ABSTRACT

Surveillance plays a major role in many fields be it at home, hospitals, schools, public places ,farmlands etc. It helps us to monitor a certain area and prevent theft and also provides proof of evidence. In the case of farmlands or agricultural lands surveillance is very important to prevent unauthorized people from gaining access to the area as well as to protect the area from animals .Various methods aim only at surveillance which is mainly for human intruders, but we tend to for get that the main enemies of such farmers are the animals which destroy the crops. This leads to poor yield of crops and significant financial loss to the owners of the farmland. This problem is sopronounced that sometimes the farmers decide to leave the areas barren due to such frequent animal attacks. This system helps us to keep away such wild animals from the farmlands as well as provides surveillance functionality.

LISTOF FIGURES

TABEL OF CONTENTS

CHAPTER	TITLE	PAGE NO
5	**RESULT AND FUTURE WORKS**	**54**
	5.1 RESULT	
	5.2 FUTURE WORKS	
6	**CONCLUSION**	**67**
	REFERENCE	**68**
	APPENDIX	
	CODE	**69-86**
	OUTPUT SCREENSHOTES	**87-88**

LIST OF ABBRETATIONS

MIT	Massachusetts Institute of Technology
IoT	Internet of Things
USB	Universal Serial Bus
IBM	International Business Machine
DC	Direct current
DHT	Digital Humidity And Temperatures

CHAPTER 1

INTRODUCTION

Detecting the different animal and birdsusing IBM visual recognition service for protection the crop from damage. There will be live video streaming in raspberry pi and in this video streaming we candetect the animal land birds. Whenever any birds and animals are detected the image will be captured and for keeping away then from the crop we can keep a siren and we can blinktheLED's.The camera will beattachedtotheservomotorit willberotatingforeverytimeinterval.The crop is also integrated with the soil moisture sensor and the DHT sensor for temperatureand humidity parameters.Wheneverthere is low soil moisture the admins will be alerted and they canblink the LED's.Thenow sounds an alarm to woo the animals awayfrom the fields as well as sendsms to the farmer so that he may know about theissue and come to the spot in case the animals don'tturn away from the alarm. This ensures complete safety of crops from animals thus protecting the farmers loss.

CHAPTER 2

LITERATURE SURVEY

Balaji Banu [1] designed a wireless sensor networks to observe the conditions of the farming and increasing the crop yield and quality. Sensors are used to monitor different conditions of environment like water level, humidity, temperature etc., The processors ATMEGA8535 and ICS8817 BS, analog to digital conversion and wireless sensor nodes with wireless transceiver module based on Zig bee protocol are used in the designing the system. Database and web application is used to retrieve and store data. In this experiment the sensor node failure and energy efficiency are managed. Liu Dan [2], Joseph Haule, Kisangiri Michael [3] and Wang Weihong, Cao Shuntian [38] carried out experiments on intelligent agriculture greenhouse monitoring system based on ZigBee technology. The system performs data acquisition, processing, transmission and reception functions. The aim of their experiments is to realize greenhouse environment system, where the of system efficiency to manage the environment area and reduce the money and farming cost and also save energy. IOT technology here is based on the B-S structure and cc2530 used like processing chip to work for wireless sensor node and coordinator. The gateway has Linux operating system and cortex A8 processor act as core. Overall the design realizes remote intelligent monitoring and control of greenhouse and also replaces the traditional wired technology to wireless, also reduces manpower cost. Joseph haule [3], Dragoş Mihai Ofrim, Bogdan Alexandru Ofrim and Dragoş Ioan Săcăleanu [18] have proposed an experiment that explains the use of wsn used in automating irrigation. Irrigation control and rescheduling based on wsn are powerful solutions for optimum water management through automatic communication to know the soil moisture conditions of irrigation design. The process used here is to determine the proper frequency and time of watering are important to ensure the efficient use of water, high quality of crop detection delay throughput and load. Simulation is done for agriculture by OPNET. Another design of wsn is deployed for irrigation system using Zig bee protocol which will impact battery life. There are some drawbacks as wsn is still under development stage with unreliable communication times, fragile, power consumption and communication can be lost in agricultural field. so automate irrigation system and scheduling based on wireless sensor networks are used. WSN uses low power and a low data rate and hence energy efficient technology. All the devices and machines controlled with the help of inputs received via sensors which are mixed with soil. Farmers can analyze whether the system performs in no

CHAPTER 3

AIM AND SCOPE

3.1 AIM

Detecting the different animal and birds using IBM visual recognition service for protection the crop from damage.

3.2 SCOPE

This project is used to protect the farmland by using Raspberry Pi this project utilizes recognition service for this purpose. Forest officer and farmer will get the message connucting area which that animals and birds observe.

Detecting the different animal and birdsusing IBM visual recognition service for protection the crop from damage. There will be live video streaming in raspberry pi and in this video streaming we candetect the animal landbirds.Wheneveranybirdsandbirdsandanimalsaredetectedtheimagewill be captured and for keeping away then from the crop we can keep a siren and we can blinktheLED's.Thecamerawillbeattachedtotheservomotoristwillberotatingforeverytimeinterval.The crop is also integrated with the soil moisturesensor and the DHT sensor for temperatureand humidity parameters.Wheneverthere is low soil moisture the admins will be alerted and they canblink the LED's.Thenow sounds an alarm to woo the animals awayfrom the fields as well as sendssms to the farmer so that he may know about theissue and come to the spot in case the animals don'tturn away from the alarm. This ensures complete safety of crops from animals thus protecting the farmers loss

CAHPTER 4

METHODOLOGY AND IMPLEMENTATION

4.1 TECHNOLOGY USED

4.1.1 SKILLS REQURIED

- IOT Open Hardware Platforms
- IOT Application Development
- IOT Cloud Platform
- IOT Communication Technologies

4.1.2

SOFTWARE REQUIREMENTS

- Python
- IBM Watson
- Node Red

4.1.3

HARDWARE REQUIREMENTS

- DHT11 Sensor
- Soil Moisture Sensor
- Servo Motor
- 9VDC Motor
- Camera
- Connecting Wires

- Raspberry pi

4.2

INTRODUCTION OF INTERNET OF THINGS:

Internet of Everything or Network of Everything is additionally known as Internet of Things (IoT). When physical objects or things are embedded with physics, sensors and software then thenet work called IoT is formed. The Internet of Things (IoT) is a system of interrelated computingdevices, mechanical and digital machines, objects, animals or people that are provided with uniqueidentifiers and the ability to transfer data over a network without requiring human-to-human orhuman-to-computer interaction.

The Internet of Things is an emerging topic of technical, social, and economic significance .Consumer products, durable goods, cars and trucks, industrial and utility components, sensors, andother everyday objects are being combined with Internet connectivity and powerful data analytic capabilities that promise to transform the way we work, live, and play.Projection for the impact of IoT on the Internet and economy are impressive, with some anticipating as many as 100 billion connected IoT devices andaglobal economic impact ofmorethan$11 trillionby 2025.

Thesametime,however,theInternetofThingsraisessignificantchallengesthatcouldstandinthewayofrealizingitspotentialbenefits.Attention-grabbingheadlinesaboutthehackingofInternet-connected devices, surveillance concerns, and privacy fears already have captured publicattention.Technicalchallengesremainandnewpolicy,legalanddevelopmentchallengesareemerging. This overview document is designed to help the Internet Society community navigate the dialoguesurroundingtheInternetofThingsinlightofthecompetingpredictions aboutitspromises and devices has existed for decades. The recent confluence of several technology market trends, how ever,is bringing the Internet of Things closer to widespread reality. These include Ubiquitous Connectivity,WidespreadAdoptionofIp basedNetworking,ComputingEconomics,Miniaturization,AdvancesinDataAnalyticand the Riseof Cloud Computing.

- **Connectivity Models:**

IoT implementations use differenttechnical communications models ,each with its own characteristics. Four common communications models described by the Internet Architecture Boardinclude:Device-to-Device,Device-to-Cloud,Device-to-Gateway,andBack-EndData-Sharing.These models highlight the flexibility in the ways that IoT devices can connect and provide value totheuser.

- **Transformational Potential:**

The implications and issues in a world where the most common interaction with the Internet comes from passive engagement with connected objects rather than active engagement with content.The potential realization of this outcome – a "hyper connected world" -- is testament to the general-purpose nature of the Internet architecture itself, which does not place inherent limitations on the applicationsorservices that can make use of the technology.

Five key IoT issue areas are examined to explore some of the most pressing challenges andquestions related to the technology. These include security; privacy; interoperability and standards ;legal, regulatory ,andrights; andemerging economies and development.

- **Security:**

While security considerations are not new in the context of information technology, theat tributesof many IoT implementations present new and unique security challenges.

Addressing these challenges and ensuring security in IoT products and services must be fundamental priority.. Poorly secured IoT devices and services can serve as potential entry points forcyberattackandexposure data to theftbyleavingdatastreamsinadequately protected.

The interconnected nature of IoT devices means that every poorly secured device that isconnectedonlinepotentiallyaffectsthesecurityandresilienceoftheInternetglobally.Thischallenge is amplified by other considerations like the mass-scale connect to other devices, and thelikelihoodoffielding thesedevicesinsecureenvironments.

As a matter of principle, developers and users of IoT devices and systems have a collectiveobligation to ensure they do not expose users and the Internet itself to potential harm. Accordingly, collaborative approach to security will be needed to develop effective and appropriate solutions toIOTsecuritychallengesthat are well suitedto thescaleandcomplexity of theissues.

Privacy:

Thefullpotential of the Internetof Thingsdepends on strategies that respectindividualprivacy choices a