC and has the functionality to determine the current supply inside the atm. We can also produce the data of amount of used current . This is the methodology we use here to prevent the atm robbery as well as to mointer atm and its components. Currently to provide protection to the ATM and to the customers using it, only CCTV cameras and emergency sirens, a low cost standalone embedded webserver, Machine to Machine (M2M) and RFID used to implement an anti-theft system.But our proposed system will be not only able to protect from physical attacks on the ATM but also provide 24*7 mointering of atm components like AC ,CCTV, power supply .It also alerts necessary people to take action at any time and save people from lot of hardships involved in the ATM attacks.

CHAPTER 1

INTRODUCTION

1.1GENERAL BACKGROUND

This project proposes a smart IOT system based on embedded technology and incorporates various sensors to continuously monitor its surroundings for suspicious activities like physical attack, fraud, theft that might harm the ATM and people nearby, using the platform ThingSpeak which is a web based open API IoT source information platform that comprehensive in storing the sensor data of varied IoT applications and conspire the sensed data output in graphical form at the web level. ThingSpeak communicate with the help of internet connection which acts as a 'data packet 'carrier between the connected 'things' and the ThingSpeak cloud is to retrieve, save/store, analyze, observe and work on the sensed data from the connected sensor to the host microcontroller such as Node MCU. Another platform called Blynk is an Open-Source based Java server, responsible for forwarding messages between Blynk mobile application and various microcontroller boards (i.e. Arduino, Raspberry Pi. etc).

This project also provide a maintenance system and controlling system for CCTV cameras, power supply, ATM machine, AC and also provide security and safety measures that can be implemented to prevent such raids and failures in the ATM by proper surveillance. The proposed system employs proactive measures to counteract the burglary attempt, here the sensors of the system act as first line of defense. Here we can detects the break-in and take the protective actions which will deter the burglars from continuing with their attack, thereby successfully thwarting the attack. The proactive measures that are employed in the system are the siren, send notification to officials using Node MCU. By stopping the attack, the ATM is prevented from bearing any more harm caused due to the attack. The system continuously monitors its surroundings by sensing temperature changes, humidity, viberation, current using the sensors.

The main aim of this project is to design a system for alerting theft to police or centralizd control room automatically. The purpose of the system is to design a smart and centralized monitoring and control system using IOT technologies.In Existing Methods commercially available anti-theft burglar systems are used and its very expensive and open type even thief can disable it. Also an human security was appointed to monitor the ATM .This makes the system costlier. Current camera surveillance systems can be used for monitoring but they require a huge amount of data storage due to continuous video recording. However, our system act as an IOT

Based Centralized Bank Security System for Monitoring . The area when motion is detected and there is a possibility of certain activity. Oursystem also sends a notification, in case of suspicious activity as it is not possible to continuously keep a watch on such activities.

1.2 OBJECTIVE AND SCOPE

The banking industry is continuing to grow and their technology implementation is forever. Regardless of that, the present world of threats and thief attacking the banking industry is not reducing . Vulnerabilities are being discovered daily and exploits developed towards them mostly targeting financial institutions. Traditional methodologies for threat and thief detection cannot work anymore thus a need for revolutionary ideas and focus when it comes in to banking security industry. IOT emerged the idea of remotely monitoring objects through the Internet. When it comes to our project, security is crucial issue to the general public banks and atm’s. Currently, the increments of various theft was identified with the bank was numerous.In prior days, we have one burglar alarm at our banks for the security, but the situation has changed turns out to be current days. From these circumstance, we should make a system that would be prepared for highly secured one. For enhancing the security of bank this framework is maintained by central processing unit. We use microcontroller which is computational circuit which processes the information inside it.. Here, we utilize the vibration sensor to catching the motion ,LDR sensor for vision blockage detection ,temperatureand humidity sensor to measure humidity and temperature in ATM ,has a feature to mointer power supply and NodeMCU which sends then notification to the central processing unit. While in central processing unit all the actions were monitored by the executives and information will be passed to the bank managers and local police stations using ThingSpeak and Blynk. After that if the theft was confirmed by the executives by checking the values of several sensor inputs and take corresponding action to prevent the attack. So that we can catch thief very easily and also we can keep the bank secure with the help of latest IOT technology. Compare to the cost of existing system this one is effective and cheaper.

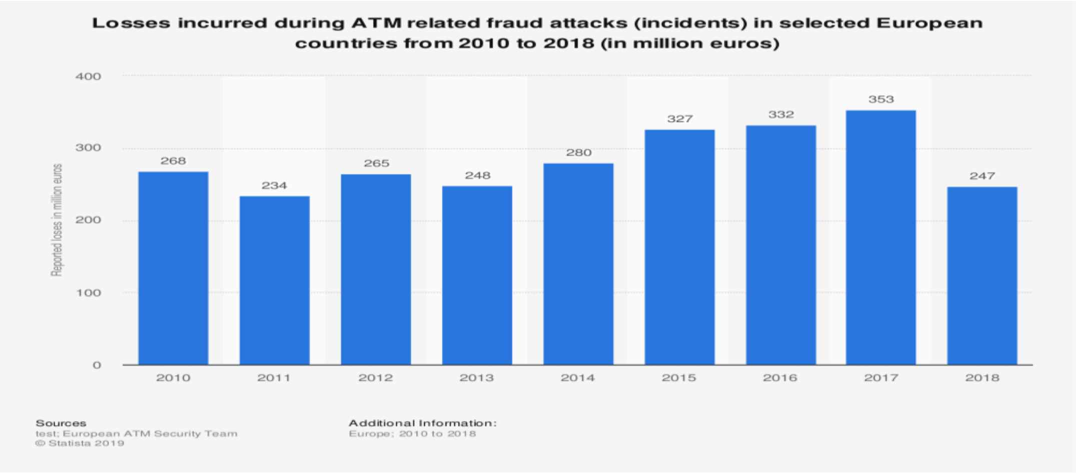
CHAPTER 2

LITERATURE SURVEY

2.1STUDY OF SIMILAR WORKS

In recent years, the usage of ATM service is increased drastically as it offers more sophistication for the customers to withdraw their amount at 24*7 hours. The growth in electronics transaction has been adapted by banking sector. Yet ATM service suffers lots of security issues, which threatens the entire banking sector and customer. Due to the various physical attacks like Ram-raid(The common method of physically removing ATM from premise with vehicle) ,Cutting (Use rotary saw, blow torch, thermal lance, and diamond drill to brutally open safe gaining direct access to cash) atm security is not ensured. According to the recent survey, rate of robbery and theft is increasing in every year. The following statistical report shows the crime rate. The ATM crimes are happening at a frequent rate because of lack of security system in center. Mostly robberies are taken place during off-peak hours, such activities lead to 11% of transaction and 60% of crime on day to day routine.

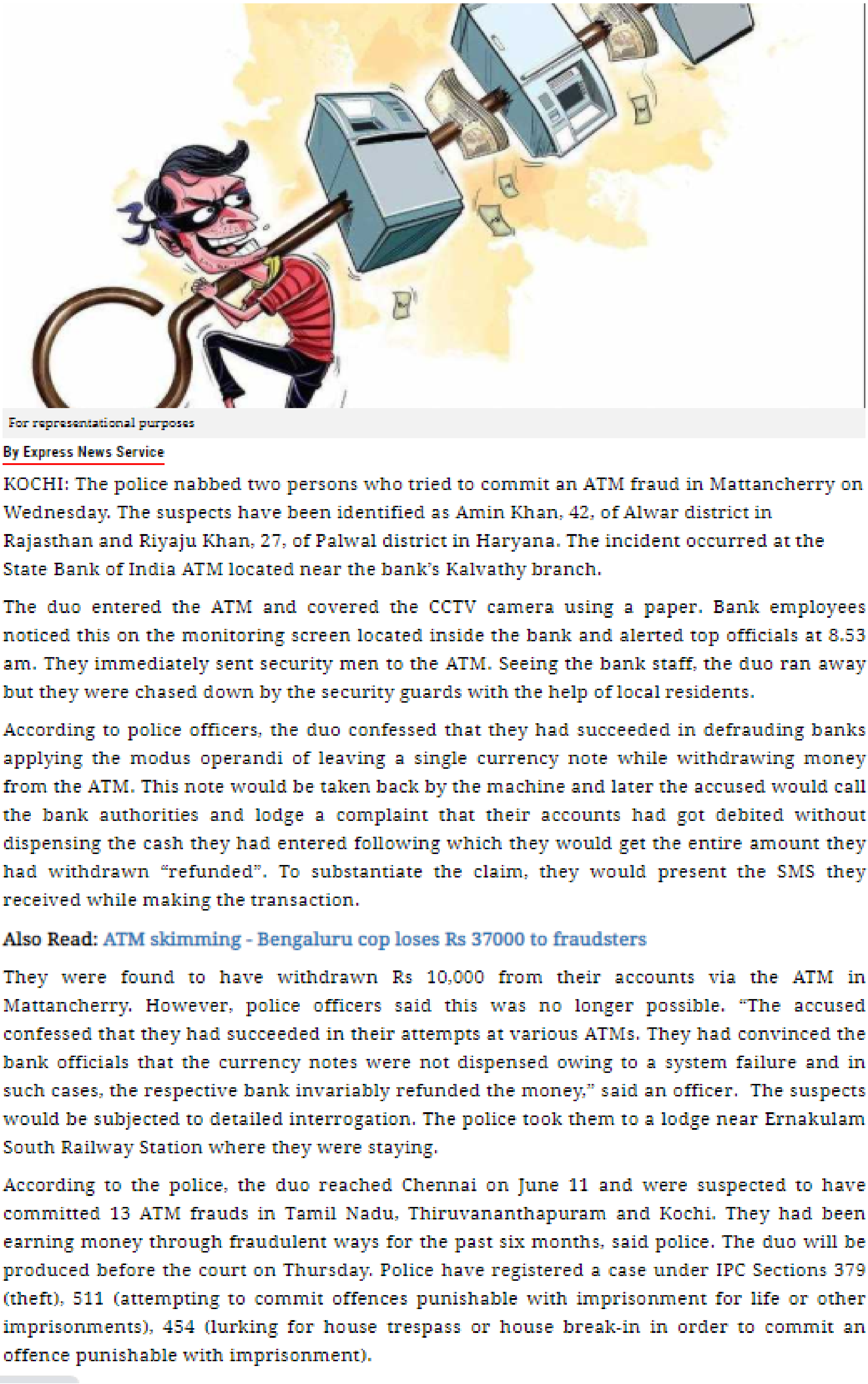
A statistics stated that, about 5500 crimes have been recorded in a year. The lack of security encourages these types of crimes which are increasing steadily. ATM centers play a vital role for money withdrawal.In the Existing system we have a watchman and a camera to monitor the ATM system. The recent enhancement made in the security system for a few ATMs is that it is provided with security to the entrance doors itself such that to enter the ATM we need to use the card to unlock the door. Thief can kill the watchman and to break the camera. It cannot be send the information. Literature study motivates us for providing the more efficient security for the banks, so that society can invest in banks without any fear. This work reduced the threats in the society related to bank theft.



Losses incurred during ATM related fraud attacks (incidents) in selected European countries from 2010 to 2018 (in million euros)

Sources
test; European ATM Security Team
© Statista 2019

Additional Information:
Europe; 2010 to 2018



For representational purposes

By Express News Service

KOCHI: The police nabbed two persons who tried to commit an ATM fraud in Mattancherry on Wednesday. The suspects have been identified as Amin Khan, 42, of Alwar district in Rajasthan and Riyaju Khan, 27, of Palwal district in Haryana. The incident occurred at the State Bank of India ATM located near the bank's Kalvathy branch.

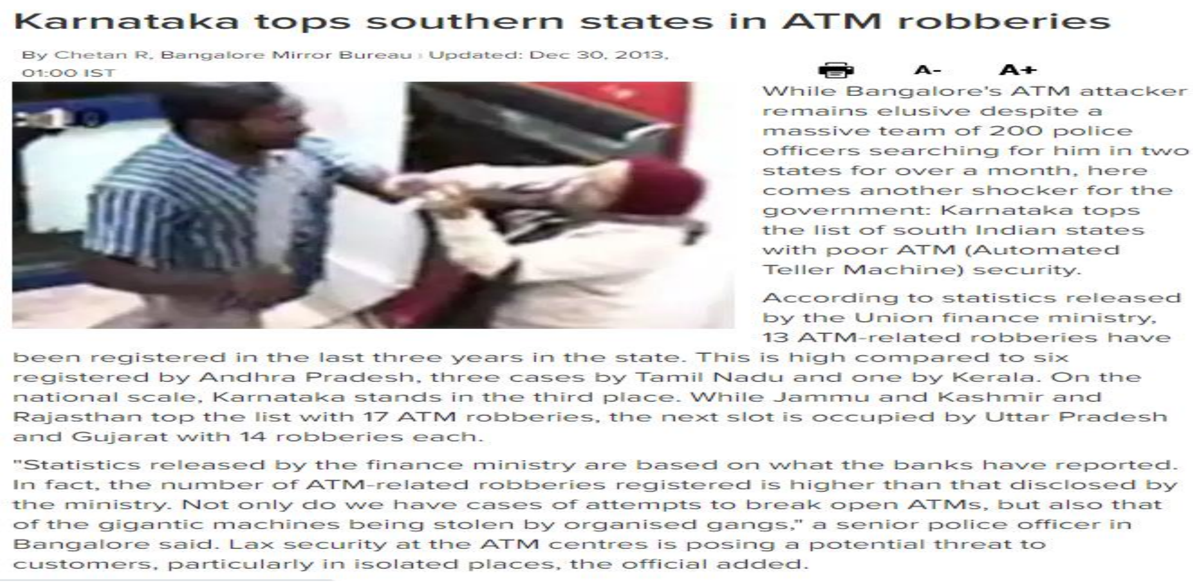
The duo entered the ATM and covered the CCTV camera using a paper. Bank employees noticed this on the monitoring screen located inside the bank and alerted top officials at 8.53 am. They immediately sent security men to the ATM. Seeing the bank staff, the duo ran away but they were chased down by the security guards with the help of local residents.

According to police officers, the duo confessed that they had succeeded in defrauding banks applying the modus operandi of leaving a single currency note while withdrawing money from the ATM. This note would be taken back by the machine and later the accused would call the bank authorities and lodge a complaint that their accounts had got debited without dispensing the cash they had entered following which they would get the entire amount they had withdrawn "refunded". To substantiate the claim, they would present the SMS they received while making the transaction.

Also Read: ATM skimming - Bengaluru cop loses Rs 37000 to fraudsters

They were found to have withdrawn Rs 10,000 from their accounts via the ATM in Mattancherry. However, police officers said this was no longer possible. "The accused confessed that they had succeeded in their attempts at various ATMs. They had convinced the bank officials that the currency notes were not dispensed owing to a system failure and in such cases, the respective bank invariably refunded the money," said an officer. The suspects would be subjected to detailed interrogation. The police took them to a lodge near Ernakulam South Railway Station where they were staying.

According to the police, the duo reached Chennai on June 11 and were suspected to have committed 13 ATM frauds in Tamil Nadu, Thiruvananthapuram and Kochi. They had been earning money through fraudulent ways for the past six months, said police. The duo will be produced before the court on Thursday. Police have registered a case under IPC Sections 379 (theft), 511 (attempting to commit offences punishable with imprisonment for life or other imprisonments), 454 (lurking for house trespass or house break-in in order to commit an offence punishable with imprisonment).



Karnataka tops southern states in ATM robberies

By Chetan R, Bangalore Mirror Bureau | Updated: Dec 30, 2013, 01:00 IST

While Bangalore's ATM attacker remains elusive despite a massive team of 200 police officers searching for him in two states for over a month, here comes another shocker for the government: Karnataka tops the list of south Indian states with poor ATM (Automated Teller Machine) security.

According to statistics released by the Union finance ministry, 13 ATM-related robberies have been registered in the last three years in the state. This is high compared to six registered by Andhra Pradesh, three cases by Tamil Nadu and one by Kerala. On the national scale, Karnataka stands in the third place. While Jammu and Kashmir and Rajasthan top the list with 17 ATM robberies, the next slot is occupied by Uttar Pradesh and Gujarat with 14 robberies each.

"Statistics released by the finance ministry are based on what the banks have reported. In fact, the number of ATM-related robberies registered is higher than that disclosed by the ministry. Not only do we have cases of attempts to break open ATMs, but also that of the gigantic machines being stolen by organised gangs," a senior police officer in Bangalore said. Lax security at the ATM centres is posing a potential threat to customers, particularly in isolated places, the official added.

ATM robberies in Bangalore

May 2012

A whopping Rs.1.91 crore was robbed in filmy style near an ATM in RT Nagar. In 10 minutes flat, seven armed men brandishing guns, choppers and machetes made off with cash from a vehicle being used to transport cash meant for Corporation Bank ATMs on May 14. However, the gang was arrested with cash and valuables worth Rs 50 lakh.

June 2013

A gang of three looted an ATM by breaking open the safe with a gas cutter and taking away Rs 19 lakh in Nagashettihalli. A guard with the Canara Bank ATM, who had plotted the robbery, was soon nabbed. Besides this, Rs.10-15 lakh was stolen from a branch of state-owned State Bank of India (SBI) from an ATM in Bagalur. There was no security guard.

October 2013

There was an attempt to rob an IDBI ATM kiosk on the Outer Ring Road at Mahadevpura. In their bid, two youth from Assam who worked in Bangalore – 21-year-old Jinto Debnath and 19-year-old Nabho Kou -- also killed the ATM guard, but were nabbed soon.

November 2013

A man with machete brutally attacked a banker and escaped with her cash at a Corporation bank ATM. While Jyoti Uday has survived after being recently discharged from hospital, the assailant is still on run.

December 2013

There was failed attempt to rob an Indian Overseas ATM kiosk in Malleshwaram recently. Though an attempt was made by miscreants to break open the ATM, they were unsuccessful.

Cybercriminals have begin targeting ATM systems with the intent to exploit vulnerabilities in the defence of financial institutions. In the rapidly evolving world of cybercrime, ‘smash and grabattacks on ATM is not new. Cash machines are now a focus for operatives aiming to siphon bounty ranging from customer data to old fashioned cash. The aim is to steal the ATM intact and transport it to a site where the cash can be extracted by force. The alternative is ‘smash and grab,’ breaking into the ATM on site to extract funds. Since 2016, almost 100 attacks of this type on ATMs using gas explosions were recorded by police in England and Wales. This included 23 attacks by a single gang over a three-month period, which saw more than £1.5 million stolen across theMidlandsregion. Similarly, in India, ATM manufacturer NCR has released a security warning of “jackpotting” attacks being conducted against ATMs in India. The alert states that criminals are gaining access to the “top box” of ATMs to connect a device to a USB port. By using the USB “black box,” the attacker can connect a keyboard, issue commands to the ATM, and tell it to dispense cash at will. Recently, Indian co-operative Cosmos Bank has fallen victim to ATM cash-out attack that saw 94.24 crore ($13.4mn) stolen in 14,000 transactions across 29 countries . an imminent global cyber-attackon commercial bank ATMs known as an ATM ‘cashout,’ the pre-empted attack centred on the hacking of a bank or payment processor to enable the fraudulent withdrawal of funds .

DifferentKind

Over the past decade, ATM malware attacks have tremendously developed and increased. According to a 2017 European ATM Crime Report by European Association for Secure Transactions (EAST) there was a 287% rise in ATM black box attacks versus the previous year. Cyber security solutions can deal with an array of infrastructural vulnerabilities but ATM hardware ATM attacks are of two kinds: physical and logical. A physical attack sees the perpetrator present before, during and after the crime. It involves the use of physical force to compromise the machine and is quite common in the UK. Logical attack on the other hand involves malware and specialist electronics to gain control of the ATM and access to common data and funds. Theft that occurs at the ATM itself is becoming more profitable and sophisticated. According to Diebold Nixdorf, the ATM manufacturers, ATM 'skimming,' now costs the global economy more than $2 billion. Skimming is the act of syphoning customer data at the ATM using hardware that mimics the appearance of legitimate machine components. The technology needed is easily available online for purchase.While methods and components vary greatly, skimming hardware is now more discreet and effective and is often very difficult to spot.

Jackpotting

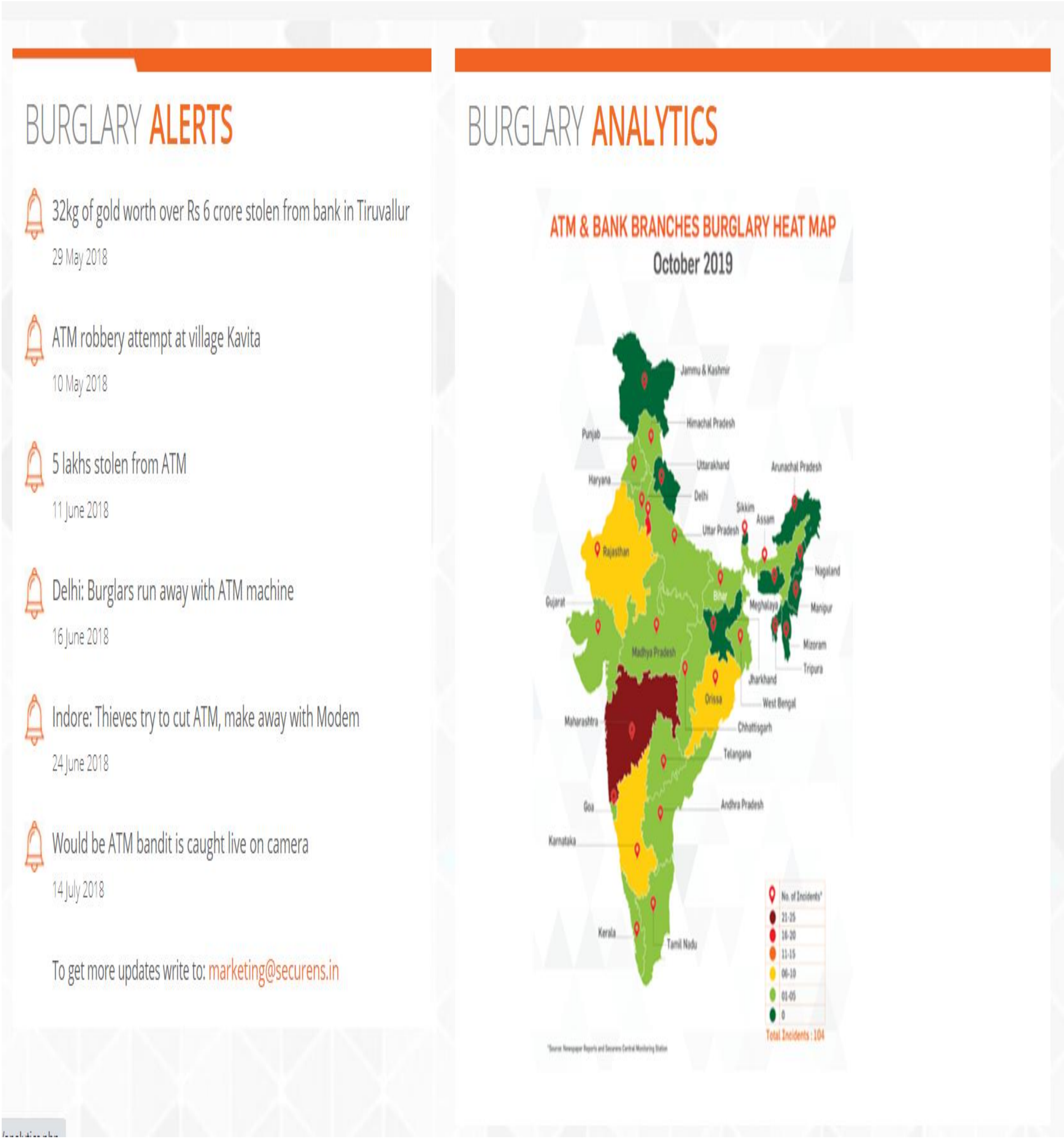
Jackpotting is the most sophisticated form of logical ATM. This approach involves infecting an ATM with malicious software. Any early form of this type of attack involved the transfer of malware to the ATM on a USB through an interface portal. Modes of infiltration have since become more effective and require even less involvement by the hacker.As recent research by EAST shows, 'black box' ATM attacks have been on the rise in Europe. To perform this type of attack, the perpetrator connects a device called 'black box' to the ATM's 'top box'. The device then reverts the machine to supervisor mode and dispenses cash. While the number of planned black box attacks in Europe have been increasing, the rates of criminal success have been decreasing .

Precautions

Money is the main driving force behind 90% of all cyberattacks and unsecure ATMs present a soft target for criminals. Hackers are always looking out for loopholes across the spectrum of bank IT infrastructures and endpoints. Banks cannot afford to ignore the dangers ATMs are vulnerable to as hackers often view ATMs as easy targets. And while unauthorised access might not always be preventable, restricting the extent of this infiltration is key.For instance, hacking using hijacked employee credentials has become prevalent in recent years. This issue can be mitigated by centrally securing privileged credentials with multi-factor authentication and controlling network access based on specific need.

Prevention

Banks have the responsibility to constantly monitor threat risks. This should involve a holistic approach to how vulnerabilities are identified and should include ATMs as a first line of defence. By constantly monitoring events and patterns one can more easily spot irregularities. If vigilance is constant, reaction times can become quicker to prevent the syphoning of data or access to cash funds by hackers.Today, ATMs require the same levels of rolling security provision and upgrading as every other aspect of bank infrastructure. Like all other forms of cybercrime, ATM attacks are changing and adapting all the time. It is therefore essential for banks to understand this threat



BURGLARY **ALERTS**

32kg of gold worth over Rs 6 crore stolen from bank in Tiruvallur

29 May 2018

ATM robbery attempt at village Kavita

10 May 2018

5 lakhs stolen from ATM

11 June 2018

Delhi: Burglars run away with ATM machine

16 June 2018

Indore: Thieves try to cut ATM, make away with Modem

24 June 2018

Would be ATM bandit is caught live on camera

14 July 2018

To get more updates write to: marketing@securens.in

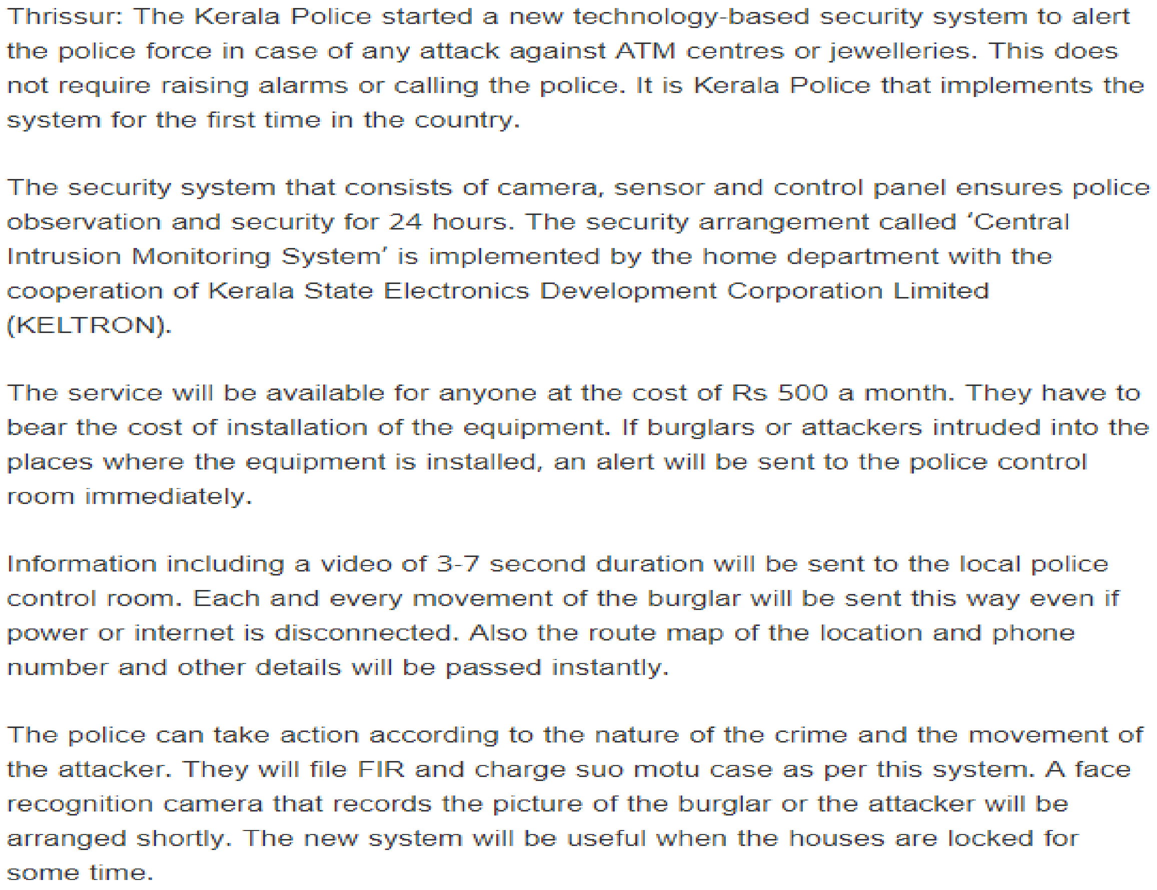
BURGLARY **ANALYTICS**

ATM & BANK BRANCHES BURGLARY HEAT MAP

October 2019

*Source: Newspaper Reports and Securens Central Monitoring Station

NEWS REPORT



Thrissur: The Kerala Police started a new technology-based security system to alert the police force in case of any attack against ATM centres or jewelleries. This does not require raising alarms or calling the police. It is Kerala Police that implements the system for the first time in the country.

The security system that consists of camera, sensor and control panel ensures police observation and security for 24 hours. The security arrangement called 'Central Intrusion Monitoring System' is implemented by the home department with the cooperation of Kerala State Electronics Development Corporation Limited (KELTRON).

The service will be available for anyone at the cost of Rs 500 a month. They have to bear the cost of installation of the equipment. If burglars or attackers intruded into the places where the equipment is installed, an alert will be sent to the police control room immediately.

Information including a video of 3-7 second duration will be sent to the local police control room. Each and every movement of the burglar will be sent this way even if power or internet is disconnected. Also the route map of the location and phone number and other details will be passed instantly.

The police can take action according to the nature of the crime and the movement of the attacker. They will file FIR and charge suo motu case as per this system. A face recognition camera that records the picture of the burglar or the attacker will be arranged shortly. The new system will be useful when the houses are locked for some time.

2.1.1 EXISTING SYSTEM

The attacks on ATM's are steadily rising and this is a serious problem for law enforcement and banking sectors.So there has to be a system developed and put into place that will make sure the ATM is safeguarded and also gives customers the confidence when using the ATM. Currently to provide protection to the ATM and to the customers using it, there are CCTV security cameras and emergency sirens. But the need of the hour is implementing a system which prevents the physical attacks made on the ATM which is rampantly increasing, using hardware devices.

Current Theft monitoring system in ATM:

- In this security system, whenever threat occurs, the ALARM (BUZZER) goes ON and hence the thief gets alerted and hence he may escape.It is one of the major drawback present.
- Incidents such as "Money snatching inside the ATM and breakage of ATM's", are increasing in numbers. Till now, no security systems can assure or provide 100 percent protection to the ATM.

DRAWBACK OF EXISTING SYSTEM

- Video surveillance systems traditionally consist of cameras attached to monitor screens. These systems are installed to give an overview of a large area to a limited number of operators. The goal is to detect abnormal situations.
- Operators often work in a room with lots of monitors.Their task is to watch constantly the monitors. If incidents happen, they warn the security or police. Some monitors show the video stream of a single camera and some show multiple streams on a single monitor simultaneously or sequentially.However, in some areas the monitors are not watched constantly.
- Video recorders record the output of each camera. After an incident, the video footage can be used as evidence. One obvious disadvantage of this approach is that operators are not able to prevent incidents or limit their damage,
- Another disadvantage is that it takes a significant amount of time to search for the right video images, especially when the suspect arrives at the scene hours before the incident and a large amount of cameras are involved.Moreover there is no continuous system for proper maintainance of ATM system components.

CHAPTER 3

OVERALL DESCRIPTION

3.1 PROPOSED SYSTEM

The proposed system employs proactive measures to counteract the burglary attempt, here the sensors of the system act as first line of defence and detects the break-in and take the protective actions which will deter the burglars from continuing with their attack, thereby successfully thwarting the attack. The proactive measures that are employed in the system are the siren, notification to officials using NodeMCU. Once any of the sensors are triggered the siren and the message will send to the authority and cause him to abandon the plot. Continues mointering is done through IOT platforms ThingSpeak and Blynk. In the proposed system we utilize this platform for mointering, analysis, visual representation, collecting of data and has many other features which help our proposed system more accurate in real time mointering. By stopping the attack, the ATM is prevented from bearing any more harm caused due to the physical attack.

3.2 FEATURES OF PROPOSED SYSTEM

- Continuous monitoring of the sensors in the system so that any burglary attempt is detected.
- Informing the controller that the sensors have been triggered and necessary safety actions are taken.
- Siren: The controller then activates the alarm system through the driver to dissuade the burglary attempt
- Warning: The controller then sends an alert and call alert to officials informing the break in happening using NodeMCU.
- Mointering of AC using Temperature and humidity sensor(DHT11) values.
- Real time mointering of each sensor values using IOT platforms ThingSpeak and Blynk.
- Graphical representation of sensor values, timeline, history can be viewed through ThingSpeak graphics chart.

3.3 FUNCTIONS OF PROPOSED SYSTEM

- Monitoring of ATM machine.
- Monitoring of CCTV visual and blockage.
- Monitoring AC damage using DHT11 sensor.
- Feature to monitor the power supply inside the ATM.
- Sending notification to the authority using NodeMCU module.
- Real time monitoring of sensor value using ThingSpeak and Blynk.

3.4 REQUIREMENTS SPECIFICATION

System analyst talk to a variety of persons to gather details about the business process and their opinions of why things happen as they do and their ideas for changing the process. These can be done through questionnaire, detailed investigation, observation, collection of samples etc. As the details are collected, the analyst study the requirements data to identify features the new system must have, including both the information the system should produce and operational features such as processing controls, response times and input-output methods.

Requirements specification simply means, "Figuring out what is to be made before making it." It determines what people need before starting to develop a product for them. Requirement definition is the activity of translating the information gathered in to a document that defines a set of requirements. These should reflect what consumer wants.

The requirements for an effective Smart ATM are as follows:

- A real-time monitoring system, to protect the ATM from attack.
- A system that will work in both daytime and nighttime conditions.
- Additionally, the other features that are implemented on the system must work efficiently.

The above requirements are subsequently the aims of this project. The project will consist of a concept level system that will meet all the above requirements

3.5 FEASIBILITY STUDY

The initial investigation points to be question whether the project is feasible. The feasibility study concerns with the considerations made to verify whether the system fit to be developed in all terms. Once the idea to develop the question that rises first will pertain to be the feasibility aspects. Feasibility study is a test of proposed system regarding its efficiency, its impact, ability to meet the need of bank security and whether it provide confidence to customers when using the ATM .

Thus, when a new project is proposed, it normally goes through a feasibility study before it is approved for development. A feasibility study is conducted to select the best system that meets the system performance requirements. This entitles an identification description, an evaluation of candidate system and the selection of the best system.

During system analysis, a feasibility study of the proposed system was carried out to see whether it was beneficial to the organization. Three key considerations that are involved in the feasibility study are,

- Technical Feasibility study
- Operational Feasibility study
- Economic Feasibility study
- Behavioural Feasibility study

3.5.1 TECHNICAL FEASIBILITY

The main objective of feasibility study is to test the technical, social and economic feasibility of developing a system. Investing the existing system in the area under investigation and generating ideas about the new system does this. Feasibility study has been done to gather required information. Training, experience and common sense are required for collection of the information. Data was gathered and checked for completeness and accuracy. Analysing the data involved identification of the components of the system and their interrelationship and identified the strength and weakness of the system. My system is developed by using Thing Speak, ArdunioUNO .It is technically feasible and it has lot of features as well as its secure too. So the technical part of this project is very secure. So my system is technically feasible.

3.5.2 OPERATIONAL FEASIBILITY

There is no difficulty in implementing the system. The proposed system is effective, user friendly and functionally. Even if the user of the system is completely unaware of the internal working of the system, users will not face any problem running the system. The system thus reduces the responsive time of computer thereby, the system is found to be operationally feasible**.** Design is the only ways that can accurately translate the user needs into finished system. Without software design, the risk of building an unstable system exists**.** System designprovides the procedural details necessary for implementing the system recommended in the feasibility study.

3.5.3 ECONOMIC FEASIBILITY

Economic and Financial analysis is used for evaluating the effectiveness of the system. The project is technically and operationally feasible. The software used for developing this system is ThingSpeak. The hardware consists of vibration sensors, humidity sensors, LDR and IR seensor,current sensor temperature sensors, an microcontroller,camera,GSM module, buzzer.The overall cost for making this prototype is considered as Rs 2000/- ThingSpeak is a free software so no cost is needed to buy the backend. My system is economically feasible because the project completed in few months. So less resources are used.

3.5.4 BEHAVIOUR FEASIBILITY

The behavioural feasibility depends upon whether the system performed in the expected way or not. Feasibility study is a test of system proposal according to it workability, impact on organization, ability to meet the user’s need and effective use of resources. However, a feasibility study provides a useful starting point for full analysis. My system is behaviorally feasible because of the effective use of the resources and also the system satisfied the user needs and the system is user friendly.

CHAPTER-4

OPERATING ENVIRONMENT

4.1 HARDWARE CONFIGURATIONS

The most common set of requirements defined by any operating system or software application is the physical computer resources, also known as hardware, A hardware requirements list is often accompanied by a hardware compatibility list (HCL), especially in case of operating systems. An HCL lists tested, compatible, and sometimes incompatible hardware devices for a particular operating system or application.

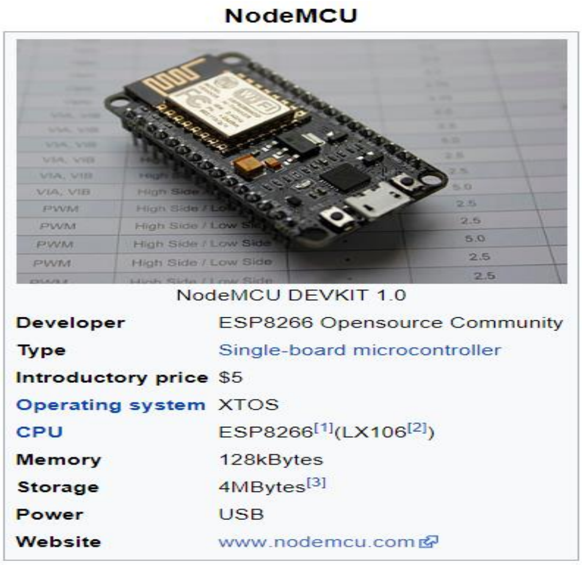
PROCESSOR	
SYSTEM	: PENTIUM IV 2.4 GHZ
MEMORY	
TOTAL RAM	:1GB
STORAGE	
HARD DISK	:250GB
FLOPPY DRIVE	: 1.44 MB
INPUT DEVICES	
KEYBOARD	:110 KEYS ENHANCED
MOUSE	:LOGITECH. OPTICAL MOUSE
OUTPUT DEVICES	
MONITOR	:15 VGA COLOUR
PRINTER	:DESKJET D2460C
EXTERNAL HARDWARE	
BOARD	: NODE MCU
SENSORS	: VIBRATION SENSOR LDR SENSOR DHT11 SENSOR

4.1.1 HARDWARE REQUIREMENTS

NODE MCU

NodeMCU is an open source firmware for which open source prototyping board designs are available. The name "NodeMCU" combines node and "MCU" (micro-controller unit). The term "NodeMCU" strictly speaking refers to the firmware rather than the associated development kits.Both the firmware and prototyping board designs are open source.The firmware uses the Luascripting language. The firmware is based on the eLua project, and built on the Espress if Non-OS SDK for ESP8266. It uses many open source projects, such as lua-cjson and SPIFFS. Due to resource constraints, users need to select the modules relevant for their project and build a firmware tailored to their needs. Support for the 32-bit ESP32has also been implemented.

The prototyping hardware typically used is a circuit board functioning as a dual in-line package(DIP) which integrates a USB controller with a smaller surface-mounted board containing the MCU and antenna. The choice of the DIP format allows for easy prototyping on breadboards. The design was initially was based on the ESP-12 module of the ESP8266, which is a Wi-Fi SoC integrated with a Tensilica Xtensa LX106 core, widely used in IoT application.

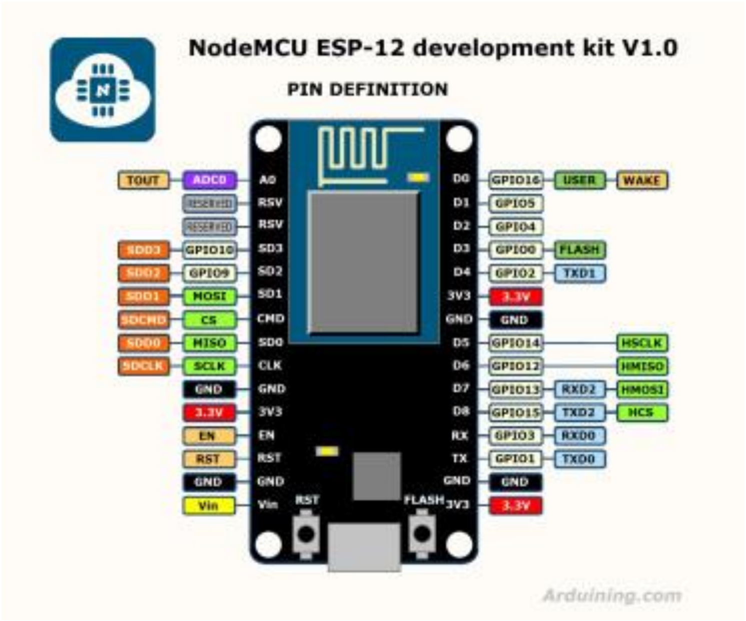


NodeMCU

NodeMCU DEVKIT 1.0

Developer	ESP8266 Opensource Community
Type	Single-board microcontroller
Introductory price	$5
Operating system	XTOS
CPU	ESP8266[1](LX106[2])
Memory	128kBytes
Storage	4MBytes[3]
Power	USB
Website	www.nodemcu.com

Fig 4.1: Node MCU



Vibration sensor

The **vibration sensor** is also called a piezoelectric **sensor**. These **sensors** are flexible devices which are used for measuring various processes. This **sensor** uses the piezoelectric effects while measuring the changes within acceleration, pressure, temperature, force otherwise strain by changing to an electrical charge.

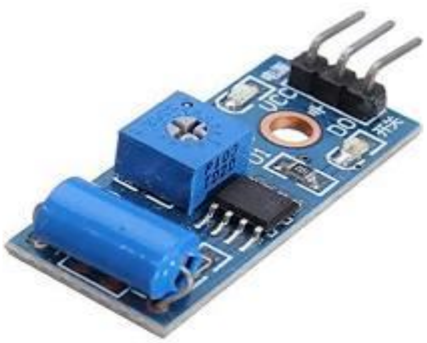


Fig 4.2: Viberation sensor

Working principle

The working principle of vibration sensor is a sensor which operates based on different optical otherwise mechanical principles for detecting observed system vibrations.The sensitivity of these sensors normally ranges from 10 mV/g to 100 mV/g, and there are lower and higher sensitivities are also accessible. The sensitivity of the sensor can be selected based on the application. So it is essential to know the levels of vibration amplitude range to which the sensor will be exposed throughout measurements.

LDR

In order to detect the intensity of light or darkness, we use a sensor called an LDR (light dependent resistor). The LDR is a special type of resistor that allows higher voltages to pass through it (low resistance) whenever there is a high intensity of light, and passes a low voltage (high resistance) whenever it is dark.

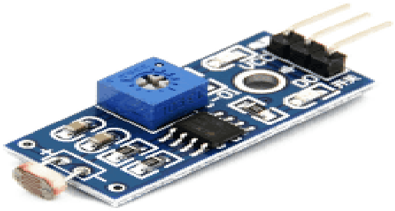
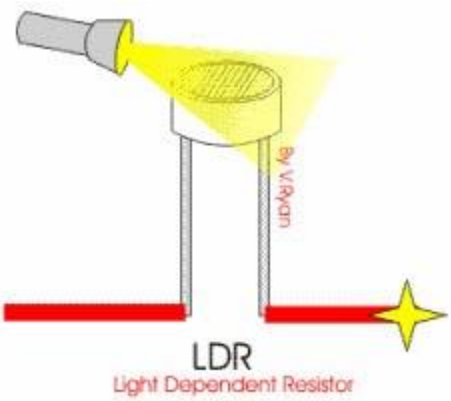


Fig 4.3 :LDR

Working principle

This resistor works on the principle of photo conductivity. It is nothing but, when the light falls on its surface, then the material conductivity reduces and also the electrons in the valence band of the device are excited to the conduction band. These photons in the incident light must have energy greater than the band gap of the semiconductor material.This makes the electrons to jump from the valence band to conduction.



Working Principle of LDR

These devices depend on the light, when light falls on the LDR then the resistance decreases, and increases in the dark.When a LDR is kept in the dark place, its resistance is high and, when the LDR is kept in the light its resistance will decrease.

Temperature and humidity sensor(DHT11)

A **temperature sensor** is an electronic device that measures the **temperature** of its environment and converts the input data into electronic data to record, monitor, or signal **temperature** changes.

A **humidity sensor** is a device that detects and measures water vapor. Based on our robust capacitive technology, these **humidity sensors** provide accurate measurement of dew point and absolute **humidity** by combining relative **humidity** (RH) and temperature (T) measurements.

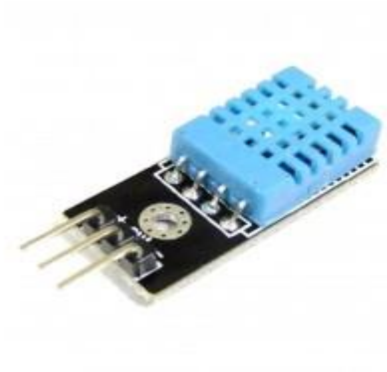
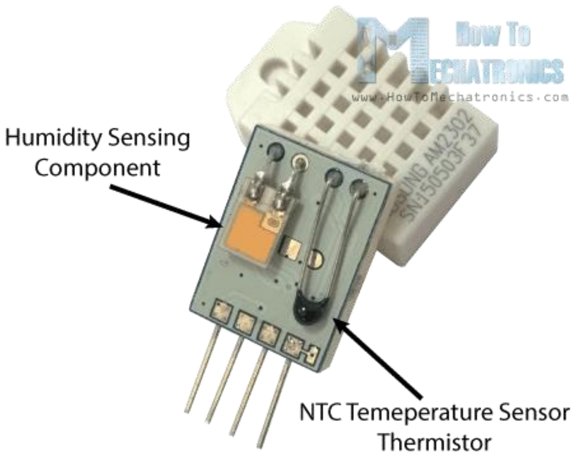
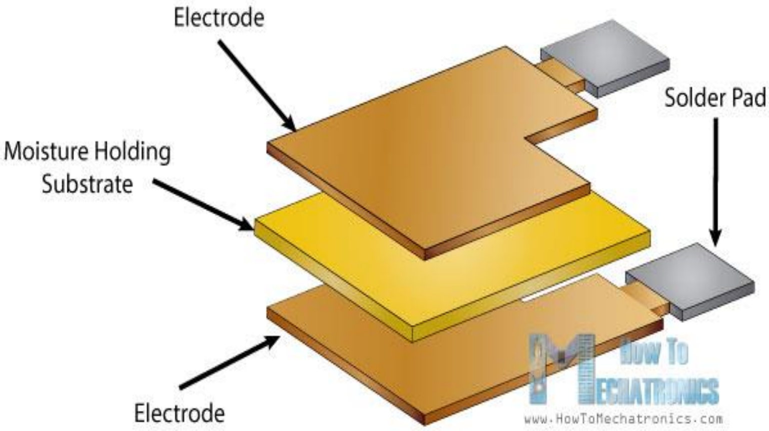


Fig 4.4 DHT11

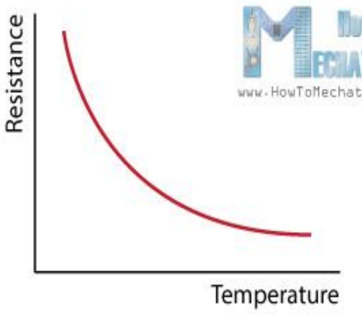
They consist of a humidity sensing component, a NTC temperature sensor (or thermistor) and an IC on the back side of the sensor.

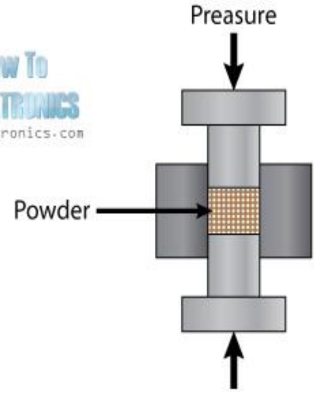

How To
MECHATRONICS
www.HowToMechatronics.com
Humidity Sensing Component
NTC Temeperature Sensor Thermistor
AOSONG AM2302
SN150503F37

For measuring humidity they use the humidity sensing component which has two electrodes with moisture holding substrate between them. So as the humidity changes, the conductivity of the substrate changes or the resistance between these electrodes changes. This change in resistance is measured and processed by the IC which makes it ready to be read by a microcontroller.



On the other hand, for measuring temperature these sensors use a NTC temperature sensor or a thermistor.A thermistor is actually a variable resistor that changes its resistance with change of the temperature. These sensors are made by sintering of semiconductive materials such as ceramics or polymers in order to provide larger changes in the resistance with just small changes in temperature. The term "NTC" means "Negative Temperature Coefficient", which means that the resistance decreases with increase of the temperature.





Buzzer

A **buzzer** or beeper is an audio signaling device

4.2 SOFTWARE REQUIREMENTS

A software requirements specification (SRS) is a description of a software system to be developed. The software requirements are description of features and functionalities of the target system. Requirements convey the expectations of users from the software product. The requirements can be obvious or hidden, known or unknown, expected or unexpected from client's point of view.

SOFTWARE	**THING SPEAK, ARDUNIO IDE, BLYNK**	ThingSpeak™ IoT Analytics with MATLAB® Blynk ARDUINO IDE
OPERATING SYSTEM	**WINDOWS 10**	Windows 10
LANGUAGE	**EMBEDDED C**	Embedded Programming C
DATABASE	**THINGSPEAK**	ThingSpeak™ IoT Analytics with MATLAB®

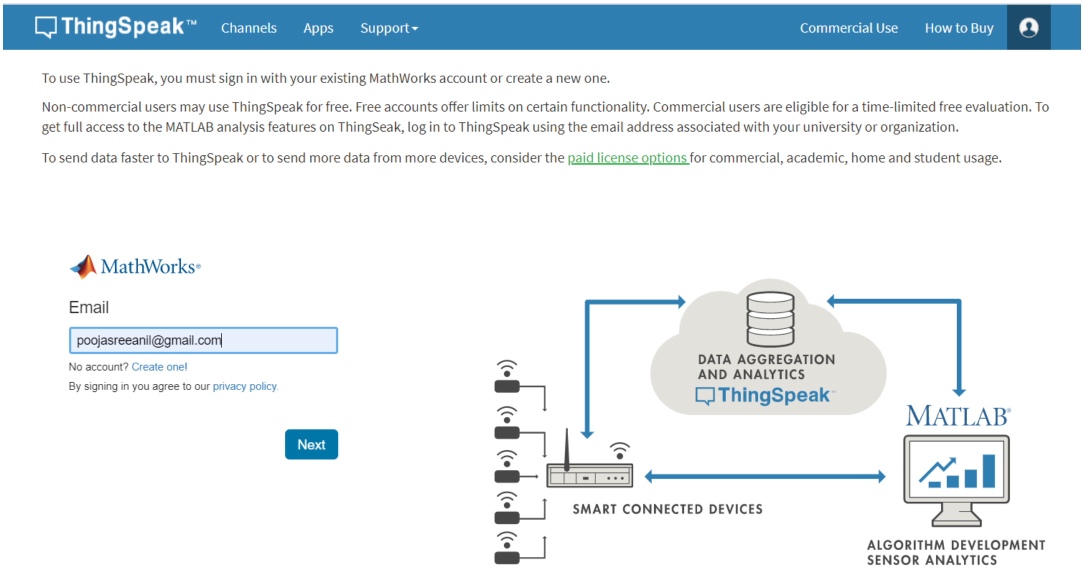
4.3 TOOLS AND PLATFORMS

THING SPEAK

ThingSpeak is a platform providing various services exclusively targeted for building applications. It offers the capabilities of real-time data collection, visualizing the collected data in the form of charts, ability to create plugins and apps for collaborating with web services, social network and other APIs..The core element of ThingSpeak is a 'ThingSpeak Channel'.

To use ThingSpeak, we need to signup and create a channel. Once we have a channel, we can send the data, allow ThingSpeak to process it and also retrieve the same. ThingSpeak allows you to aggregate, visualize and analyze live data streams in the cloud. Some of the key capabilities of ThingSpeak include the ability to:

- Easily configure devices to send data to ThingSpeak using popular IoT protocols.
- Visualize your sensor data in real-time.
- Aggregate data on-demand from third-party sources.
- Use the power of MATLAB to make sense of your IoT data.
- Run your IoT analytics automatically based on schedules or events.
- Prototype and build IoT systems without setting up servers or developing web software.
- Automatically act on your data and communicate using third-party services like Twitter.



To use ThingSpeak, you must sign in with your existing MathWorks account or create a new one.

Non-commercial users may use ThingSpeak for free. Free accounts offer limits on certain functionality. Commercial users are eligible for a time-limited free evaluation. To get full access to the MATLAB analysis features on ThingSpeak, log in to ThingSpeak using the email address associated with your university or organization.

To send data faster to ThingSpeak or to send more data from more devices, consider the paid license options for commercial, academic, home and student usage.

MathWorks

Email: poojasreeanil@gmail.com

No account? Create one!

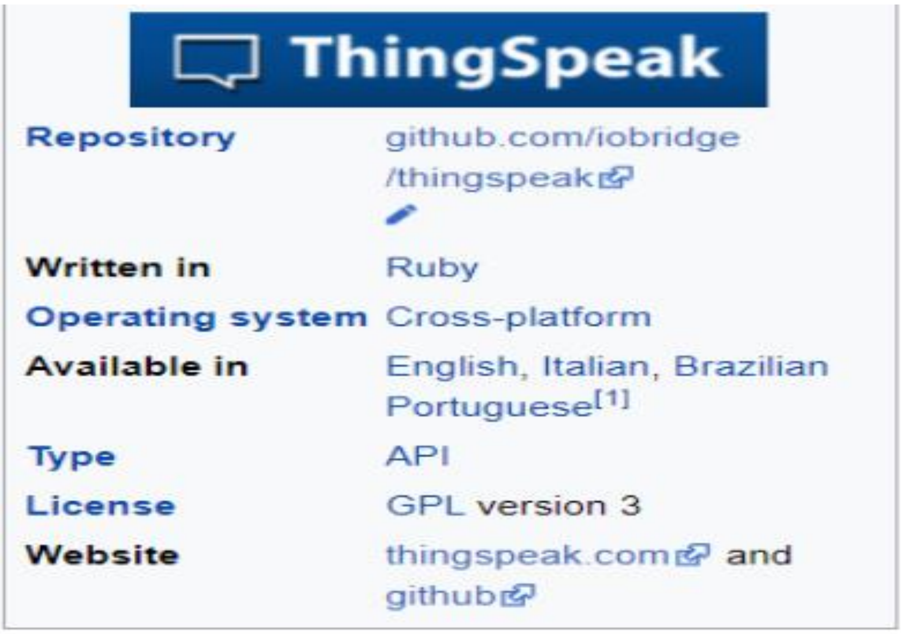
By signing in you agree to our privacy policy.

Procedure

Collect : Send sensor data privately to the cloud.

Analyze: Analyze and visualize your data with MATLAB.

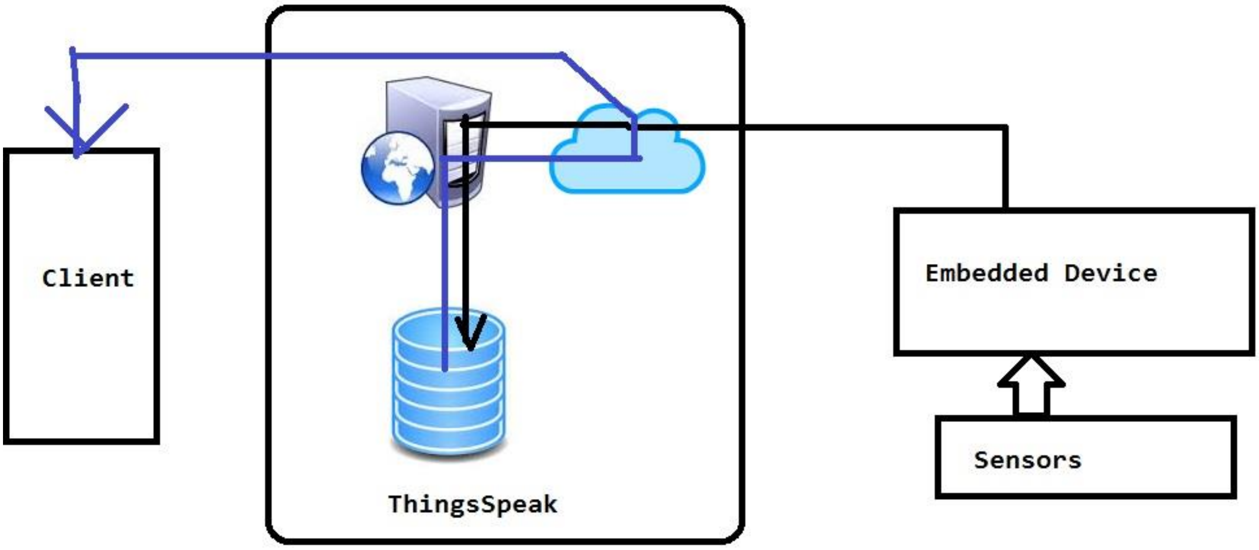
Act: Trigger a reaction.



ThingSpeak

Repository	github.com/iobridge/thingspeak
Written in	Ruby
Operating system	Cross-platform
Available in	English, Italian, Brazilian Portuguese[1]
Type	API
License	GPL version 3
Website	thingspeak.com and github

THING SPEAK ARCHITECTURE



THINGSPEAK IOT PLATFORM

CHANNEL VISUALIZATION: The system uses ThingSpeak IoT platform for monitoring the data. The system uses channels for monitoring the data from each ATM. Android app named ThingChart is used to visualize and monitor the data through a smart phone.

REACT APP: React app Send a tweet or trigger a ThingHTTP request when the Channel meets a certain condition. In this project when the viberation sensor,LDR sensor,DHT11 sensor of any ATM is triggered it triggers ThingTweet to send warning message to the control room, The react app is also used to trigger the ThingHTTP app to warn by sending messages.

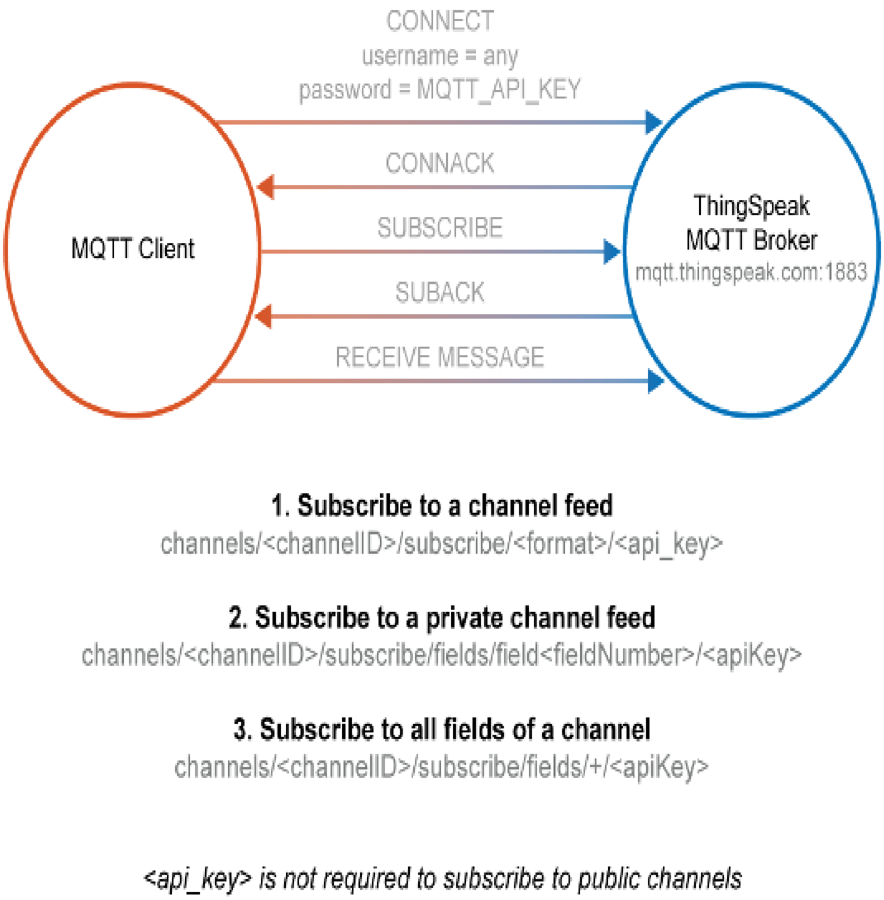
THINGHTTP APP: ThingHTTP enables communication among devices, websites, and web services without having to implement the protocol on the device level. It is done using the GET, PUT, POST and DELETE methods of HTTP

TALKBACK APP: TalkBack is used to queue up commands and then allow a device to act upon these queued commands. TalkBack API is used to add, get and execute a TalkBack command, which can be accessed by ThingHTTP app. In this project TalkBack app is used to add commands for device control based on time or twitter message.

PROTOCOLS

MQTT

MQTT is a common protocol used in IoT systems to connect low-level devices and sensors. MQTT is used to pass short messages to and from a broker. ThingSpeak has recently added an MQTT broker so devices can send messages to ThingSpeak. A message might contain the current temperature in an office collected by a sensor. ThingSpeak takes the message and stores its content in a ThingSpeak channel. Once the data is in a channel, you can easily visualize and analyze the data with MATLAB code.



1. Subscribe to a channel feed
channels/<channelID>/subscribe/<format>/<api_key>

2. Subscribe to a private channel feed
channels/<channelID>/subscribe/fields/field<fieldNumber>/<apiKey>

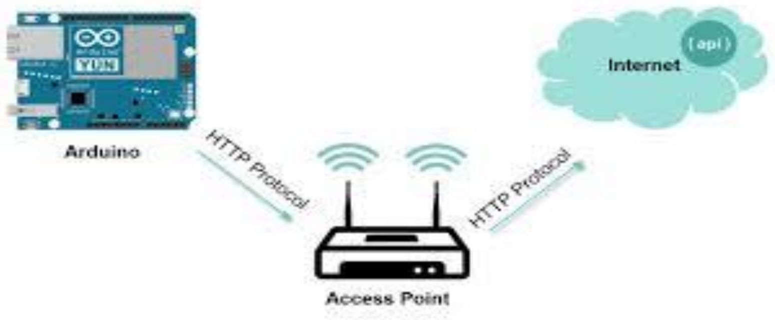
3. Subscribe to all fields of a channel
channels/<channelID>/subscribe/fields/+/<apiKey>

<api_key> is not required to subscribe to public channels

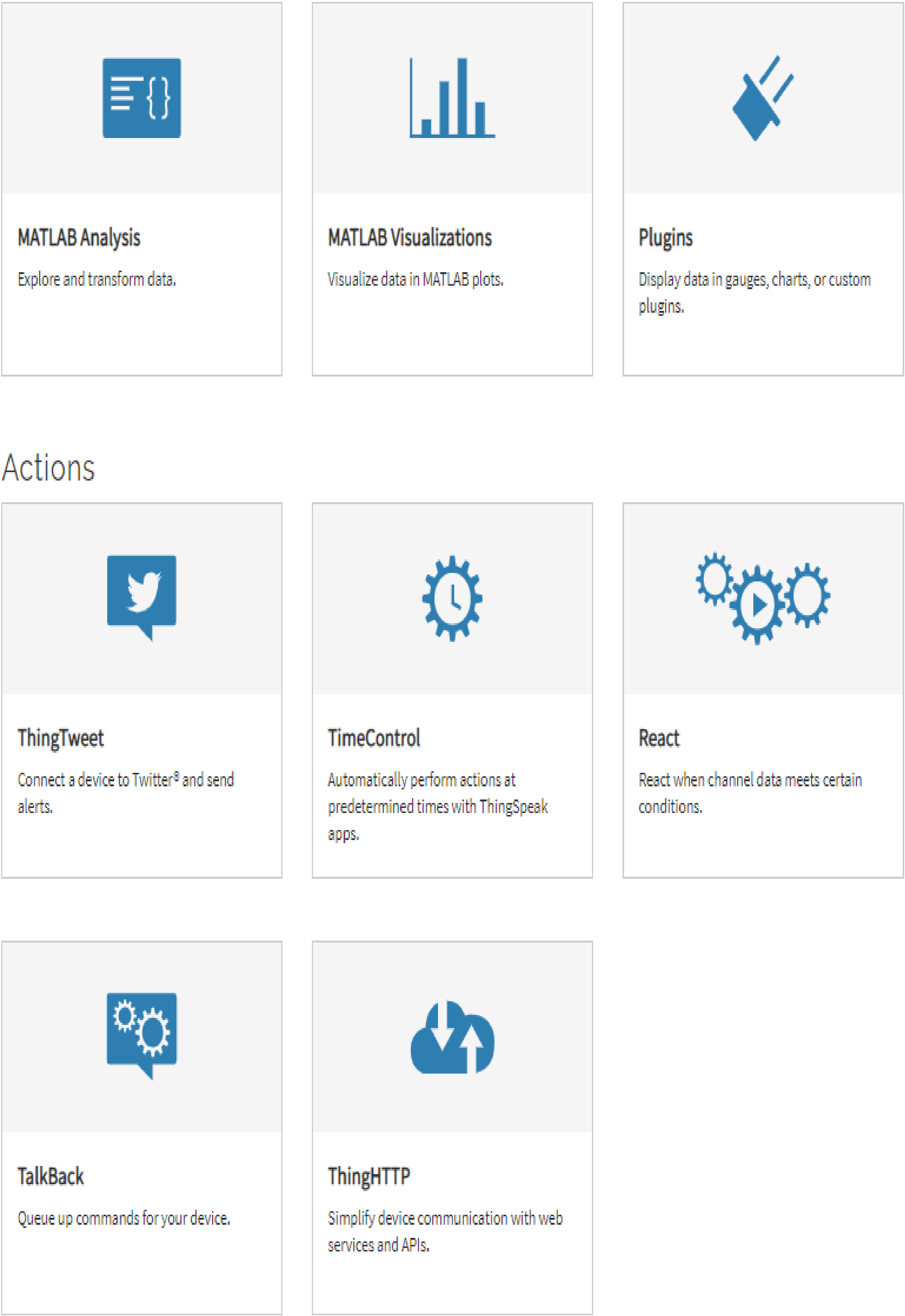
HTTP(Hyper Text Transfer Protocol)

The ThingHTTP App allow a microcontroller or low level device to connect to any web service using HTTP over internet.We can create an HTTP object using ThingHTTP app and then control the object using simple API commands.

ThingSpeak supports GET,POST,PUT,DELETE method.we have a device interface with many web services and API without having to implementing on the device level.



FEATURES



MATLAB Analysis

Explore and transform data.

MATLAB Visualizations

Visualize data in MATLAB plots.

Plugins

Display data in gauges, charts, or custom plugins.

Actions

ThingTweet

Connect a device to Twitter® and send alerts.

TimeControl

Automatically perform actions at predetermined times with ThingSpeak apps.

React

React when channel data meets certain conditions.

TalkBack

Queue up commands for your device.

ThingHTTP

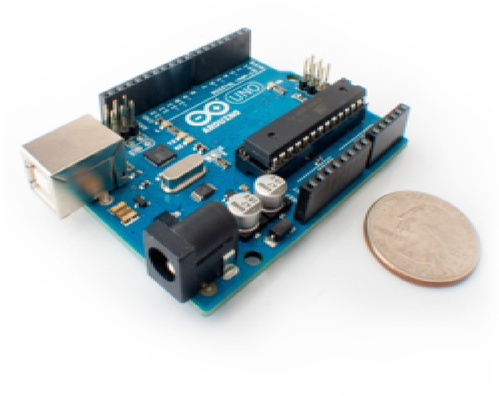
Simplify device communication with web services and APIs.

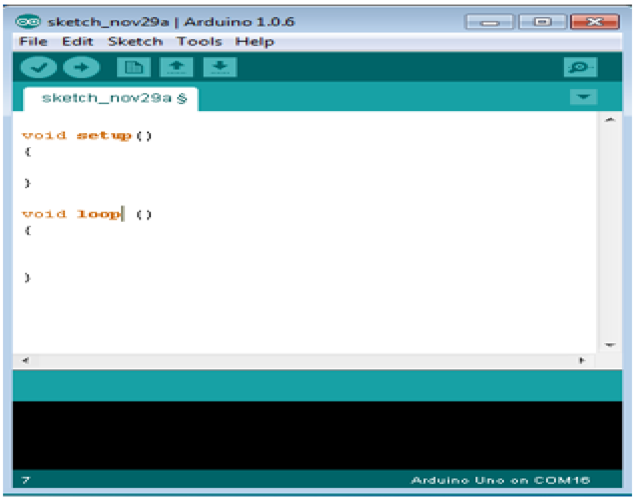
ARDUNIO IDE

Arduino is a prototype platform (open-source) based on an easy-to-use hardware and software. It consists of a circuit board, which can be programed (referred to as a microcontroller) and a ready-made software called Arduino IDE (Integrated Development Environment), which is used to write and upload the computer code to the physical board.

The key features are −

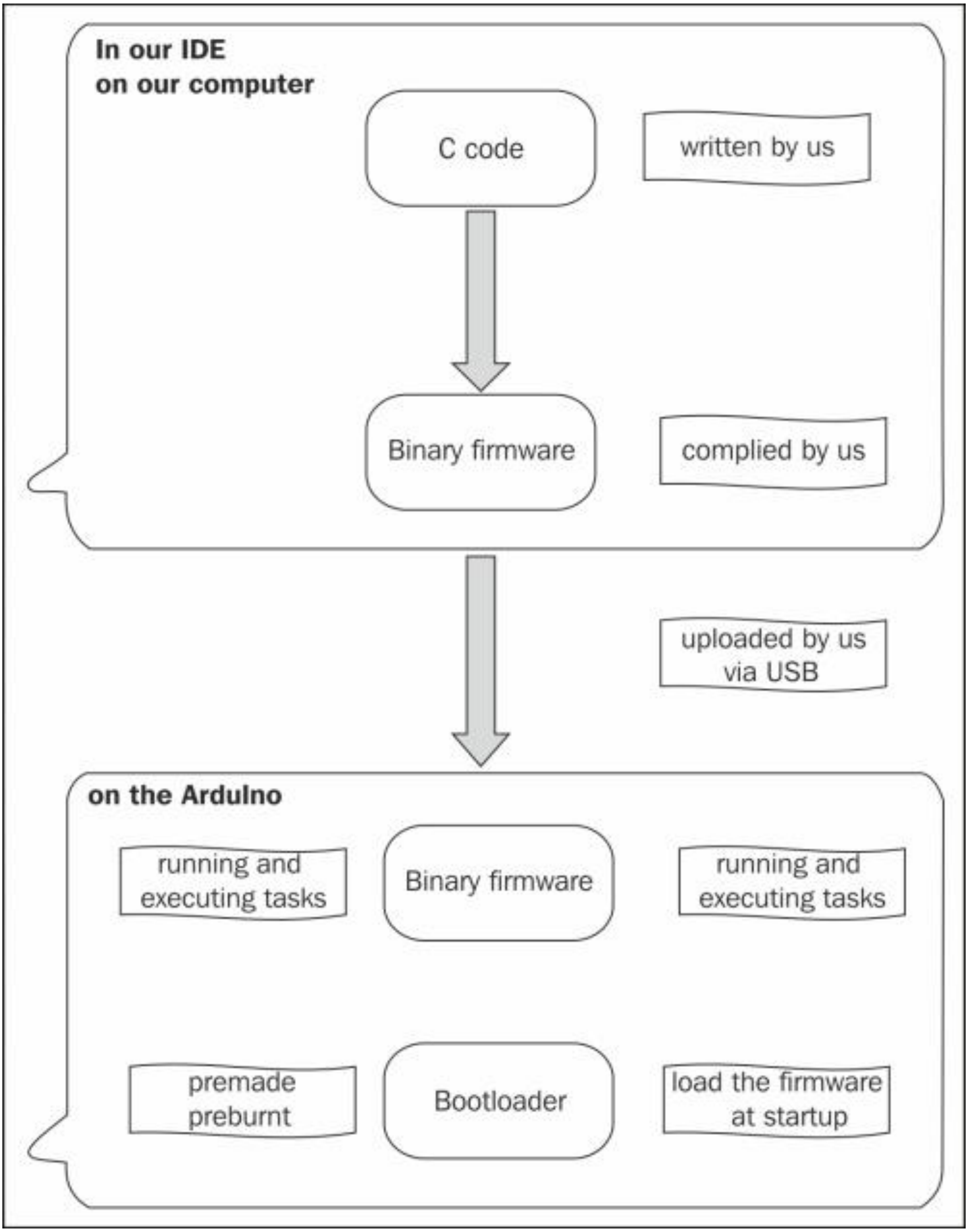
- Arduino boards are able to read analog or digital input signals from different sensors and turn it into an output such as activating a motor, turning LED on/off, connect to the cloud and many other actions.
- You can control your board functions by sending a set of instructions to the microcontroller on the board via Arduino IDE (referred to as uploading software).
- Unlike most previous programmable circuit boards, Arduino does not need an extra piece of hardware (called a programmer) in order to load a new code onto the board. You can simply use a USB cable.
- Additionally, the Arduino IDE uses a simplified version of C++, making it easier to learn to program.
- Finally, Arduino provides a standard form factor that breaks the functions of the micro-controller into a more accessible package.



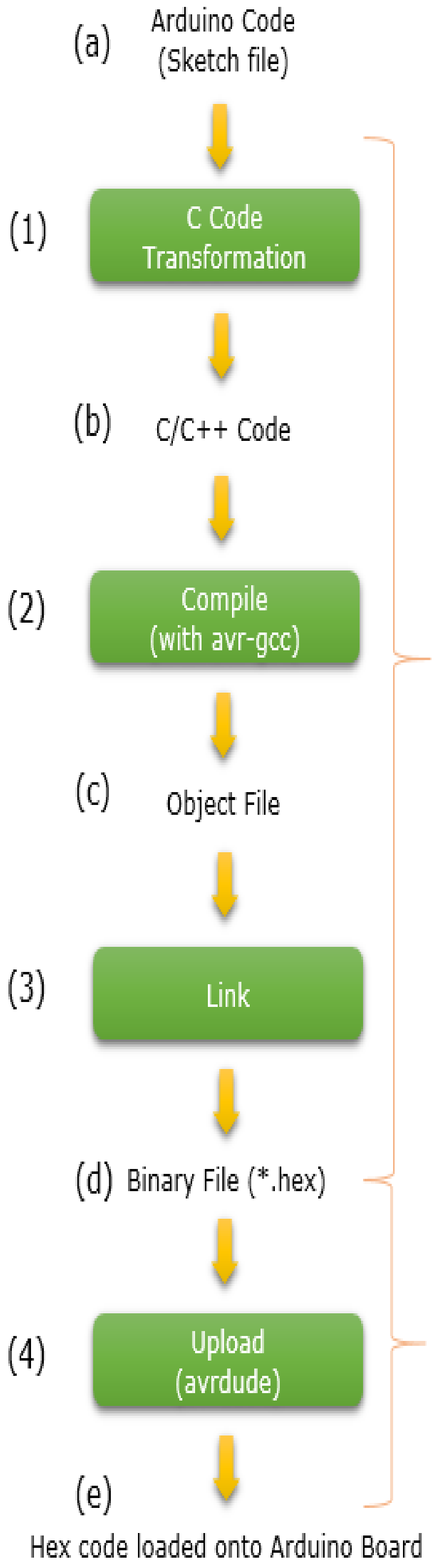


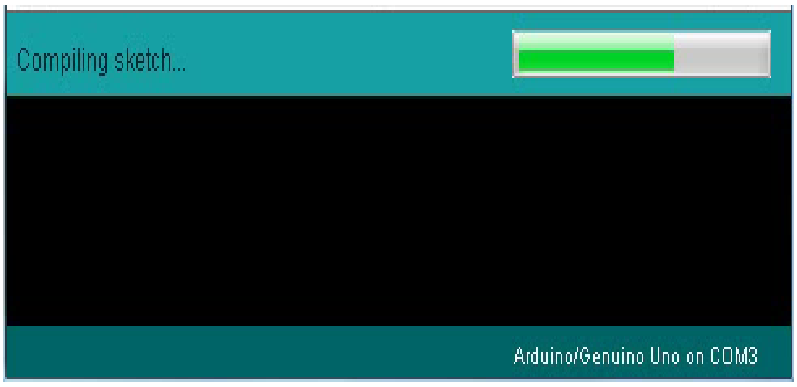
```
void setup()
{

}

void loop()
{


}
```

ARCHITECTURE

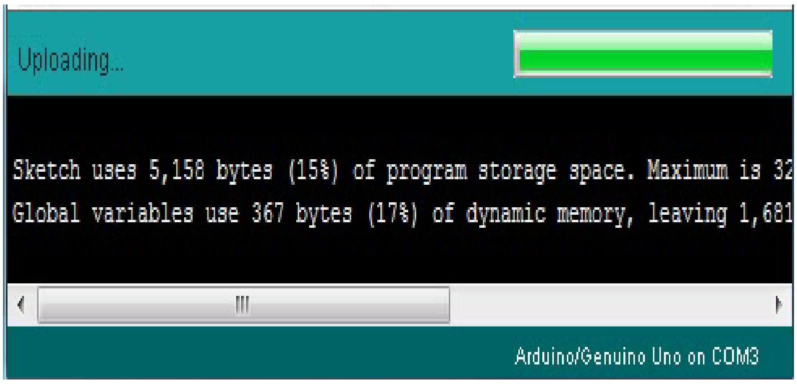


HOW IDE WORKS?



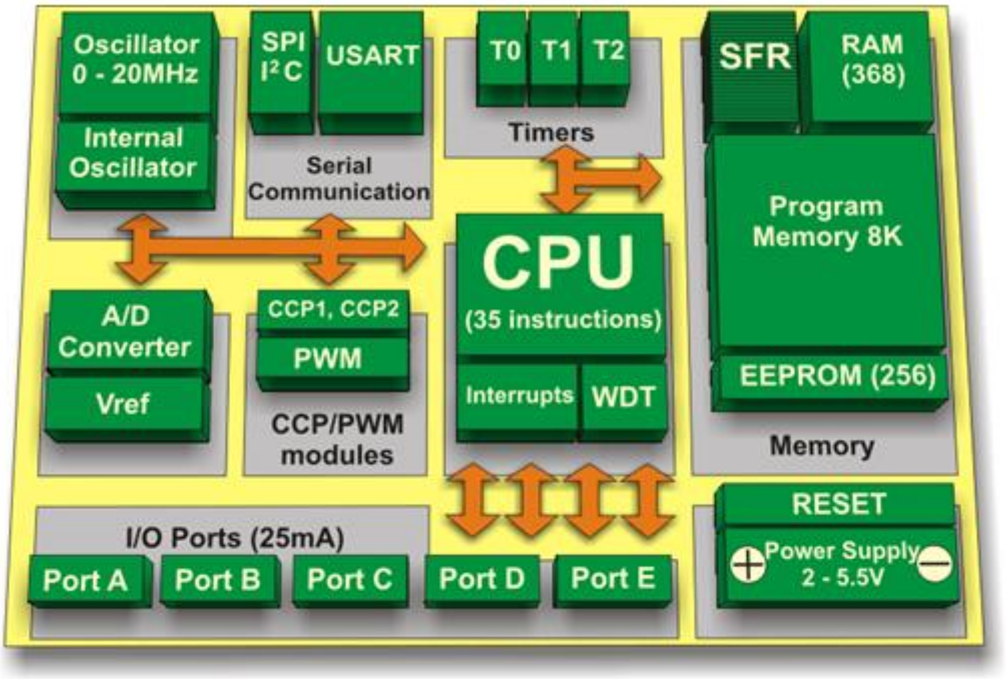


```
Compiling sketch...
```

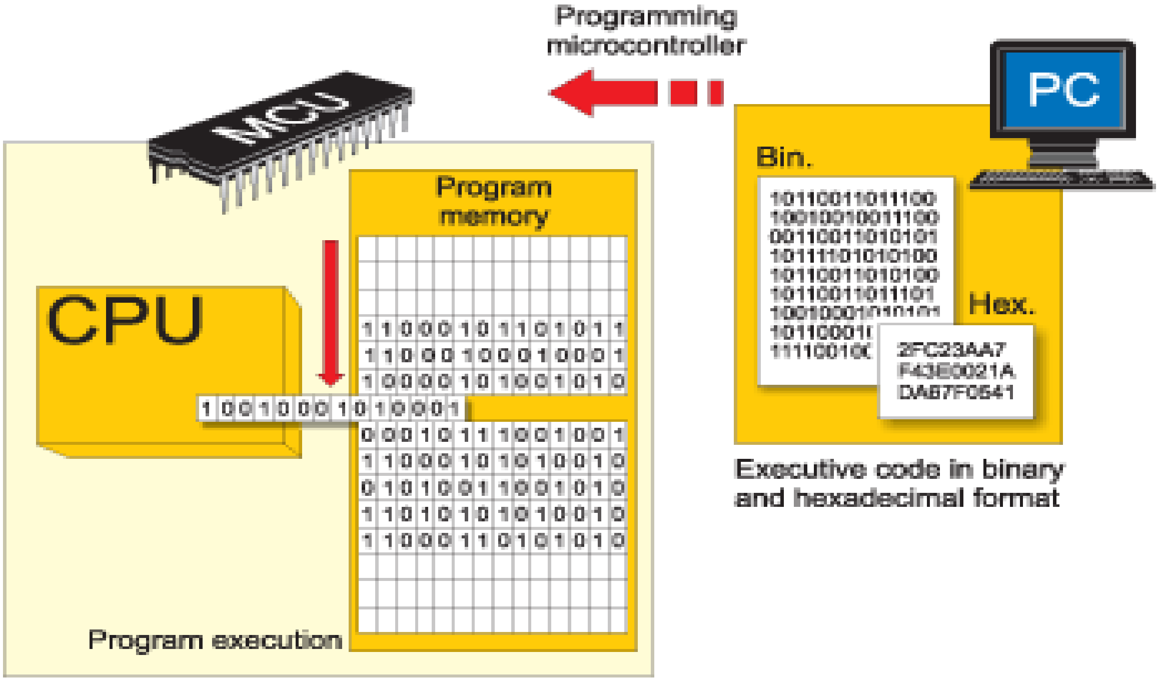


```
Uploading...

Sketch uses 5,158 bytes (15%) of program storage space. Maximum is 32
Global variables use 367 bytes (17%) of dynamic memory, leaving 1,681
```

MICROCONTROLLER ARCHITECTURE:

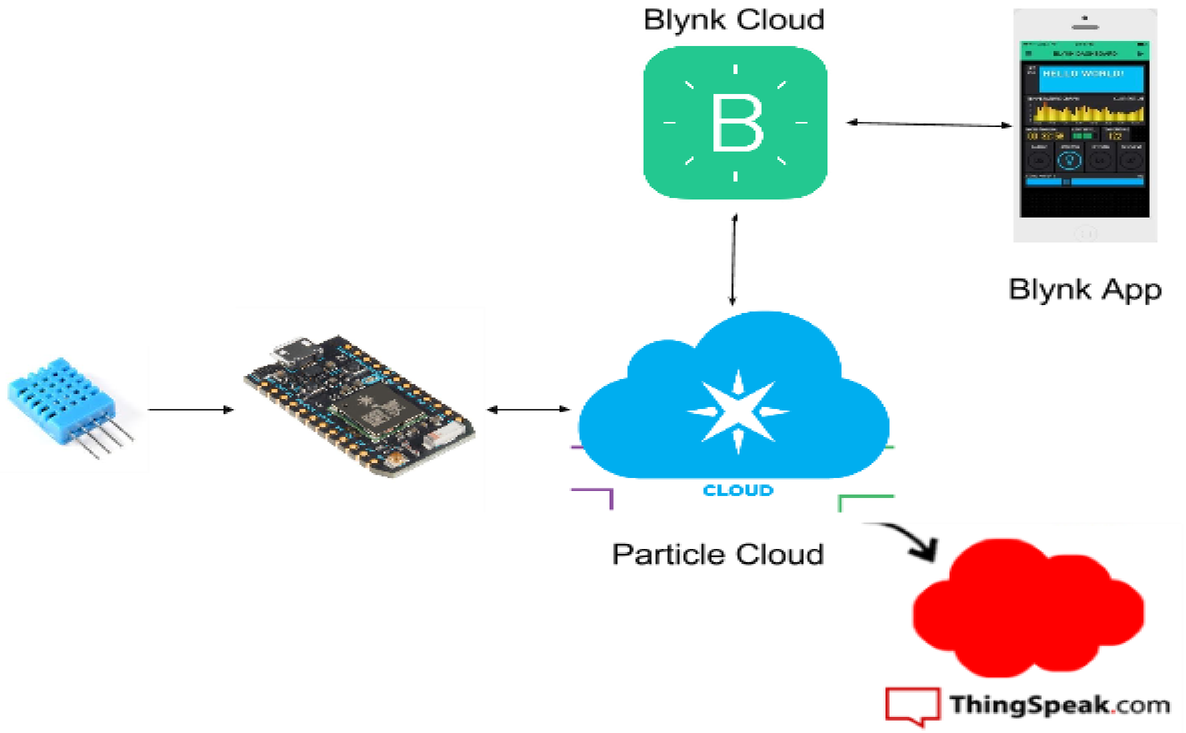


HOW MICROCONTROLLER WORKS?



BLYNK

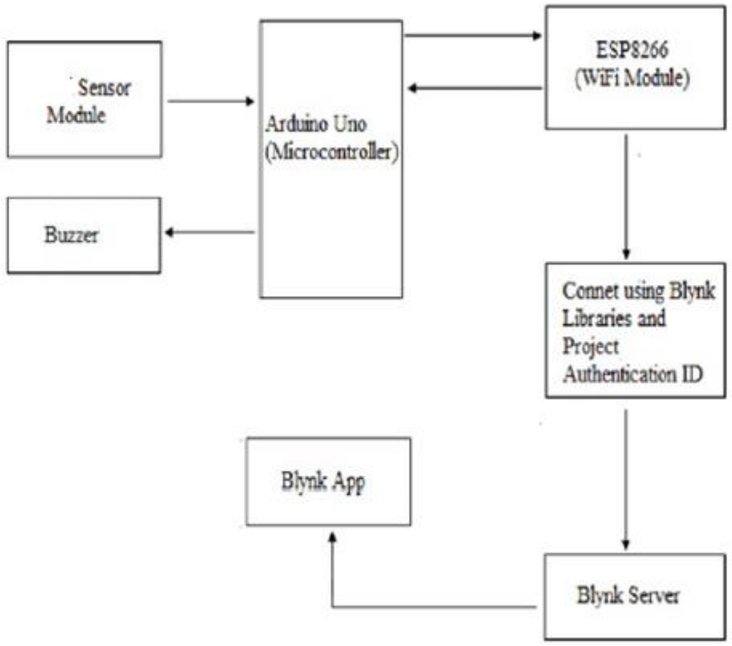
Blynk is a new platform that allows you to quickly build interfaces for controlling and monitoring hardware projects from iOS and Android device. After downloading the Blynk app, we can create a project dashboard and arrange buttons, sliders, graphs, and other widgets onto the screen. Using the widgets, you can turn pins on and off or display data from sensors.



BLYNK ARCHITECTURE

The Blynk platform includes the following components:

- **Blynk app builder**: Allows to you build apps for your projects using various widgets. It is available for Android and iOS platforms.
- **Blynk server**: Responsible for all the communications between your mobile device that's running the Blynk app and the hardware. You can use the Blynk Cloud or run your private Blynk server locally. It's open source, could easily handle thousands of devices, and can even be launched on a Raspberry Pi.
- **Blynk libraries**: Enables communication with the server and processes all the incoming and outcoming commands from your Blynk app and the hardware. They are available for all the popular hardware platforms.


Sensor Module
Buzzer
Arduino Uno (Microcontroller)
ESP8266 (WiFi Module)
Connet using Blynk Libraries and Project Authentication ID
Blynk App
Blynk Server

EMBEDDED C

Embedded C is a set of language extensions for the C Programming language by the C Standards committee to address commonality issues that exist between C extensions for different embedded systems. Historically, embedded C programming requires nonstandard extensions to the C language in order to support exotic features such as fixed-point arithmetic, multiple distinct memory banks, and basic I/O operations. In 2008, the C Standards Committee extended the C language to address these issues by providing a common standard for all implementations to adhere to. It includes a number of features not available in normal C, such as, fixed-point arithmetic, named address spaces, and basic I/O hardware addressing. Embedded C uses most of the syntax and semantics of standard C, e.g., main() function, variable definition, data type declaration, conditional statements (if, switch case), loops (while, for), functions, arrays and strings, structures and union, bit operations, macros, etc.

CHAPTER 5

DESIGN

5.1 SYSTEM DESIGN

System design involves translating system requirements and conceptual design into technical specifications and general flow of processing. After the system requirements have been identified, information has been gathered to verify the problem and after evaluating the existing system, a new system is proposed. System design is the process of planning of new system or to replace or complement an existing system. It must be thoroughly understood about the old system and determine how computers can be used to make its operations more effective. There are two levels of system design:

- Logical design.
- Physical design.

In the logical design, the designer produces a specification of the major features of the system which meets the objectives. The delivered product of logical design includes current requirements of the following system components:

- Input design.
- Program design
- Output design
- Database design

Physical design takes this logical design blue print and produces the program software, files and a working system. Design specifications instruct programmers about what the system should do. The programmers in turn write the programs that accept input from users, process data, produce reports and store data in files.

5.1.1 Activity Diagram and Flow Chart

i. Block Diagram

A block diagram is a diagram of a system in which the principal parts or functions are represented by blocks connected by lines that show the relationships of the blocks. They are heavily used in engineering in hardware design, electronic design, software design, and process flow diagrams. Block diagrams are typically used for higher level, less detailed descriptions that are intended to clarify overall concepts without concern for the details of implementation. Contrast this with the schematic diagrams and layout diagrams used in electrical engineering, which show the implementation details of electrical components and physical construction.

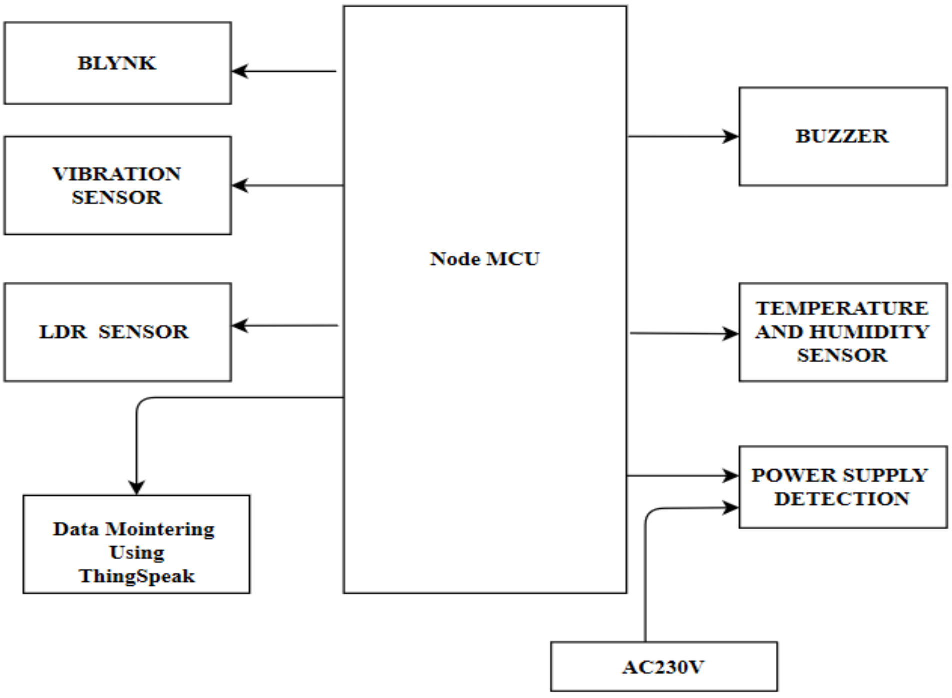


Figure 5.1: Block Diagram

Block Diagram Description

In this project we have two modules

Hardware Module

Software Module

Hardware Module

In this module, we use a microcontroller Node MCU, Viberation Sensor, LDR sensor ,DHT11 Sensor as hardware module.

NODE MCU stands for Node Microcontroller Unit is an Open source software and hardware development environment.

Viberation sensor which is placed inside the atm machine mointers each minute if any value triggerd during the attack msg automatically send message to blynk and email.Continous mointering is done through the ThingSpeak platform.

LDR sensor is used for the CCTV mointering ,It act as obstacle detector if the attacker block the CCTV visuals.

DHT11 is used for AC mointering.If the value became higher than the specified degree it automatically take corresponding action.

Power failure detection can be calculated from the circuit using ThingSpeak.If it fail message send through Blynk and Email.

Software Module

ThingSpeak which is an open source IOT and API to store sensor value,perform action and display output in graphical form at web level.

Blynk which is a new platform for making Quick interface for our hardware project.

WORKING

FOR CCTV AND ATM PROTECTION

- When an attacker enter the ATM ,if he try to hide the CCTV visual then LDR used here is for CCTV Mointering.when he hide the CCTV camera density of light decreases and resistance increases.with this principle we implement the technique to mointer CCTV Camera is working or not.

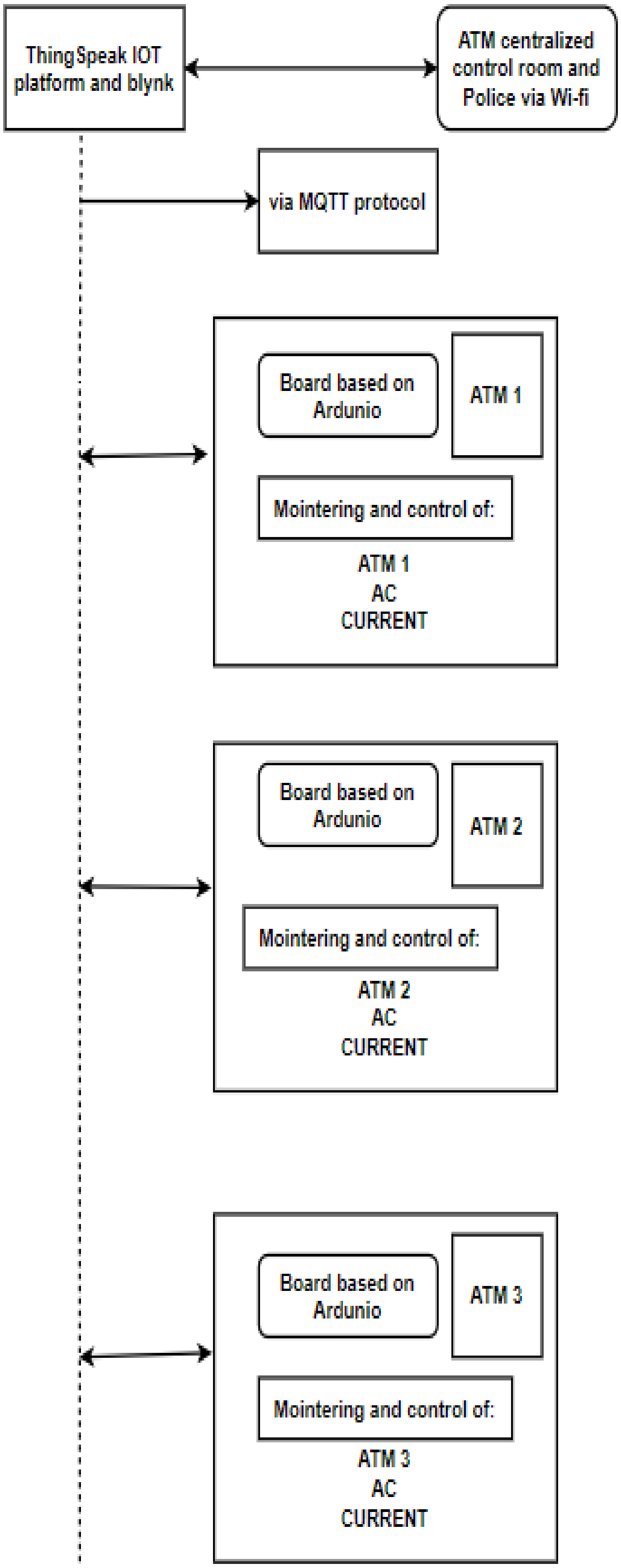
- If attacker attack the ATM, the ,value of the viberation sensor inside the ATM start to triggered.When value triggered isystem dentified it as an attack and take corresponding action.

MOINTERING AC AND POWER

- DHT11 which is a temperature and humidity sensor which is used to measure amount of humidity and temperature inside the ATM .If temperature and humidity value increases than the specified limit it means the AC is not working properly and automatically send message via blynk.
- To check power supply,We can check whether current is present in the circuit or not using ThingSpeak.

SYSTEM ARCHITECTURE

The system architecture of the proposed system is shown in figure . The system consists ATMs from different places and mointering platform IOT and Blynk. The smart atm are connected to WiFi and communicate to the server via MQTT protocol. The architecture of the proposed system is as follows. The Smart ATM system consists of multiple sensors to monitor the environment and security conditions. The value of sensor data is used to control devices or to trigger an alarm. The sensor data would be sent to ThingSpeak IoT platform using MQTT protocol. The data will be visualized in charts and can also trigger various activities like sending alert message via twitter or alert other homes based on various conditions. The user can monitor the security and environmental conditions of their respective ATM via smartphone. using Blynk.


ThingSpeak IOT platform and blynk
ATM centralized control room and Police via Wi-fi
via MQTT protocol
Board based on Ardunio
ATM 1
Mointering and control of:
ATM 1
AC
CURRENT
Board based on Ardunio
ATM 2
Mointering and control of:
ATM 2
AC
CURRENT
Board based on Ardunio
ATM 3
Mointering and control of:
ATM 3
AC
CURRENT

ii. Flow Chart

A flowchart is a type of diagram that represents a workflow or process. A flowchart can also be defined as a diagrammatic representation of an algorithm, a step-by-step approach to solving a task. The flowchart shows the steps as boxes of various kinds, and their order by connecting the boxes with arrows. This diagrammatic representation illustrates a solution model to a given problem. Flowcharts are used in analyzing, designing, documenting or managing a process or program in various fields

Components of Flowchart

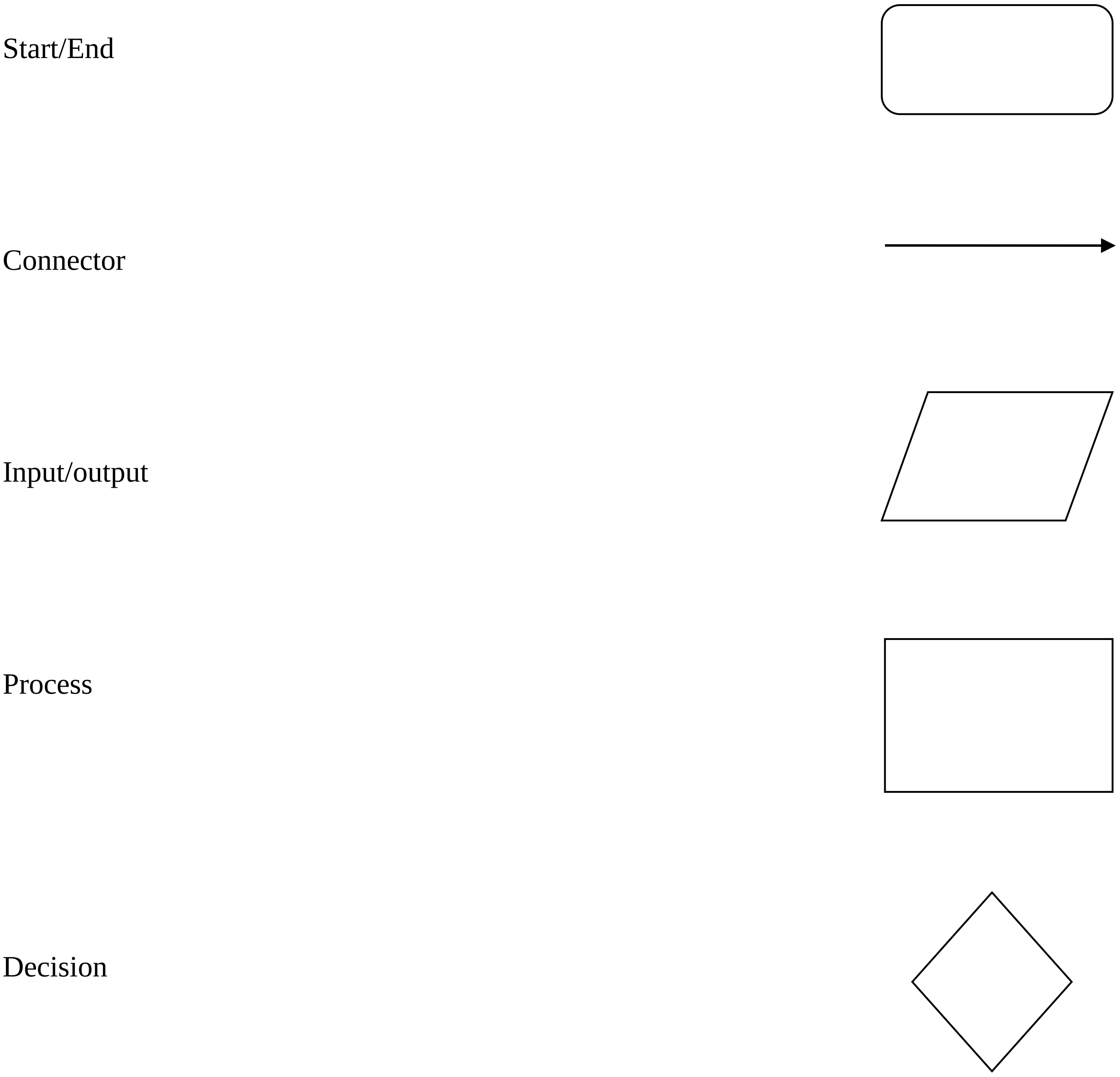
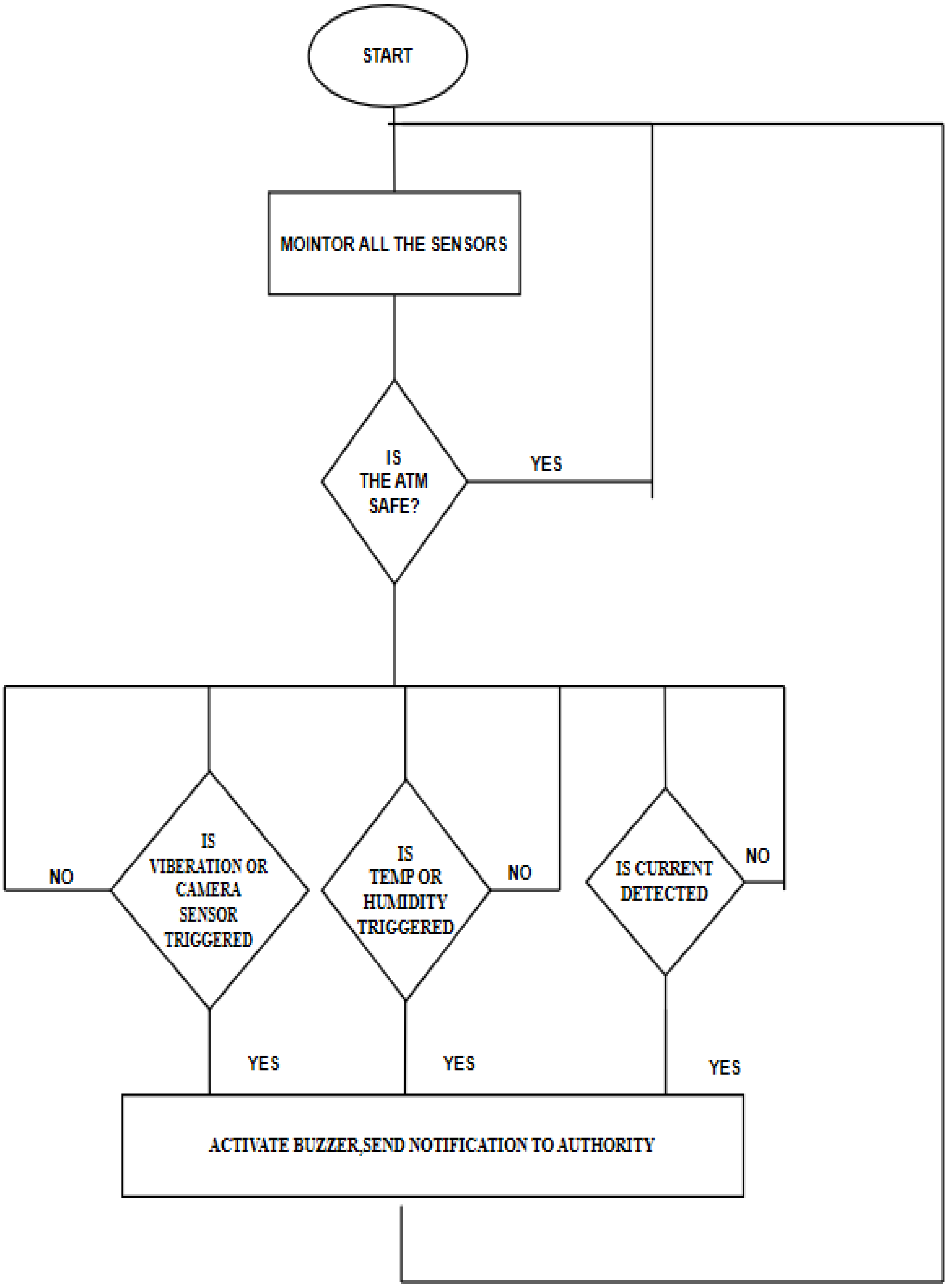


Figure 5.1.2 Components of flow chart


START
MOINTOR ALL THE SENSORS
IS THE ATM SAFE?
YES
NO
IS VIBERATION OR CAMERA SENSOR TRIGGERED
IS TEMP OR HUMIDITY TRIGGERED
NO
IS CURRENT DETECTED
NO
YES
YES
YES
ACTIVATE BUZZER,SEND NOTIFICATION TO AUTHORITY

iii. Activity Diagram

An activity diagram is a UML behavior diagram that represents the workflow of stepwise activities of the system. Activity diagram is basically a flowchart to represent the flow from one activity to another activity. The activity can be described as an operation of the system. The control flow is drawn from one operation to another. UML models basically three types of diagrams, namely, structure diagrams, interaction diagrams, and behavior diagrams. An activity diagram is a behavioral diagram i.e. it depicts the behavior of a system. An activity diagram is used by developers to understand the flow of programs on a high level.

- Components of Activity Diagram

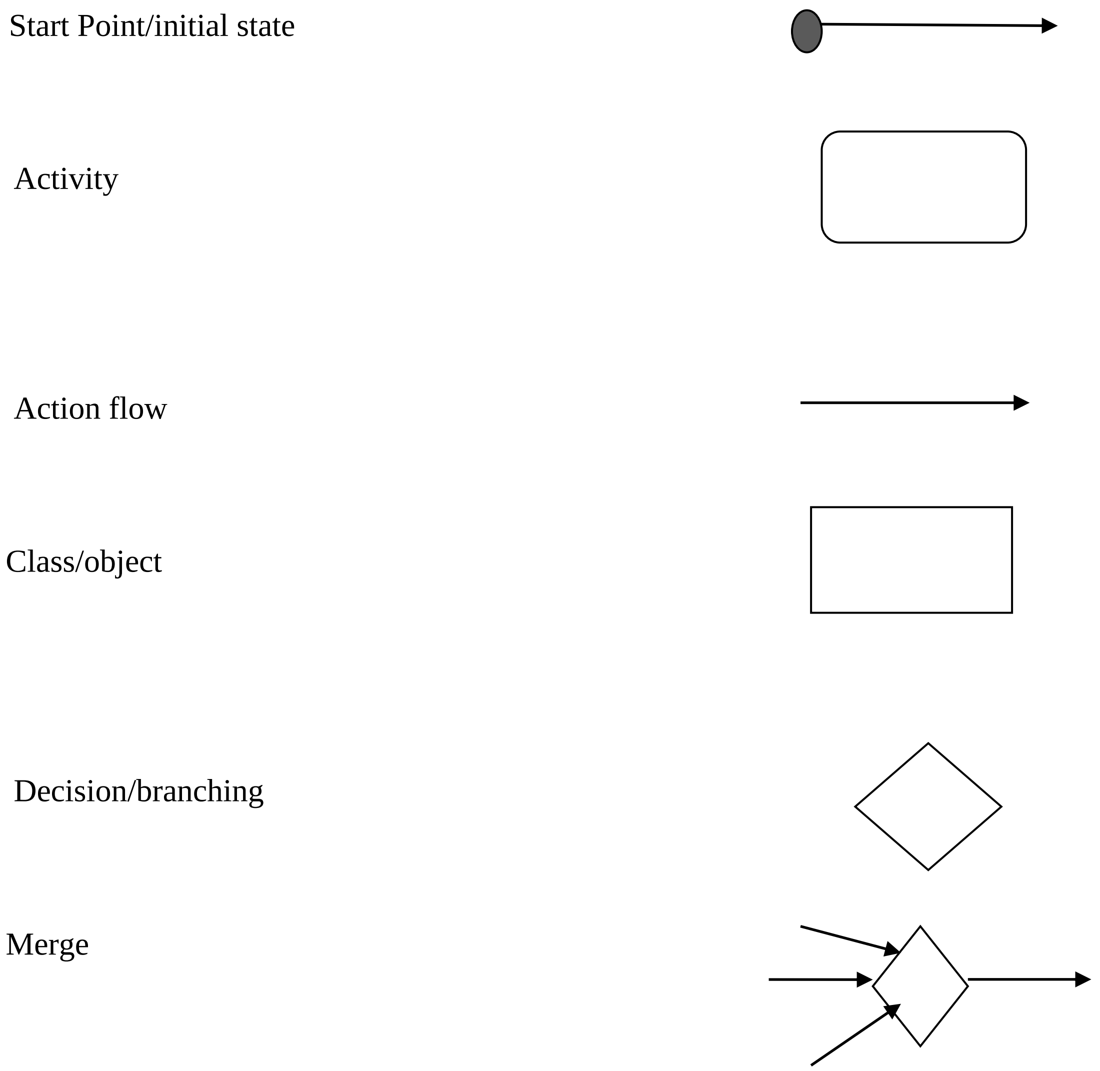
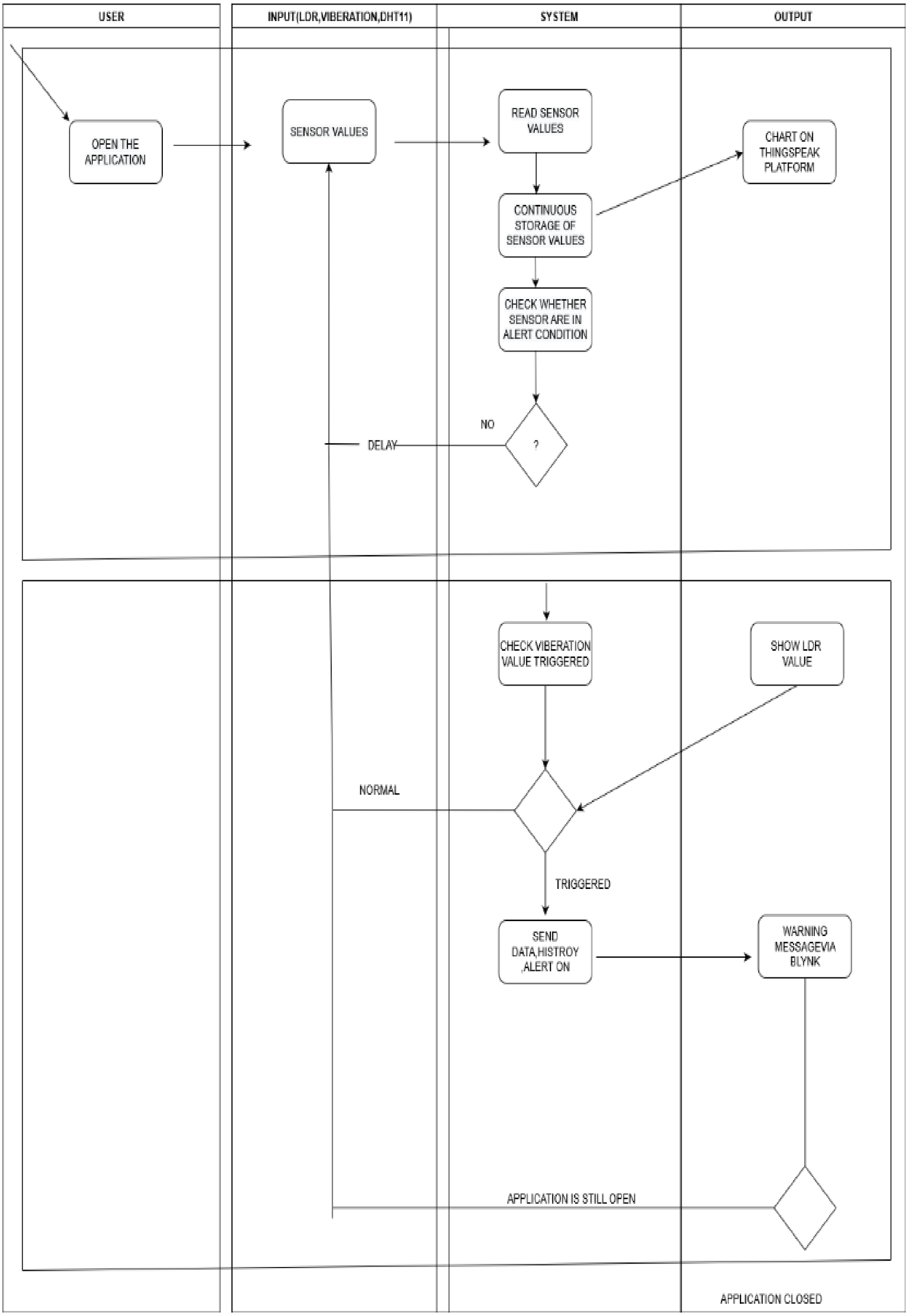


Fig 5.1.1 Components of activity diagram

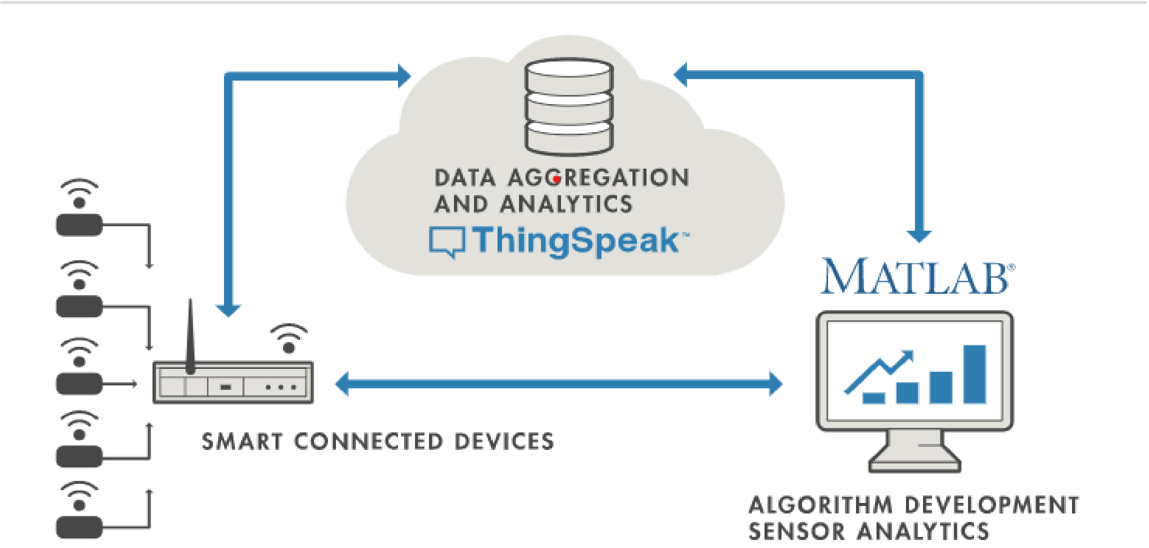

USER
INPUT(LDR,VIBERATION,DHT11)
SYSTEM
OUTPUT
OPEN THE APPLICATION
SENSOR VALUES
READ SENSOR VALUES
CHART ON THINGSPEAK PLATFORM
CONTINUOUS STORAGE OF SENSOR VALUES
CHECK WHETHER SENSOR ARE IN ALERT CONDITION
NO
DELAY
?
CHECK VIBERATION VALUE TRIGGERED
SHOW LDR VALUE
NORMAL
TRIGGERED
SEND DATA,HISTROY ,ALERT ON
WARNING MESSAGEVIA BLYNK
APPLICATION IS STILL OPEN
APPLICATION CLOSED

5.2 DATABASE DESIGN

The most important aspect of building software systems is database design. The highest level in the hierarchy is the database. It is a set of inter-related files for real time processing. It contains the necessary data for problem solving and can he used by several users accessing data concurrently. The general objective of database design is to make the data access easy, inexpensive and flexible to the user. Database design is used to define and then specify the structure of business used in the client/server system. A business object is nothing but information that is visible to the users of the system.

Database Name: ThingSpeak

Description : Store the values from Sensor and histroical time.



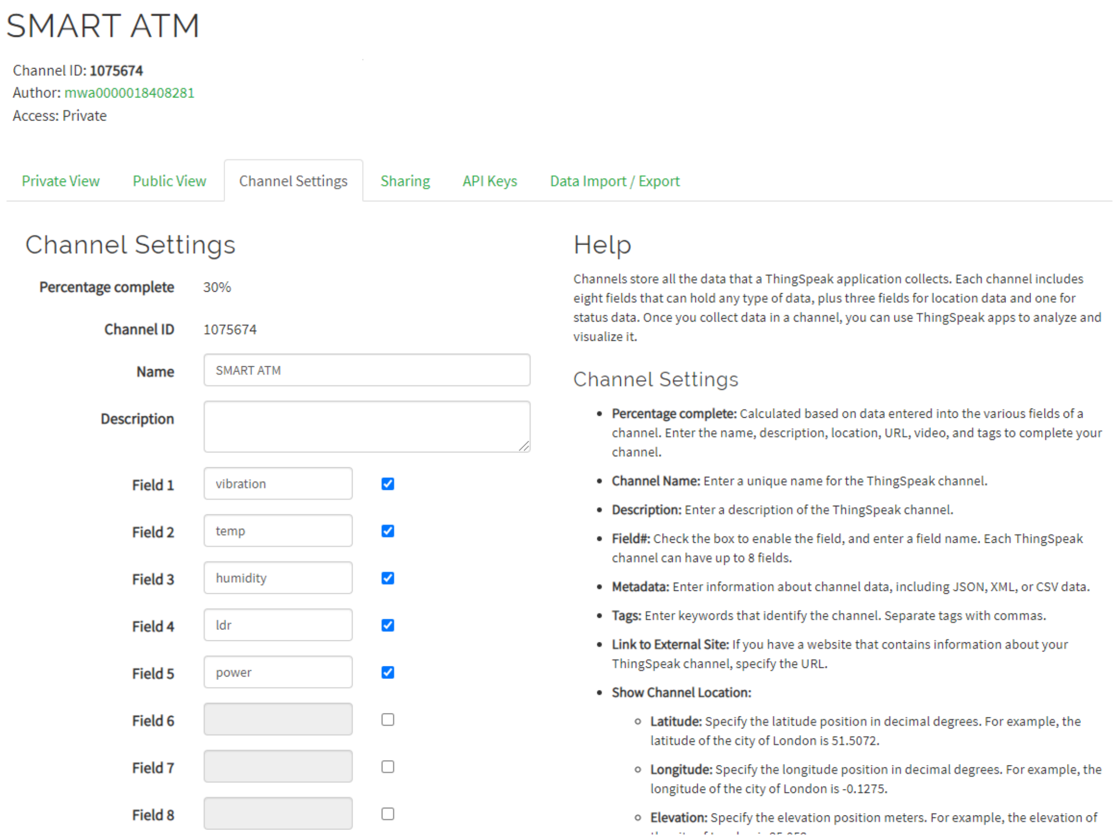
5.3INPUT DESIGN

The input design is the process of converting the user oriented inputs in to the computer based format. The goal of designing input data is to make automation as easy and free from errors as possible. The input design requirements such as user friendliness, consistent format and interactive dialogue for giving the right message and help for the user at right time are also considered for the development of the project. The input design is the link between the information system and the user.

Hardware inputs are:

- Vibration Sensor
- LDR
- DHT11 Sensor
- Power supply

Input form:



SMART ATM

Channel ID: **1075674**
Author: mwa0000018408281
Access: Private

Channel Settings

Percentage complete	30%	
Channel ID	1075674	
Name	SMART ATM	
Description		
Field 1	vibration	☑
Field 2	temp	☑
Field 3	humidity	☑
Field 4	ldr	☑
Field 5	power	☑
Field 6		□
Field 7		□
Field 8		□

Help

Channels store all the data that a ThingSpeak application collects. Each channel includes eight fields that can hold any type of data, plus three fields for location data and one for status data. Once you collect data in a channel, you can use ThingSpeak apps to analyze and visualize it.

Channel Settings

- **Percentage complete:** Calculated based on data entered into the various fields of a channel. Enter the name, description, location, URL, video, and tags to complete your channel.
- **Channel Name:** Enter a unique name for the ThingSpeak channel.
- **Description:** Enter a description of the ThingSpeak channel.
- **Field#:** Check the box to enable the field, and enter a field name. Each ThingSpeak channel can have up to 8 fields.
- **Metadata:** Enter information about channel data, including JSON, XML, or CSV data.
- **Tags:** Enter keywords that identify the channel. Separate tags with commas.
- **Link to External Site:** If you have a website that contains information about your ThingSpeak channel, specify the URL.
- **Show Channel Location:**
    - **Latitude:** Specify the latitude position in decimal degrees. For example, the latitude of the city of London is 51.5072.
    - **Longitude:** Specify the longitude position in decimal degrees. For example, the longitude of the city of London is -0.1275.
    - **Elevation:** Specify the elevation position meters. For example, the elevation of

5.4 OUTPUT DESIGN

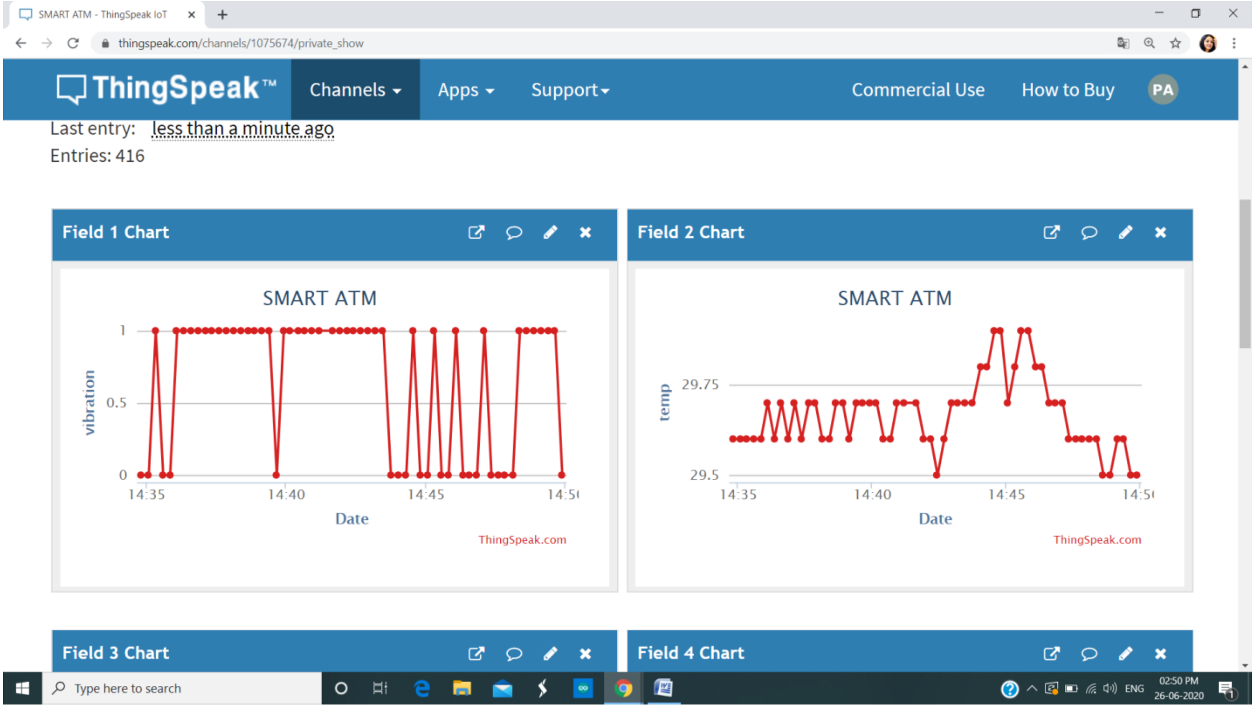
The output generally refers to the results and information that are generated by the system. A major form of the output is the display of the information generated by the system and servicing the user requests to the system. In this project the necessary outputs are;

The device outputs are:

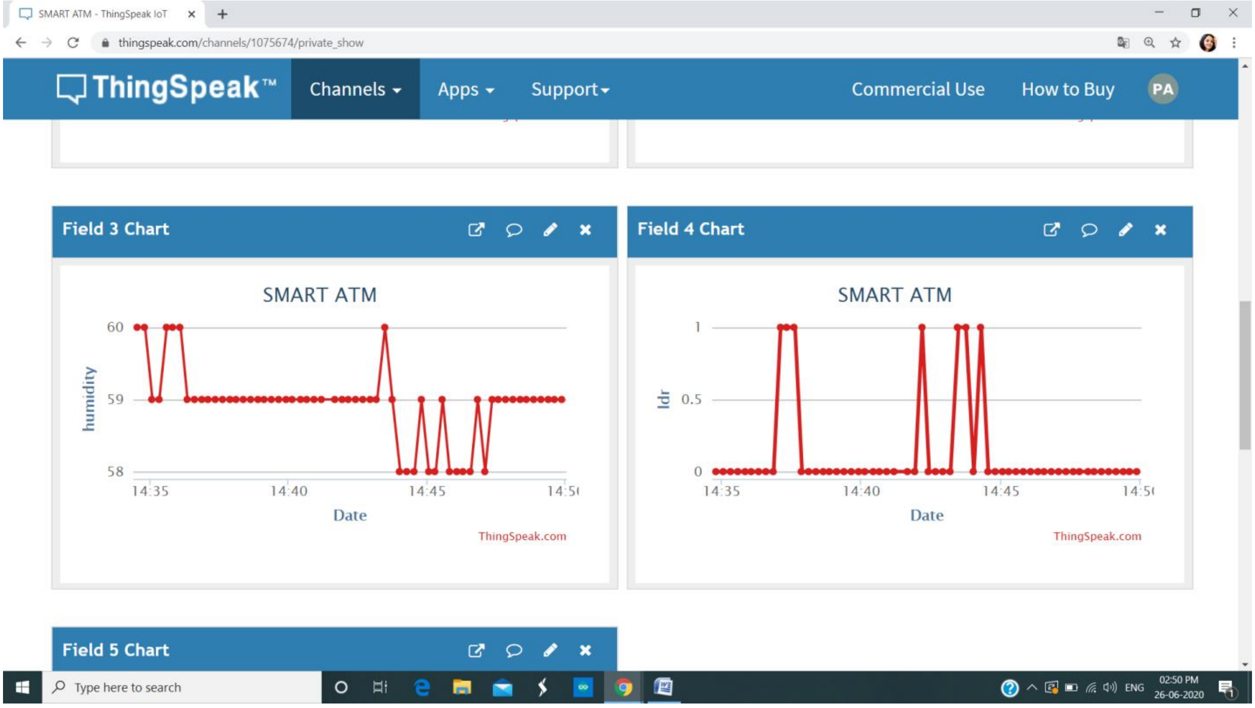
- Alarm : It will alert when attack occures.
- Notification : It will send a notification to bank authority as well as Police.

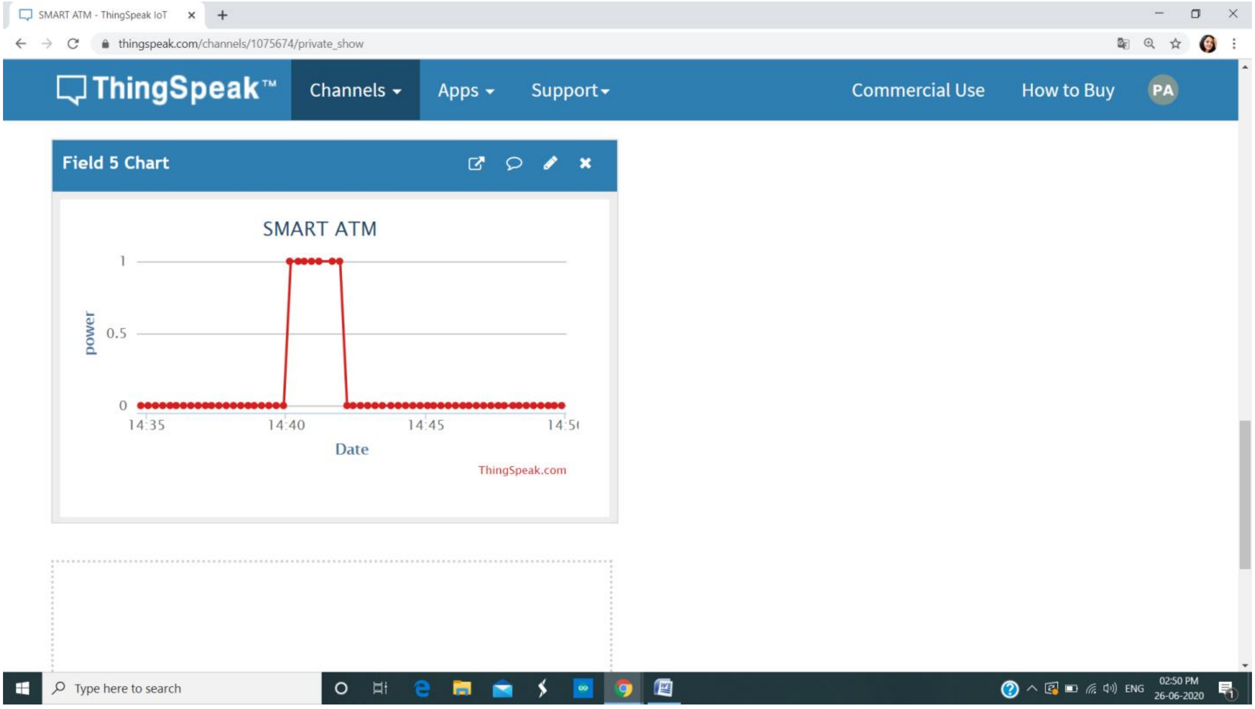
- Provide chart of sensor values for analysis using ThingSpeak and Blynk.

SENSOR REAL TIME READING VIA THINGSPEAK

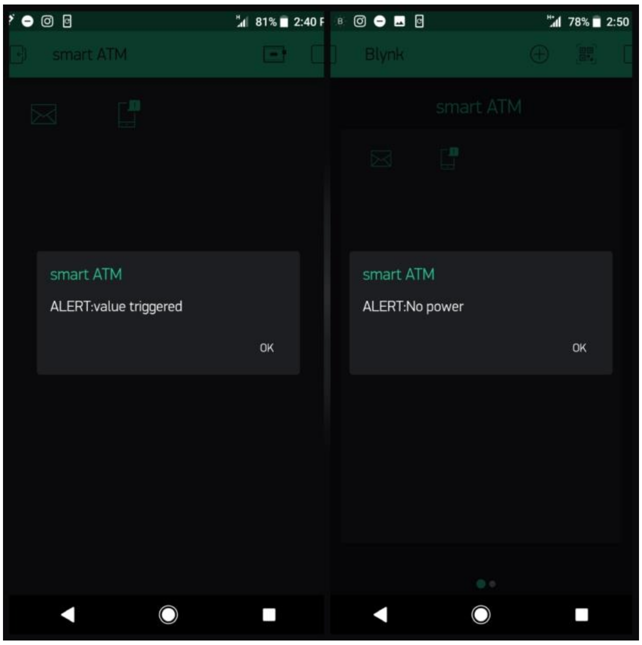


Last entry: less than a minute ago
Entries: 416





BLYNK ALERT



smart ATM

ALERT:value triggered

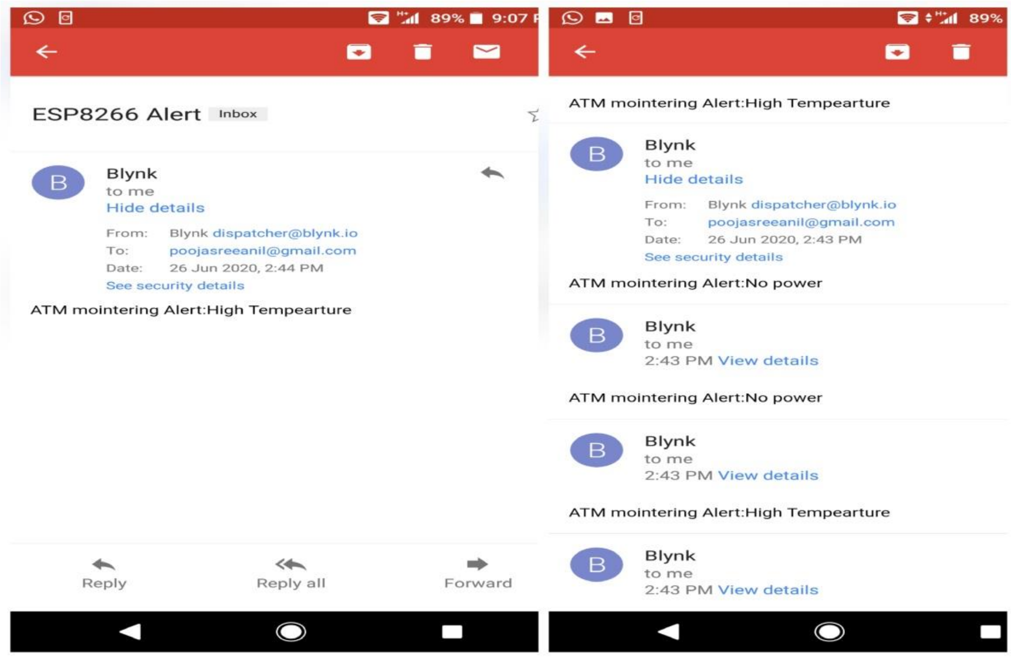
OK

smart ATM

ALERT:No power

OK

MAIL ALERT



ESP8266 Alert Inbox

Blynk
to me
Hide details
From: Blynk dispatcher@blynk.io
To: poojasreeanil@gmail.com
Date: 26 Jun 2020, 2:44 PM
See security details

ATM mointering Alert:High Tempearture

ATM mointering Alert:High Tempearture

Blynk
to me
Hide details
From: Blynk dispatcher@blynk.io
To: poojasreeanil@gmail.com
Date: 26 Jun 2020, 2:43 PM
See security details

ATM mointering Alert:No power

Blynk
to me
2:43 PM View details

ATM mointering Alert:No power

Blynk
to me
2:43 PM View details

ATM mointering Alert:High Tempearture

Blynk
to me
2:43 PM View details

PROCESS	INPUT DESIGN	OUTPUT DESIGN
When Attacker attack the ATM machine	Viberation Sensor placedinside the ATM. During attack it Viberates and send triggered values as input	Graph of the values are displayed on ThingSpeak and Blynk.
Visual Blockage Detection	LDR triggered sensor values	Triggered values,date and time are shown in Thing Speak and Blynk.
AC maintance &controlling	Values from DHT11 sensors are taken to mointer the AC	Values are shown in the ThingSpeak chart and blynk.
Power supply mointering	Check whether power supply in the circuit or not	Graph is displayed on the ThingSpeak and Blynk.

Table 5.1: Input/output Design

5.5 PROGRAM DESIGN

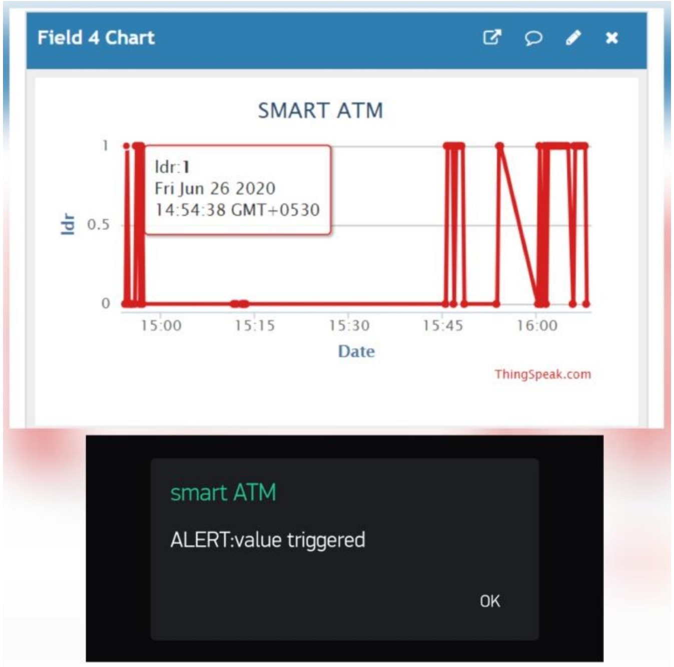
i. LDR SENSOR

Step 1: If the application is active, LDR sensor detect the light intensity.

Step 2: If there is no presence of light or detect any obstacles

a) Buzzer get Alerted.
b) Message Send to Authority through NODE MCU and Blynk.
c) Correspondingly, All the values are saved and display on the ThingSpeak chart.

Step 3:If the detected then check for vibration sensor status and then take correspondive measure.



smart ATM

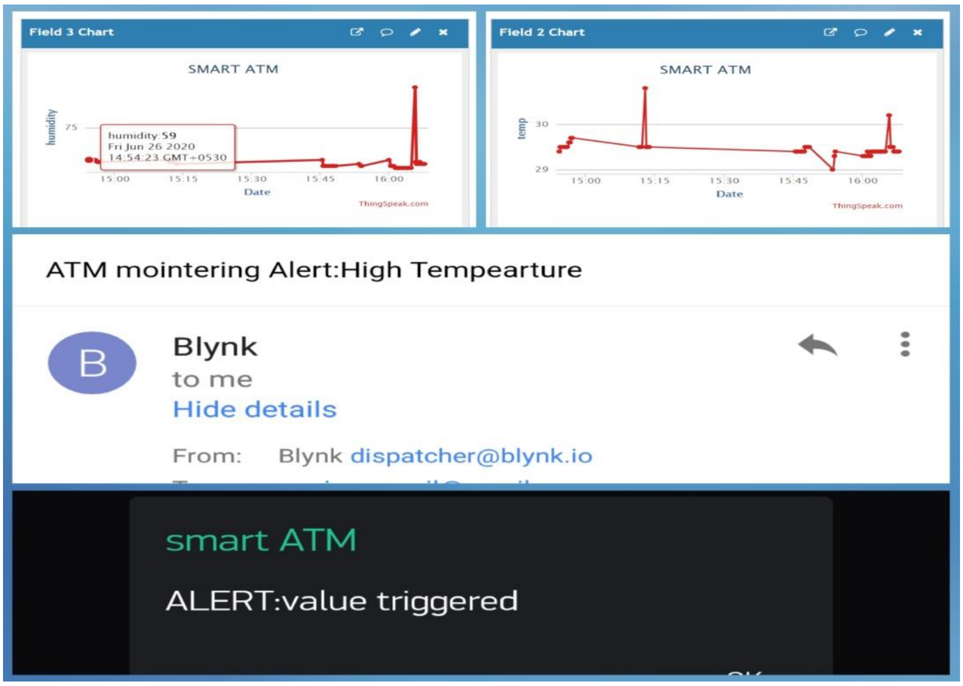
ALERT:value triggered

ii TEMPERATURE AND HUMIDITY SENSOR

Step 1: If the application is active, the temperature and humidity sensor will detect the room temperature and the humidity level.

Step 2: If the value is greater than specified value

a) Buzzer get Alerted.
b) Message Send to Authority through NODE MCU and Blynk.
c) Correspondingly, All the values are saved and display on the ThingSpeak chart.



ATM mointering Alert:High Tempearture

Blynk
to me
Hide details

From: Blynk dispatcher@blynk.io

smart ATM

ALERT:value triggered

iii. VIBERATION SENSOR

Step 1: If the theft attack the ATM ,then the viberation sensor value triggered .

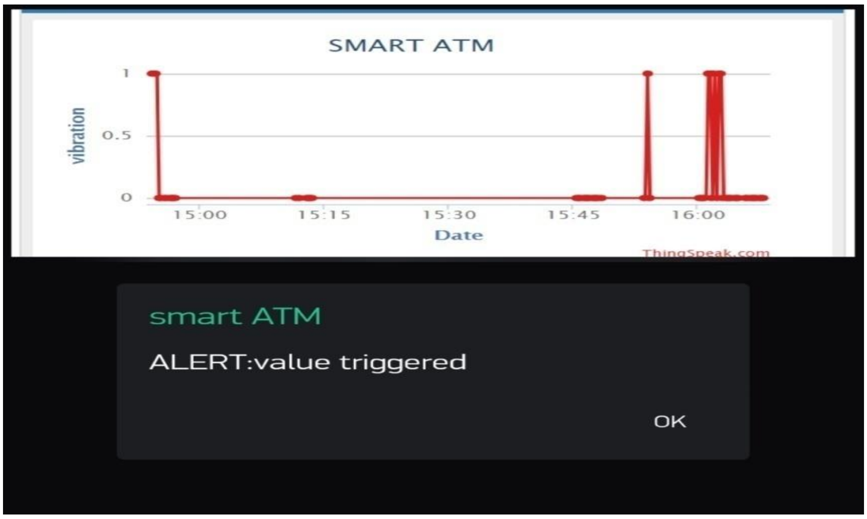
Step 2: Then it take corresponding action.

a) Buzzer get Alerted.

b) Message Send to Authority through NODE MCU and Blynk.

c) Correspondingly, All the values are saved and display on the ThingSpeak chart.

Step 3: If the detected then check for vibration sensor status and then take correspondive measure.



smart ATM

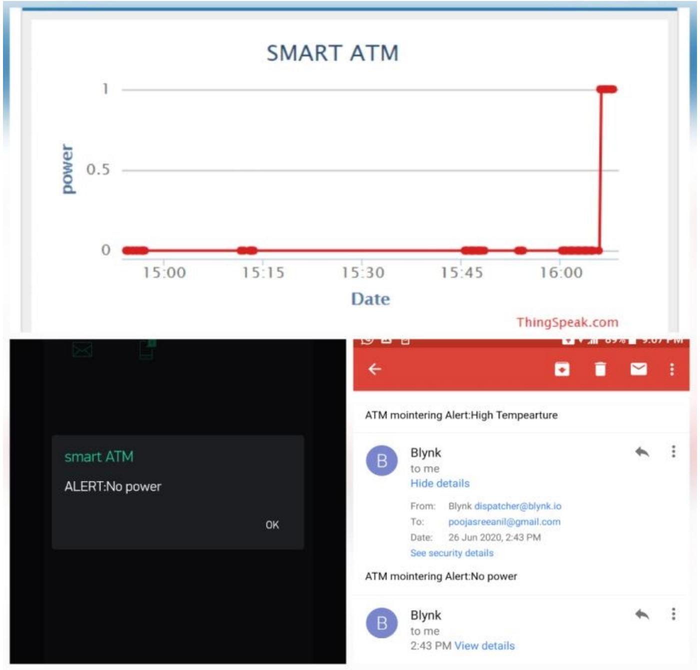
ALERT:value triggered

iv POWER SUPPLY

Step 1: Check whether there is power supply inside the circuit or not.

Step 2: If not

a) Message Send to Authority through NODE MCU and Blynk.
b) Correspondingly, All the values are saved and display on the ThingSpeak chart.



smart ATM

ALERT:No power

ATM mointering Alert:High Tempearture

Blynk
to me

From: Blynk dispatcher@blynk.io
To: poojasreeanil@gmail.com
Date: 26 Jun 2020, 2:43 PM

ATM mointering Alert:No power

Blynk
to me
2:43 PM

CHAPTER 6

FUNCTIONAL AND NON-FUNCTIONAL REQUIREMENTS

6.1 FUNCTIONAL REQUIREMENTS

In software engineering, a functional requirement defines a function of a system or its component. A function is described as a set of inputs, the behavior, and outputs. Functional requirements may be calculations, technical details, data manipulation and processing and other specific functionality that define what a system is supposed to accomplish. Generally, functional requirements are expressed in the form “system must do requirement”. Functional requirements for each of the uses cases described below:

- Descriptions of data to be entered into the system.
- Descriptions of operations performed by each inputs.
- Descriptions of work-flows performed by the system.
- Descriptions of system outputs.
- How the system meets applicable regulatory requirements.

6.2 NON-FUNCTIONAL REQUIREMENTS

A non-functional requirement is a requirement that specifies criteria that can be used to judge the operation of a system, rather than specific behaviors. Non-functional requirements are “system shall be requirement ". Non-functional requirements are often called qualities of a system. Other terms for non-functional requirements are "constraints", "quality attributes”, “quality goals", "quality of service requirements" and "non-behavioral requirements. Some of the non-functional requirements are mentioned below:

i. Performance requirements

Requirements about resources required, response time, transaction rates, throughput, benchmark specifications or anything else having to do with performance.

ii. Operating constraints

List any run-time constraints. This could include system resources, people, needed software, etc.

iii. Platform constraints

Discuss the target platform. Be as specific or general as the user requires. If the user doesn't care, there are still platform constraints.

iv. Accuracy and Precision

Requirements about the accuracy and precision of the data. Beware of 100% requirements; they often cost too much.

v. Modifiability

Requirements about the effort required to make changes in the software. Often, the measurement is personnel effort (person- months).

vi. Portability

The effort required to move the software to a different target platform. The measurement is most commonly person-months or % of modules that need changing.

vii. Reliability

Requirements about how often the software fails. The measurement is often expressed in MTBF (mean time between failures). The definition of a failure must be clear. Also, don't confuse reliability with availability which is quite a different kind of requirement. Be sure to specify the consequences of software failure, how to protect from failure, a strategy for error detection, and a strategy for correction.

viii. Security

One or more requirements about protection of your system and its data. The measurement can be expressed in a variety of ways (effort, skill level, time) to break into the system. Do not discuss solutions (e.g. passwords) in a requirements document.

ix. Usability

Requirements about how difficult it will be to learn and operate the system. The requirements are often expressed in learning time or similar metrics.

CHAPTER 7

TESTING

7.1 TESTING STRATEGIES

A **test strategy** is an outline that describes the testing approach of the software development cycle.The purpose of a test strategy is to provide a rational deduction from organizational, high-level objectives to actual test activities to meet those objectives from a quality assurance perspective. The creation and documentation of a test strategy should be done in a systematic way to ensure that all objectives are fully covered and understood by all stakeholders. It should also frequently be reviewed, challenged and updated as the organization and the product evolve over time. Furthermore, a test strategy should also aim to align different stakeholders of quality assurance in terms of terminology, test and integration levels, roles and responsibilities, traceability, planning of resources, etc.

7.2 UNIT TESTING

Unit testing focuses on verification effort on the smallest limit of software design. Using the unit test plan prepared in the design phase of the system, important control paths are tested to uncover the errors within the module. This testing was carried out during the coding itself. In this testing step each module is going to be working satisfactorily as the expected output from the module.

7.3 INTEGRATION TESTING

It is the systematic technique for constructing the program structure to uncover errors associated with the interface. The objective is to take unit-tested module and built the program structure that has been dictated by design. All modules are combined in this step. Then the entire program is tested as a whole. If a set of errors is encountered connection is difficult because the isolation of causes is complicated by vastness of the entire program. Using this test plan preparing the design phase of the system, the integration was carried out. All the errors found in the system were corrected for the next testing step.

7.4 SYSTEM TESTING

In system testing, the software and other system elements are tested as a whole. System testing is actually a series of different test whose primary purpose is to fully exercise the computer-based system.

Sl.No	Test Case	Input	Expected Output	Actual Output	Pass or Fail
1	Application is open	Read each sensor values	Chart on Thing Speak	Get Chart	Pass
2	Thing Speak is open	Login with User name And password.	Get in to the platform	Get into ThingSpeak	Pass
3	Blynk app is open	Login with Username And password	Get ready with the App for messages	Get message When value is triggered	Pass
4	Shake the ATM	Small viberation produced	Start Alarmand Tiggered value should display	Value displayed But fail to produce alarm	fail
5	Shake the ATM	Huge viberation Is produced	Start Alarmand Tiggered value should display	Value displayed And chart is Displayed on thingspeak	Pass
6	Light is shown to the LDR	Low Light	Charting values And alarm	Chart value but fail to produce alarm	fail
7	Light is shown to the LDR	Medium light	Charting values	Correctly recorded	Pass
8	No light	No light	Send message and chart	Correctly record And send message	pass
9	Temperature And humidity	High Temperature And humidity	Chart and send notification	Chart and send notification	pass
10	Power supply	No power supply	Get notification And chart	Get notification And chart	pass

CHAPTER 8

RESULTS AND DISCUSSION

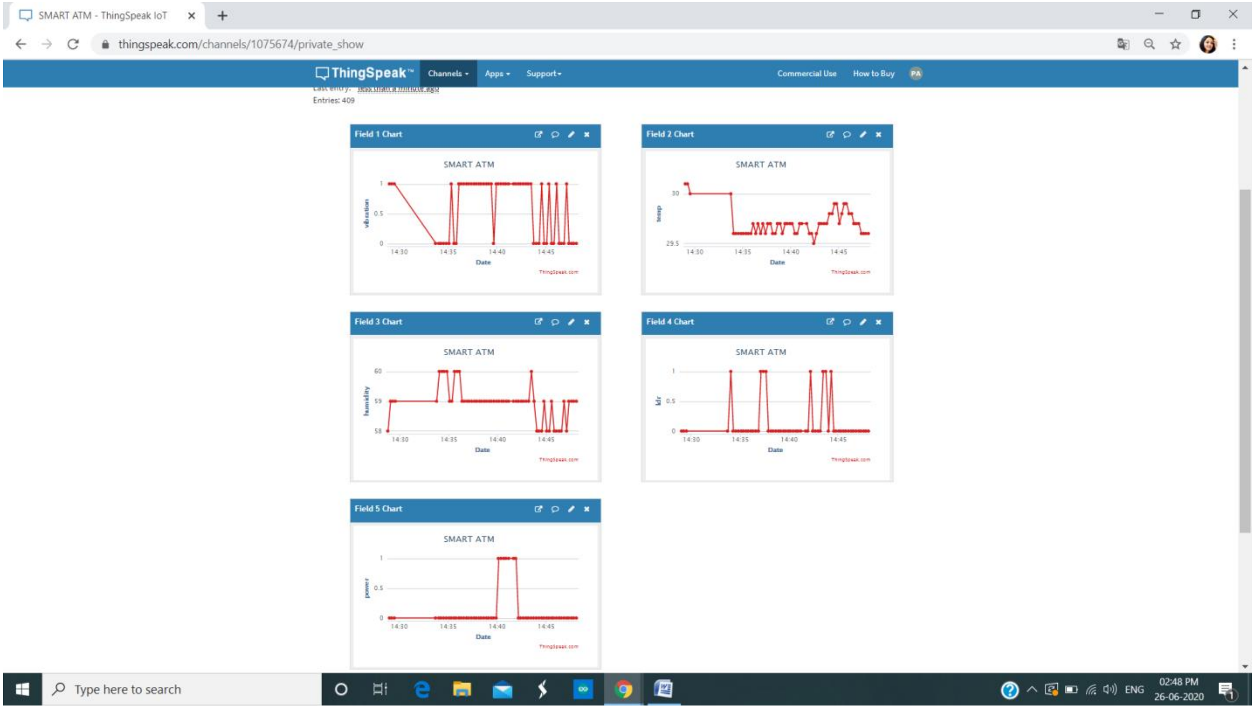
Results of our experiments show that the SMART ATM , i.e. mointering and notification android application called Blynk and real time mointering had been designedusing ThingSpeak and the programs were uploading into NODE MCU. The project is successfully tested for all the commands and it alsoensure security by implementing as a central processing unit. Once the attack is detected, yhe system send notification to bank and police.. The ThingSpeak can mointer each and every second ,can display output in the form of graphs.

8.1 RESULTS

The proposed system incorporated with the following features.

- Quick and appropriate action can be taken easily.
- Human effort can be reduced.
- Improved efficiency.
- Security enhanced for ATM system.
- Can control remotely from anywhere.
- Give proper data history for all mointering.
- Provide maintance and controlling system

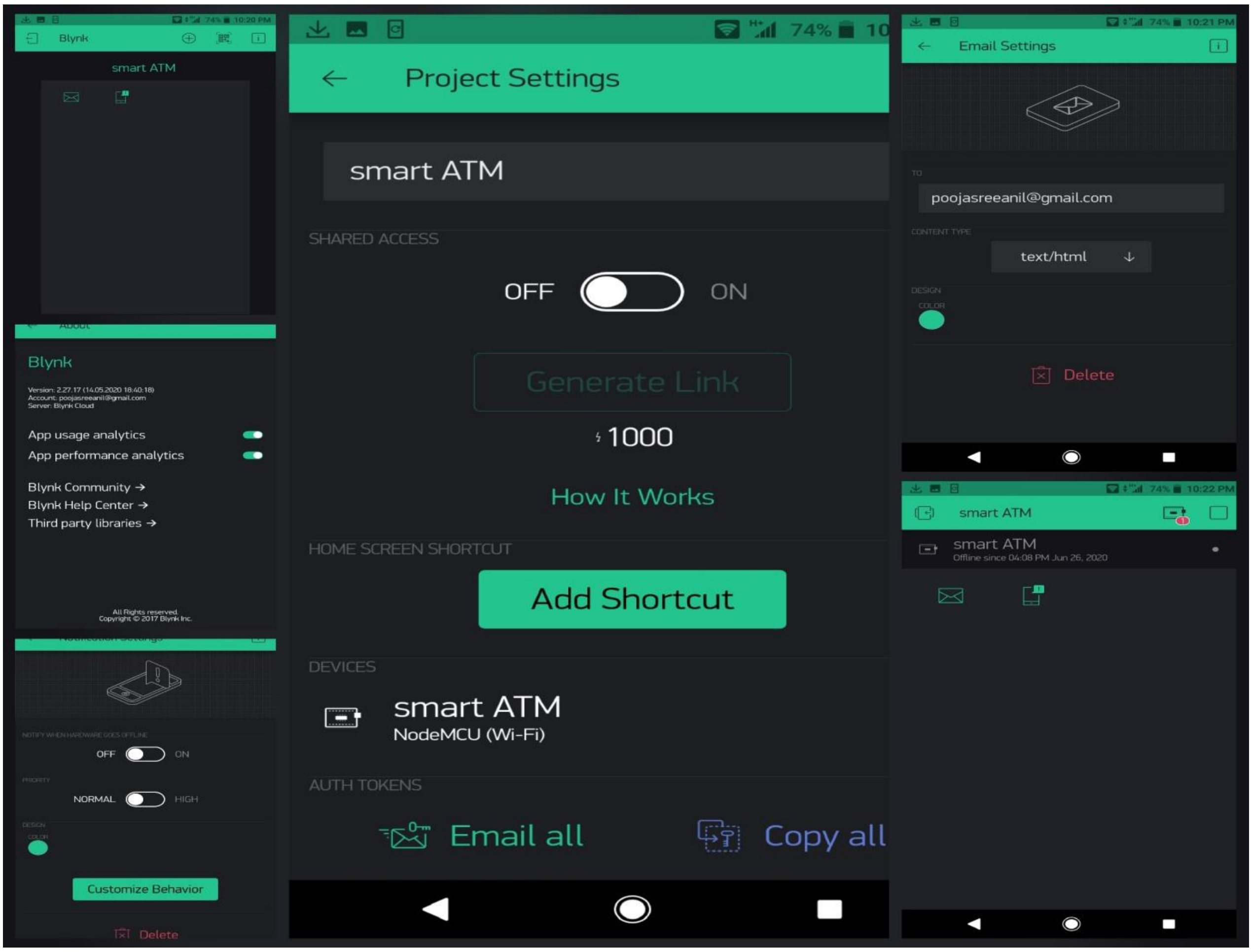
8.2 SCREENSHOTS



SMART ATM - ThingSpeak IoT

thingspeak.com/channels/1075674/private_show

Entries: 409



Blynk

smart ATM

About

Blynk

Version: 2.27.17 (14.05.2020 18:40:18)
Account: poojasreeanil@gmail.com
Server: Blynk Cloud

App usage analytics ●
App performance analytics ●

Blynk Community →
Blynk Help Center →
Third party libraries →

All Rights reserved.
Copyright © 2017 Blynk Inc.

Notification Settings

NOTIFY WHEN HARDWARE GOES OFFLINE: OFF ○ ON

PRIORITY: NORMAL ○ HIGH

DESIGN
COLOR ●

Customize Behavior

Delete

Project Settings

smart ATM

SHARED ACCESS

OFF ○ ON

Generate Link

ϟ1000

How It Works

HOME SCREEN SHORTCUT

Add Shortcut

DEVICES

smart ATM
NodeMCU (Wi-Fi)

AUTH TOKENS

Email all   Copy all

Email Settings

TO: poojasreeanil@gmail.com

CONTENT TYPE: text/html

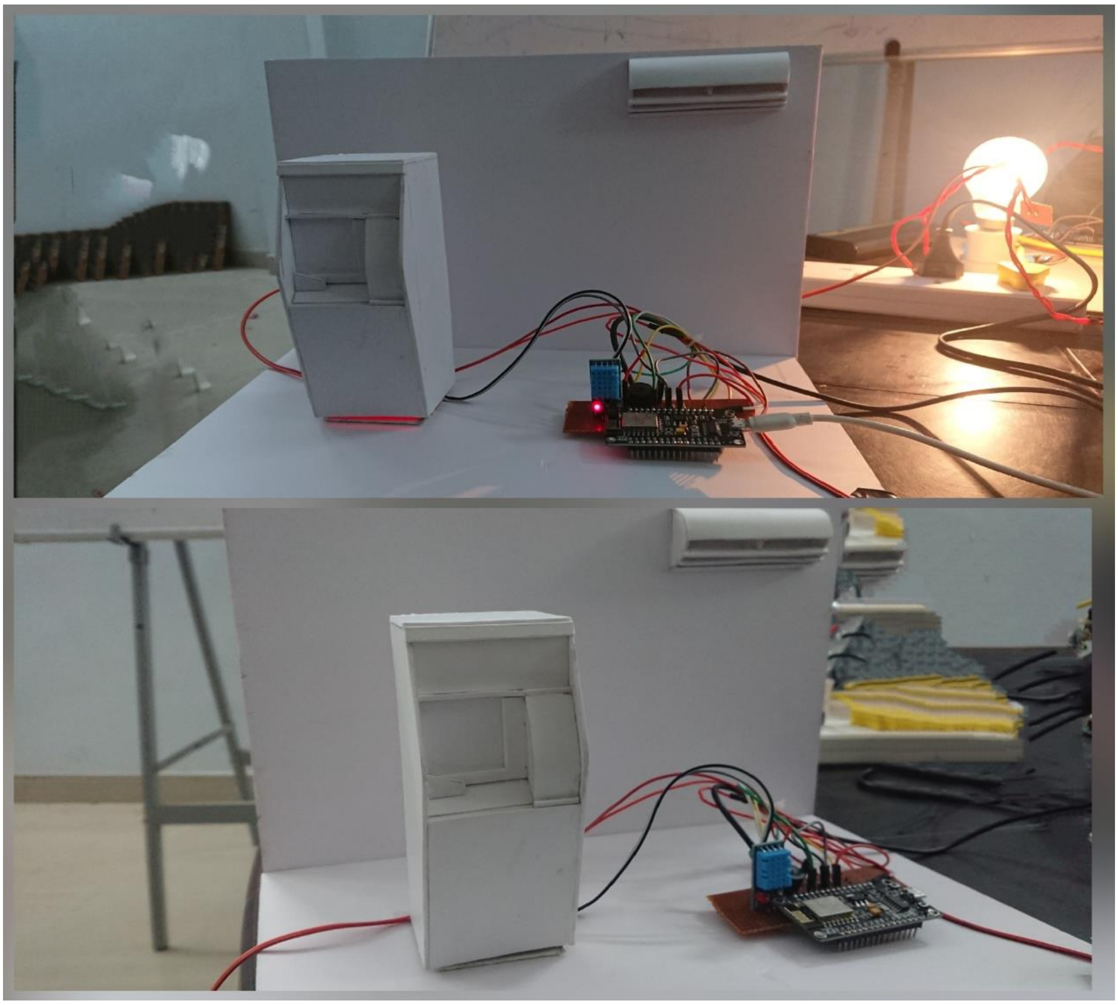
DESIGN
COLOR ●

Delete

smart ATM

smart ATM
Offline since 04:08 PM Jun 26, 2020

PROTOTYPE



CHAPTER 9

CONCLUSION

9.1 SYSTEM IMPLEMENTATION

Implementation means converting a new design into iteration .During implementation there should be a strong interaction between the developer of the software and the users. Implementation involves installing hardware terminals and training the operating staff. In this phase, user training is critical for minimizing reluctance to change and giving the new system a chance to prove its worth. The new system may be totally new replacing the existing system, or it may be the modifications of existing system. In either case proper implementation is essential to provide a reliable system to meet organizational requirements.

Major steps in the implementation of the system are as follows:

Installation of the hardware required for “SMART ATM SURVEILLANCE SYSTEM”, is required special hardware (Arduino UNO, Node MCU,LDR,DHT11,viberation sensor) which is to be installed for the working of both software and hardware. This can be worked on any system that support Ardunio IDE,ThingSpeak and a mobile device which support Blynk.Since the application is being developed with a server configured machine with a machine language. This case study is comparatively easy to implement. There are some technical risks where we can mointer Only five ATM through ThingSpeak at freeof cost. As a prerequisite you have to study about ThingSpeak,Basic of Ardunio, Ardunio coding,basic of electronics and working different sensors. other commonly used functionality will reduce our work and make the case study a beautiful one.

9.2 CONCLUSION

The implementation of ATM surveillance by using smart sensors and NODE MCU 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 NODE MCU 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.

9.3 FUTURE ENHANCEMENT

- This project can be implemented in the form of small device which is easy to install inside the ATM.
- This project can be integrated with additional features like detecting proper lightining inside the ATM
- Can implementing an automatic arresting system.
- Can provide an emergency button if a user trap inside the ATM.
- Ccan use tilt sensor for second time verification whether an attack happen.
- It can also integrated with a functionality of automatically checking user body temperature to take primary caution test against various spreading epidemic like Coronavirus disease (COVID-19)

REFERENCE / BIBLIOGRAPHY

1. BOOKS

- Fundamentals of software engineering

2.JOURNELS

- 2016 International Conference on Circuit, Power and Computing Technologies [ICCPCT]Smart ATM Surveillance System by S.Shriram1, Swastik B.Shetty1, Vishnuprasad P. Hegde1 , KCR Nisha2, Dharmambal.[IEEE 2016]

- M. Raj and Anitha Julian, "Design and Implementation of Antitheft ATM Machine using Embedded Systems," International Conference on Circuit, Power and Computing Technologies [ICCPCT]

- IOT Based Centralized Bank Security System for Monitoring and Auto Arresting by Satvik Gogineni1, K Marimuthu and Syed Amma Sheik2 1School of computer Science and Engineering, Vellore Institute of Technology (VIT), Vellore-632014, India. 2Department of Electrical and Electronics, Ibra College of Technology, Oman.

- International Journal of Applied Engineering Research ISSN 0973-4562 Volume 14, Number 6, 2019 (Special Issue) on iot based atm maintenance and security system

3. WEBSITES

https://thingspeak.com/channels?tag=database

http://help.blynk.cc/en/articles/512105-how-to-install-blynk-library-for-arduino-ide

APPENDICES

1.SCRUM BOARD

i. Git

Git is a version-control system for tracking changes in computer files and coordinating work on those files among multiple people. It is primarily used for source-code management in software development, but it can be used to keep track of changes in any set of files. As a distributed revision-control system, it is aimed at speed, data integrity, and support for distributed, non-linear workflows.

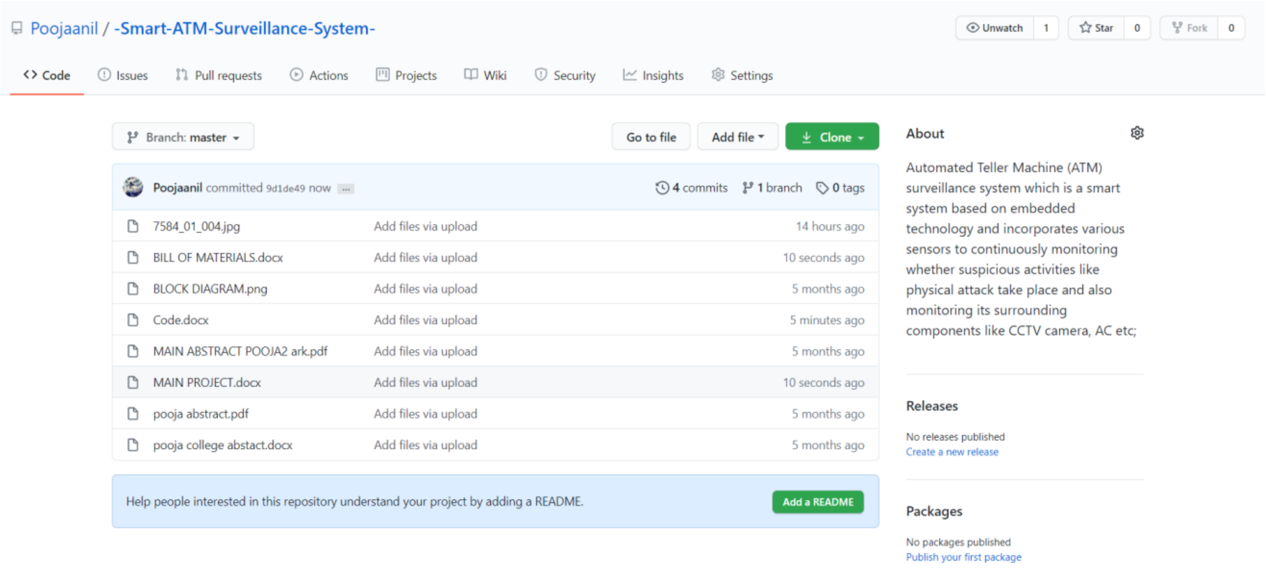
ii. Git Repositories

A Git repository contains the history of a collection of files starting from a certain directory. The process of copying an existing Git repository via the Git tooling is called cloning. After cloning a repository the user has the complete repository with its history on his local machine. Of course, Git also supports the creation of new repositories. If you want to delete a Git repository, you can simply delete the folder which contains the repository. If you clone a Git repository, by default, Git assumes that you want to work in this repository as a user

iii. Scrum

Scrum is an agile way to manage a project, usually software development. Agile software development with Scrum is often perceived as a methodology; but rather than viewing Scrum as methodology, think of it as a framework for managing a process. In the agile Scrum world, instead of providing complete, detailed descriptions of how everything is to be done on a project, much of it is left up to the Scrum software development team. In the agile Scrum world, instead of providing complete, detailed descriptions of how everything is to be done on a project, much of it is left up to the Scrum software development team. Within agile development, Scrum teams are supported by two specific roles. The first is a Scrum Master, who can be thought of as a coach for the team, helping team members use the Scrum process to perform at the highest level. The product owner (PO) is the other role, and in Scrum software development, represents the business, customers or users, and guides the team toward building the right product.

iv. Git History



Poojaanil committed 9d1de49 now ... 4 commits 1 branch 0 tags

7584_01_004.jpg	Add files via upload	14 hours ago
BILL OF MATERIALS.docx	Add files via upload	10 seconds ago
BLOCK DIAGRAM.png	Add files via upload	5 months ago
Code.docx	Add files via upload	5 minutes ago
MAIN ABSTRACT POOJA2 ark.pdf	Add files via upload	5 months ago
MAIN PROJECT.docx	Add files via upload	10 seconds ago
pooja abstract.pdf	Add files via upload	5 months ago
pooja college abstact.docx	Add files via upload	5 months ago

Help people interested in this repository understand your project by adding a README. Add a README

About

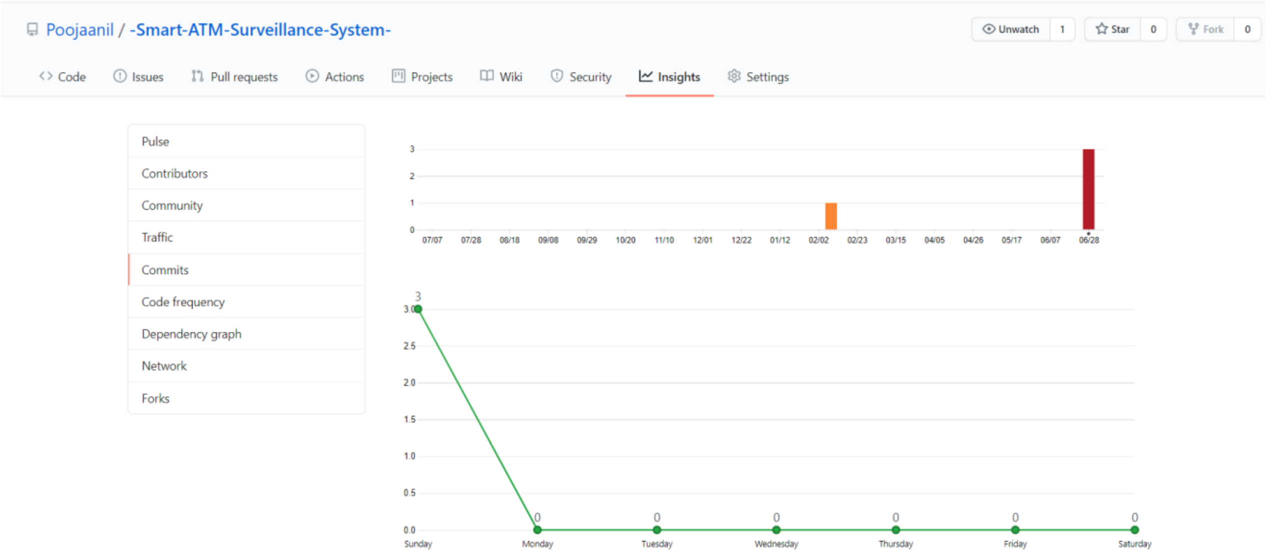
Automated Teller Machine (ATM) surveillance system which is a smart system based on embedded technology and incorporates various sensors to continuously monitoring whether suspicious activities like physical attack take place and also monitoring its surrounding components like CCTV camera, AC etc;

Releases

No releases published
Create a new release

Packages

No packages published
Publish your first package



2. LIST OF TABLES

3. LIST OF FIGURES

4. ABBREVIATIONS AND NOTATION

Notation	Description
Node MCU	Node Microcontroller
IOT	Internet of Things

5. CODING

```
#include <ESP8266WiFi.h> // ESP8266WiFi.h library

#include <DHT.h>

#define DHTPIN 2

#define DHTTYPE DHT11

DHT dht(DHTPIN, DHTTYPE);

const char* ssid     = "abc";// replace subscribe with your WiFi SSID(Name)

const char* password = "12345678";//replace with Your Wifi Password name

const char* host = "api.thingspeak.com";

const char* writeAPIKey = "TQ23GRLLN7PI5511"; //copy yout ThingSpeak channel API Key.

char auth[] = "FmNUNzcnBN6HbGrB_14QPTfEVqnnjl99";s

 #include <BlynkSimpleEsp8266.h>

BlynkTimer timer;

void setup() {

 Serial.println("Connecting to ");



  Serial.println(ssid);

//  Connect to WiFi network

  WiFi.begin(ssid, password);

while (WiFi.status() != WL_CONNECTED) {

delay(500);

    Serial.print(".");

  }

   Serial.println("");

   Serial.println("WiFi connected");

 Blynk.begin(auth, ssid, password);

 dht.begin();

 pinMode(D5,INPUT);//VIB

 pinMode(D6,INPUT);//POWER

 pinMode(D7,OUTPUT);//BUZ

 pinMode(D8,INPUT);//LDR
```

```
// Initialize sensor
 Serial.begin(115200);
}
void loop() {
Blynk.run();
float humidity = dht.readHumidity();
 float temperature = dht.readTemperature();
int Viberation=digitalRead(D5);
int Power =digitalRead(D6);
int Buzzer=digitalRead(D7);
int Ldr=digitalRead(D8);
if(Viberation==1||Ldr==0)
{

  Blynk.email("poojasreeanil@gmail.com", "ESP8266 Alert", "ATM mointering Alert:High Tempearture");
    Blynk.notify("ALERT:value triggered");
    digitalWrite(D7,HIGH);
  }
  else
  {
    digitalWrite(D7,LOW);
  }
if(temperature > 35){
    Blynk.email("poojasreeanil@gmail.com", "ESP8266 Alert", "ATM mointering Alert:High Tempearture");
    Blynk.notify("ALERT:High Tempearture");
  }
  if(humidity>80){
    Blynk.email("poojasreeanil@gmail.com", "ESP8266 Alert", "ATM mointering Alert:High Humidity");
    Blynk.notify("ALERT:High Humidity");
  }
 if(Power==0){
   Blynk.email("poojasreeanil@gmail.com", "ESP8266 Alert", "ATM mointering Alert:No
power");
   Blynk.notify("ALERT:No power");
  }
 WiFiClient client;
const int httpPort = 80;
if (!client.connect(host, httpPort)) {
return;
  }
  String url = "/update?key=";
  url+=writeAPIKey;
  url+="&field1=";
  url+=String(Viberation);
  url+="&field2=";
  url+=String(temperature);
  url+="&field3=";
  url+=String(humidity);
  url+="&field4=";
  url+=String(Ldr);
  url+="&field5=";
  url+=String(Power);
  url+="\r\n";
// Request to the server
  client.print(String("GET ") + url + " HTTP/1.1\r\n" +
"Host: " + host + "\r\n" +
"Connection: close\r\n\r\n");
  Serial.println("Send to ThingSpeak.\n");
  Serial.println(Ldr);
client.stop();
  Serial.println("Wait for 15 sec to update next datapack in thingSpeak");
delay(1000);}
```