# Security in Smart Agriculture System

[1]Achal Singh
Department of Information Technology
Shree L.R. Tiwari College of Engineering,
Mira Road, India

[2]Pawan Suthar
Department of Information Technology
Shree L.R. Tiwari College of Engineering,
Mira Road, India

[3]Ankit Yadav
Department of Information Technology
Shree L.R. Tiwari College of Engineering,
Mira Road, India

[4]Madhuri Gedam
Department of Information Technology
Shree L.R. Tiwari College of Engineering,
Mira Road, India

**Abstract:- In all human history, agriculture is one of the most important industries and a backbone for prevalence of life. This project, aims to the diffusion of new digital technologies renders digital transformation relevant to nearly every economic activity sector, including in the agriculture sector. Farming and how farmers work is changing, the use of Information and Communications Technology (ICT) together with the increased use of the Internet of Things (IoT) is developing a concept. In this we present a holistic study on security and privacy in a smart farming ecosystem. The paper outlines a multi layered architecture relevant to the precision agriculture domain and discusses the security and privacy issues in this dynamic and distributed cyber physical environment. Further more, the paper elaborates on potential cyber attack scenarios and highlights open research challenges and future directions. In the Agriculture and Farming industries the Smart devices are widely used by a range of people from farmers to entrepreneurs. These technologies are used in a variety of ways, from finding real- time status of crops and soil moisture content to deploying drones to assist with tasks such as applying pesticide spray.**

***Keywords:-*** *Security, Privacy, Precision Agriculture, Cloud Computing, Iot, Artificial Intelligence (AI).*

## I. INTRODUCTION

Food and energy are indispensable to human beings, and we can see from this study how, as countries around the globe experience increased population and economic development, the demand of human for crops are bigger than ever. This study mentions that the human demand for farm crops will increase drastically by 2050 and, therefore, agriculture production must be doubled. However, the agriculture labour force of today is facing the problem of ageing. The benefits of using Information and Communications Technologies (ICT) together with the increasing use of the Internet of Things (IoT) in developing precision farming, also called Smart Farming. Using drones, robots, smart energy meters, smart security devices, smart data for seed traits and to treat soil conditions, these and other new systems offer unprecedented conveniences and improvements to managing the agriculture farming quality. Every day, the world is facing challenges. These challenges are also present in the agriculture and farming sector. Smart Farming involves the use of Information and Communications Technology (ICT) and, in particular, the Internet of Things (IoT) and related big data analytics to improve agricultural operations and processes. In India, farm data has been used to predict and prevent crop diseases, which reduced the risk associated with the failure of crop production. Similar data driven approaches have helped fruit farmers in Slovenia effectively fight against pests. Smart farming, however, goes beyond primary production. In fact, it has impacted the complete food supply chain, by employing big data analytics to provide useful insights about the entire farming process by facilitating real-time operational decision making, and revolutionizing existing agriculture business models. Smart farming enhances conventional farming practices by introducing on-field smart sensors and devices. These sensors and devices work in a synergistic manner to provide efficient farming experiences, as well as, an improved crop yield.

## II. LITERATURE REVIEW

The paper [1] present an a Cyber Security in Agri-food Sector which discusses data security challenges within the agri-food sector. It provides use cases showing the increase of data in the agri-food sector and their need of data security measurements and Interviewed companies about theircybersecurity concerns. But there are no security solution andalso have a limited scope of data security.

The paper [2] present an a Cyber biosecurity: A New Perspective on Protecting the Food and Agricultural System. The objective of paper is defines bio economy and investigates cyber bioeconomy security. It discusses how current and emerging data and infrastructure security issues affect the food and agricultural system and its cybersecurity. And also have no feasible solution has been suggested to enhance cyber bioeconomy security.

The paper [3] present an a Cyber Security on the Farm: An Assessment of Cyber Security Practices in the Agriculture Industry. In this they surveys farmers and agribusiness ownersabout their perceptions of cybersecurity and how age, gender and education might affect these perceptions. They conclude the Quantifies levels of previous cybercrime victimization, technology implementation and details how individuals react to known threats, and what motivates them to adopt protection technologies.

The paper [4] present an a Cyber Risk and Security Implications in Smart Agriculture and Food System. In this paper they demonstrates the nature of modern information risk in causing unknown risks. They research the emphasises the extent of cyber insurance coverage for the agriculture sector and discussion on the regulatory response to use of smart devices and its impact on smart farm security.

The paper [5] present an a Framework for Cyber Security Approaches in Precision Farming. They discusses the challenges of wireless sensor network (WSN) in digital farm, and proposes a framework of security approach for data flow in precision agriculture and also provide proposes a cyber physical architecture introducing the notion of virtual farms, proposed cyber physical system offers real time high frequency decision systems and discusses security framework elements.

## III. EXISTING RESEARCH

- *Cyber Attacks, Threats and Proposed Solutions*

Researchers and federal agencies have started gauging the impact cyber-attacks as more and more farmers and communities are adopting technologies in the farms. The report highlights the confidentiality, integrity, and availability model of information security in farming. It defines different technologies involved in PA including in-farm devices, location and remote sensing technologies, machine learning, etc. It briefly discusses the impacted groups by the misuse of technologies in farming including farmers, livestock producers, and also industries that support or rely on agriculture. This report also discusses hypothetical threat scenarios on real life examples.

The research also highlights a security framework to enable farmers to better understand security implications. However, the paper is unable to discuss open research issues, and challenges to secure the environment without evidence of how the discussed attacks are orchestrated in the domain.

- *Blockchain Related Research*

Recently, the usefulness of blockchain in domains other than cryptocurrency and financial transactions has been acknowledged. Agriculture and food supply chain is one of the domains in which blockchain technology has shown its capabilities. Accordingly, the authors in study overall implications, challenges and potential of existing blockchain- based projects in the field. Besides, it critically reviews maturity of such projects and elaborates on possible barriers and challenges, which hinder acceptability of such projects among farmers and existing cyber farming systems. Also focused on the use of blockchain technology for food safety. Authors created a system that tracks and monitors food production cycle, including the processes of raw materials, cultivation/breeding, processing, transporting,

- *AI and Machine Learning Assisted Work*

The advent of new age technologies such as artificial intelligence (AI) and machine learning (ML) not only facilitate the adaptation of advanced analytics in smart farming, but also create an ecosystem for improving the cybersecurity of services. Fusion of these technologies enable farmers to achieve higher average yield and better price control over their products in highly competitive markets. Design and implementation of a low cost IoT based security monitoring system have been proposed by Shabadi and Biradar [85]. The system focuses on physical layer of smart farming where it collects data from sensors.

## IV. PROBLEM STATEMENT

The adoption of sensor based technologies and cloud supported smart applications in agriculture has unleashed opportunities for adversaries to orchestrate cyber attacks. Therefore, it is important to first understand major security and privacy issues in smart farming domain before discussing specific cyberattacks. In this section, we will elaborate these issues in detail followed by attacks in the following section.

- *Data Security & Privacy*

In a smart farm, an enormous amount of complex, dynamic and spatial data gets generated from many heterogeneous sensors, devices and equipment. Leakage of such information either through unauthorized access or by an insider can cause potential threats. For example, leakage of agriculture anti- jamming devices information can help an attacker bypass these security measures, while leakage of soil, crop, and agriculture purchase information can cause severe economic losses to farmers.

- *Authorization & Trust*

In smart farming applications, connected entities including autonomous tractors, flying drones, on field sensors etc. communicate and interact with each other, and issue command and control operations to provide automated and efficient experience. Such communication can be direct machine to machine or via a cloud or edge assisted network which can support Message Queue Telemetry Transport, Constrained Application Protocol or other IoT communication protocols.

- *Authentication & Secure Communication*

One of the most important aspects of security and privacy in smart farming is authentication of connected devices. Devices need to be authenticated first in order to get connected to various services on a smart farming system. They are usually low power devices, with limited processing power, memory, and storage, so legacy public-key infrastructure authentication mechanisms cannot be considered as feasible solutions.

## V. SYSTEM ARCHITECTURE

The components are put together in a way of defining a structured solution that meets the technical and operational requirements while optimizing common quality attributes suchas performance in real-time.

❖ *There is the List of Project-Development Components:*

➢ *Hardware*

- Arduino™ UNO
- LEDs
- Moisture sensors
- Breadboard
- Jumper wires
- Water level sensors
- Water pump
- DHT11 temperature & humidity sensors
- Garden sets (soil samples)Software

➢ Software

- Firebase™ Database
- Mobile Application
- Web Application

Table 1 Layout and Connections

| **Arduino** | **Connections** | | |
|---|---|---|---|
| GND | All GND connections are connected to the GND of Arduino, the +ve terminal of the LEDs, the +ve Terminal of the H2Op | | |
| 5V | VCC of Moisture sensors, Comm of R, VCCof R, + terminal of H2OLv | | |
| A0 | H2OLv S terminal | | |
| A1 | MS1 | | |
| A2 | MS2 | | |
| A3 | MS3 | | |
| A4 | MS4 | | |
| A5 | | | |
| Digital Pin2 | RLD1(-ve) | | |
| Digital Pin3 | GLD1(-ve) | | |
| Digital Pin4 | RLD2(-ve) | | |
| Digital Pin5 | GLD2(-ve) | | |
| Digital Pin6 | RLD3(-ve) | | |
| Digital Pin7 | GLD3(-ve) | | |
| Digital Pin8 | RLD4(-ve) | | |
| Digital Pin9 | GLD4(-ve) | | |
| DigitalPin10 | | | |
| DigitalPin11 | | | |
| DigitalPin12 | | | |
| DigitalPin13 | IN pin of R | | |
| Relay | NO pin is connected to the +ve terminal of the H2Op | | |
| ID | KEY | ID | KEY |
| Moisturesensor1 | MS1 | Green LEDfor MS1 | GLD1 |
| Moisturesensor2 | MS2 | Green LEDfor MS2 | GLD2 |
| Moisturesensor3 | MS3 | Green LEDfor MS3 | GLD3 |
| Moisturesensor4 | MS4 | Green LEDfor MS4 | GLD4 |
| | | Red LED forMS1 | RLD1 |
| | | Red LED forMS2 | RLD2 |
| | | Red LED forMS3 | RLD3 |
| Water pump | H2Op | Red LED forMS4 | RLD4 |
| Relay | R | | |
| Water levelsensor | H2OLv | | |

Table 2 Comparative Table

| **Parameter** | **Client- Server** | **Peer- Peer** | **Publish Subscribe** | **Rest** |
|---|---|---|---|---|
| Availability | Low | High | Marginal | Marginal |
| Reliability | High | High | Less | Less |
| Performance | Marginal | High | Marginal | Less |
| Ease ofSystem | Less | High | Marginal | Less |
| Design | Easier | Marginal | Difficult | Easier |
| Security | Supported | Cannot Guaranteed | Supported | Cannot Guarant |
| Privacy | Marginal | Not Provided | Provided | Not Provide |

## VI. ANALYSIS MODELING

All the aspects of the proposed system will be covered in this chapter in the diagrammatic manner and provides the detailed manner of the system.

- *Use Case Diagram*

To model functionality of the system, we use different actors, external entities ("roles"), and the associated use cases represented on the use case diagram. The use case diagrams are also used to show the functions, actions and services that the systems will perform.

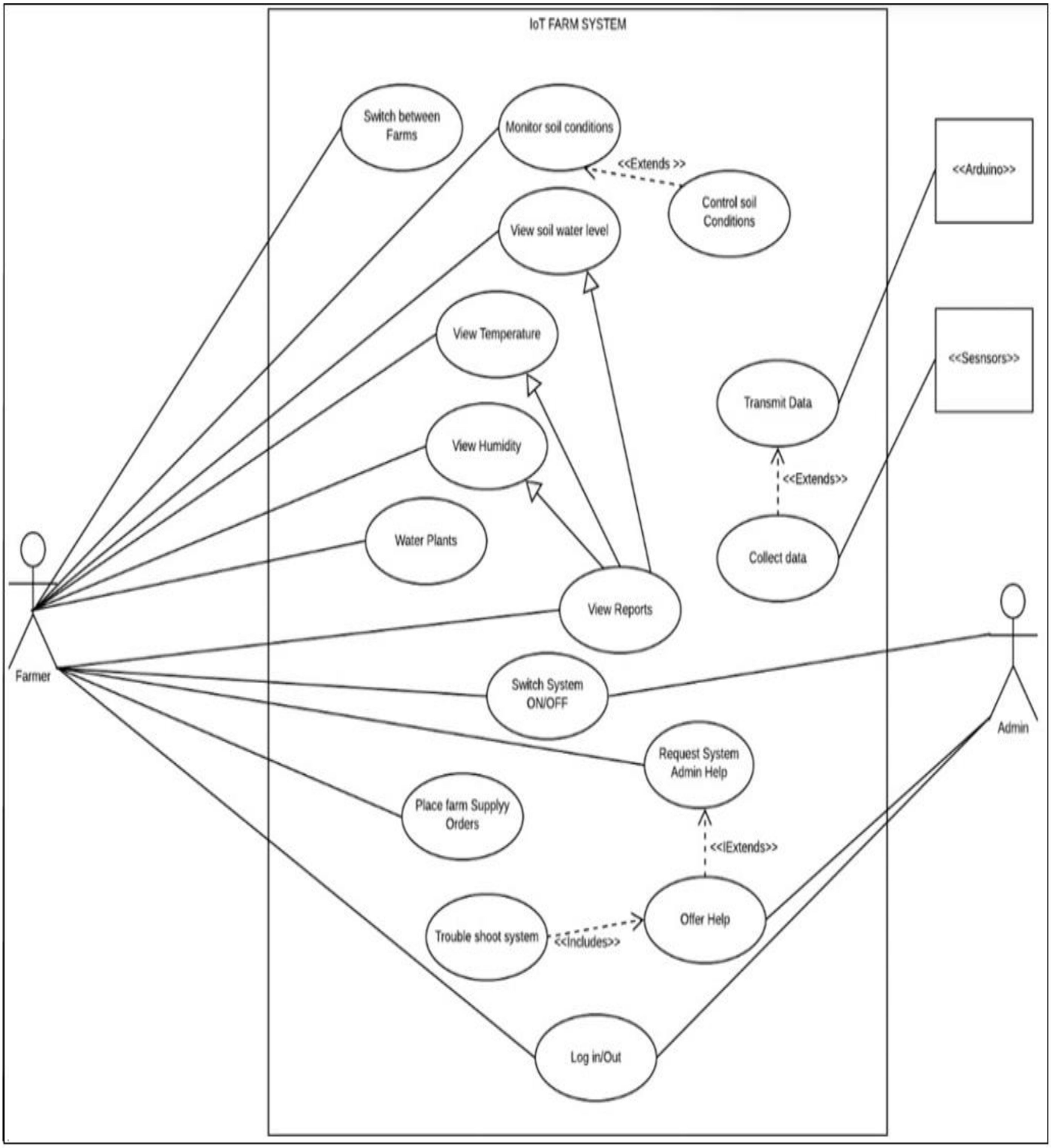

Fig 1 Use Case Diagram

- *Class Diagram*

Class diagrams are structural Unified Modeling Language (UML) diagrams that are used to demonstrate the static view of the system.

They are used to document, visualize and describe different aspects of the object-oriented system as well as for constructing the executable functions and developing the programming code for the system. Class diagrams are widelyused for describing the attributes and operations of the class and constraints imposed on the system.

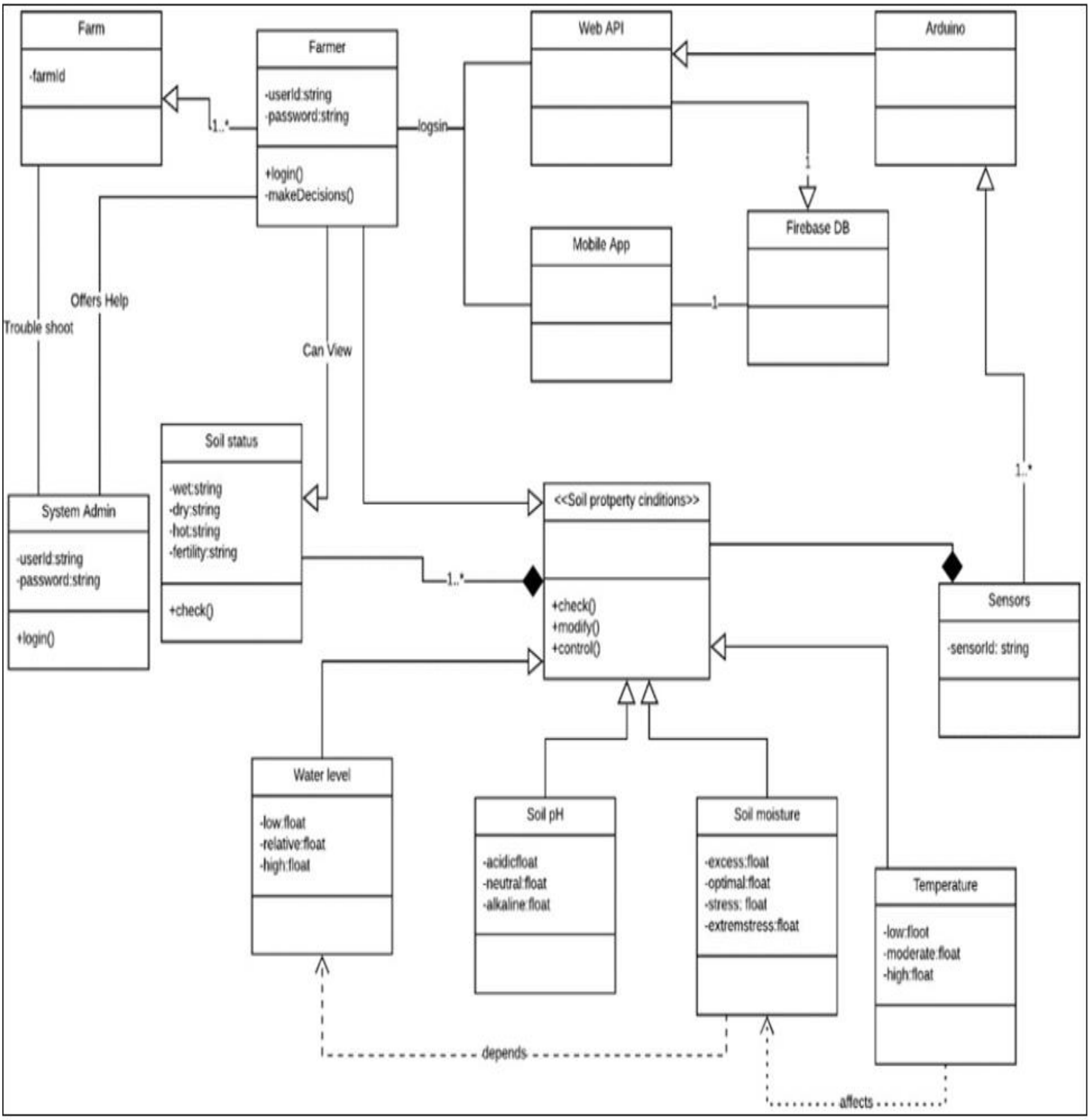

Fig 2 Class Diagram

- *Object Diagram*

Object diagrams can be used to represent specific instances of classes and relationships between them at a point of time. Object diagrams are similar to class diagrams, however, objectdiagrams show the instances of classes within a system. Theyshow the complete or partial view of the structure of a modeled system at a specific time. This can help us study the behavior of the system at a particular instant.

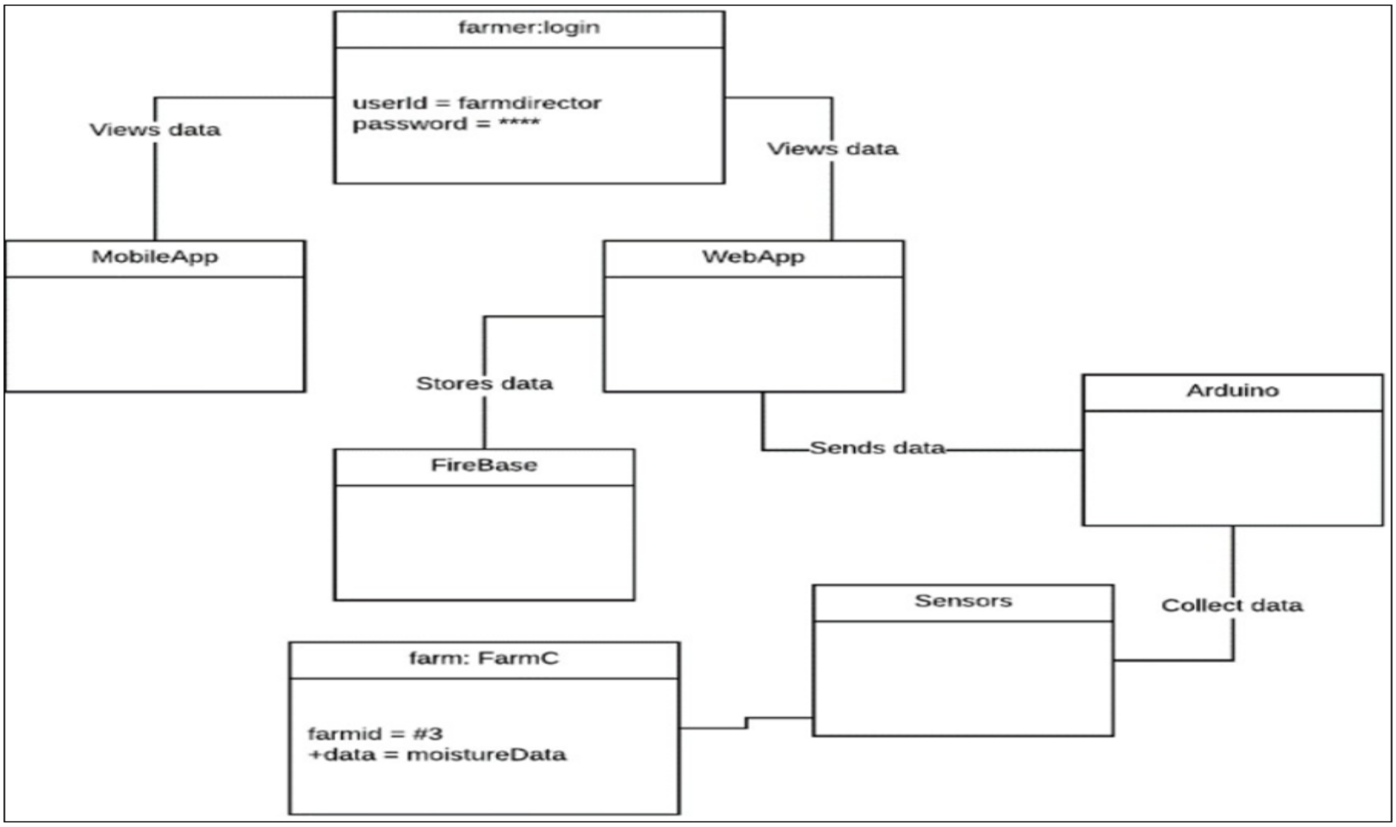

Fig 3 Object Diagram

- *Sequence Diagram*

In order to demonstrate the interaction among classes in terms of message exchange over time/events we use “sequence diagrams” also called “event diagrams”. Sequence diagrams help us validate and visualize several system eventsfor predicting and analyzing how the system will behave.

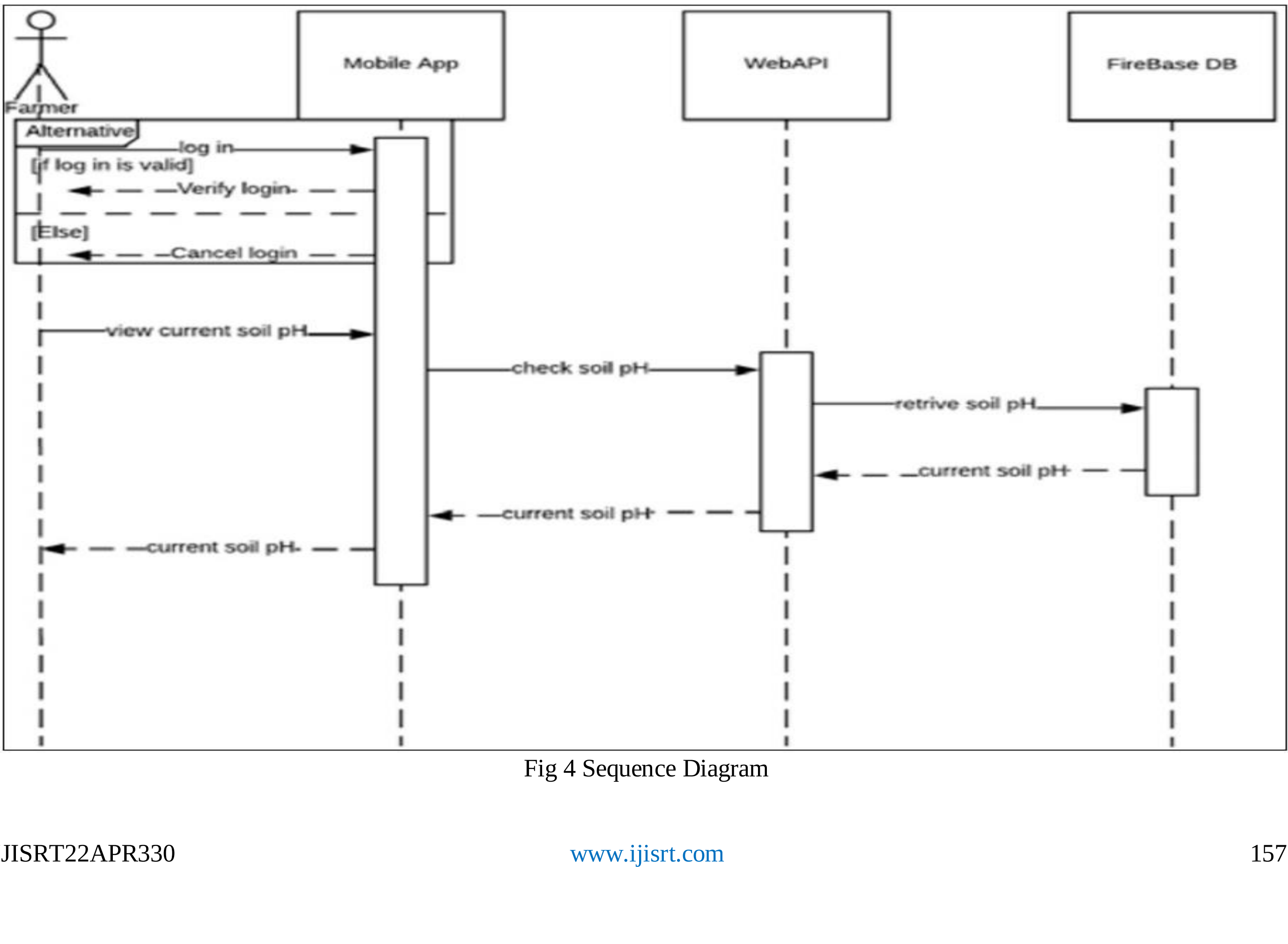

Fig 4 Sequence Diagram

➢ *Flowchart Diagram*

A flowchart is a diagram that depicts a process, system or computer algorithm. They are widely used in multiple fields to document, study, plan, improve and communicate often complex processes in clear, easy-to-understand diagrams. They can range from simple, hand-drawn charts to comprehensive computer-drawn diagrams depicting multiple steps and routes. If we consider all the various forms of flowcharts, they are one of the most common diagrams on the planet, used by both technical and non-technical people in numerous fields.

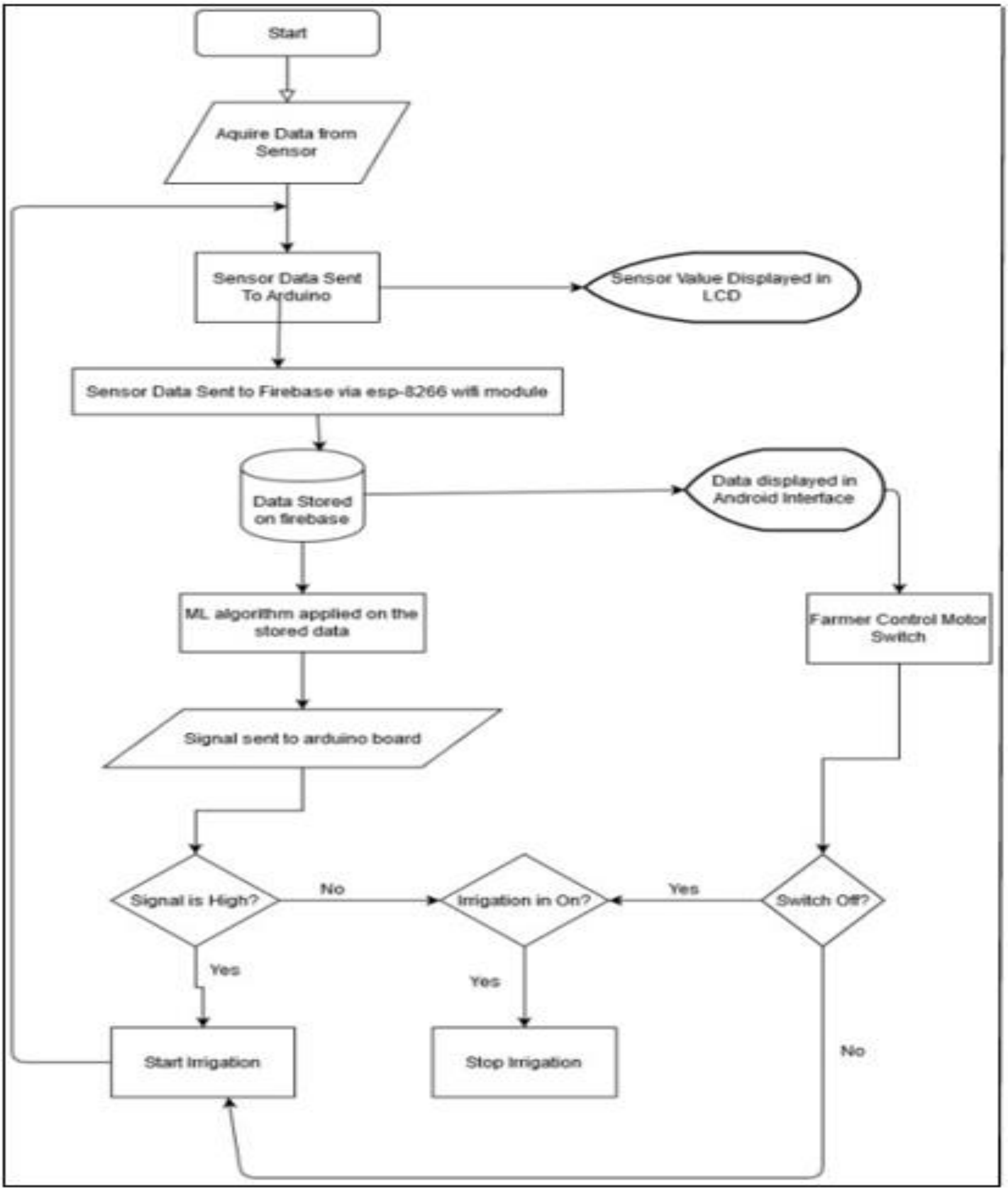
Start
Aquire Data from Sensor
Sensor Data Sent To Arduino
Sensor Value Displayed in LCD
Sensor Data Sent to Firebase via esp-8266 wifi module
Data Stored on firebase
Data displayed in Android Interface
ML algorithm applied on the stored data
Farmer Control Motor Switch
Signal sent to arduino board
Signal is High?
No
Irrigation in On?
Yes
Switch Off?
Yes
Yes
Start Irrigation
Stop Irrigation
No

Fig 5 Flowchart Diagram

## VII. CONCLUSION AND FUTURE WORK

The uses of smart devices with communication and sensing capabilities have unleashed plethora of user services, and at the same time made tasks more convenient and efficient for humans. However, wide adoption of such internet connected devices and data driven applications across various domains have raised security and privacy issues, making these systems vulnerable to cyber-attacks. In this project we look into security and privacy issues and highlights different attacks scenarios in smart farms as well as scenarios affecting the entire food supply chain. The smart farming opposes new challenges, especially in the technological and cyber security domains, being essential that all the involved in the process are aware ofthat.

In agriculture sector, one of the most important factor for the healthy growth of crops is irrigation. The objective of thisproject is to propose and IoT based Smart Farming Systemwhich will enable farmers to have live data of soil moisture environment temperature at very low cost so that live monitoring can be done. We make use of ML to automate the irrigation process to reduce labor cost for the farmers. Future works would focus on optimizing the entire system and incorporating automated defensive (attack) mechanisms towade off intruders in farmlands.

## REFERENCES

[1]. Deepti M. Roser. (2020). Future Population Growth. [Online]. Available: https://ourworldindata.org/future-population-growth.

[2]. M. Gupta, ‘‘Secure cloud assisted smart cars and big data: Access control models and implementation,’’ Ph.D. dissertation, Dept. Comput. Sci., Univ. Texas San Antonio, San Antonio, TX, USA, 2018.

[3]. M. Gupta, J. Benson, F. Patwa, and R. Sandhu, ‘‘Secure V2V and V2I communication in intelligent transportation using cloudlets,’’2020,arXiv:2001.04041.[Online].Available:http://arxiv.org/abs/2001.0401

[4]. J. V. Stafford, Precision Agriculture ’19. Wageningen, The Netherlands: Academic, 2019.

[5]. D. Vasisht, Z. Kapetanovic, J. Won, X. Jin, R. Chandra,

[6]. S. Sinha, A. Kapoor, M. Sudarshan, and S. Stratman, ‘‘Farmbeats: An IoT platform for data-driven agriculture,’’ in Proc. 14th USENIX Symp. Netw. Syst. Design Implement. (NSDI), 2017,

[7]. S. Wolfert, L. Ge, C. Verdouw, and M.-J. Bogaardt, ‘‘Big data in smart farming—A review,’’ Agricult. Syst., vol. 153, May 2017.

[8]. John Nussey. Arduino for Dummies, 2nd edition. JohnWiley & Sons, 2018.

[9]. Lin, D. He, N. Kumar, K.-K.-R. Choo, A. Vinel, and X. Huang, ‘‘Security and privacy for the Internet of drones: Challenges and solutions,’’ IEEE Commun. Mag, Jan. 2018.

[10]. Barreto and A. Amaral, ‘‘Smart farming: Cyber security challenges,’’ in Proc. Int. Conf. Intell. Syst. (IS), Sep. 2018