Volume: 9 Issue: IV Month of publication: April 2021

DOI: https://doi.org/10.22214/ijraset.2021.33689

A Systematic Literature Review of IoT Security in Smart Farming

Arora Kritika[1], Bandarupalli Akash[2]
[1] *Department of Computer Engineering, SVKM's Narsee Monjee Institute of Management Studies, Mumbai*
[2]*Department of Metallurgical Engineering and Materials Science, IIT Bombay, Powai*

Abstract: Internet of Things is no longer a newbie and has paved a long journey acting as the topmost business growth driver. Every business today has started depending on IoT technology for its operational excellence in the market. IoT creates an intelligent, invisible network fabric that can be sensed, controlled, and programmed. IoT has spread its wings to every industry slowly. The Agriculture and farming industry has also embraced IoT technology. These technologies are used by farmers to monitor crop yield and measure soil moisture content to deploying drones to assist with tasks such as applying pesticide spray. With more and more connected devices to the Internet, there are more challenges to be faced securing smart farming environments cybersecurity threats and vulnerabilities. Smart farming is projected to create a massive impact on the agricultural economy by bridging the gap between small and large-scale businesses. This review paper will briefly investigate the security challenges faced by IoT devices at first and later review on its current progress and application in the field of smart farming. With the introduction of smart homes, smart cities, and other smart devices, the Internet of Things (IoT) has formed as an area of importance with potential, and growth. It has been well established that most of these IoT devices are easy to hack and compromise. IoT devices are limited in computational power, storage, and network capacity, and thus they are more vulnerable to attacks than other smart devices such as smartphones, tablets, or computers. Finally, fog computing technology is discussed as a recommended solution to support IoT security in Smart farming are reviewed in this paper.

Keywords: Internet of Things, Smart farming, Cyber Security, Cyberattacks, Fog Computing.

I. INTRODUCTION

Smart farming is a philosophy that uses advanced technology to control farming practices in order to improve the quality and quantity of agricultural products. GPS, soil scanning, data management, and IoT technologies are all available to farmers in the twenty-first century. Farmers may significantly improve the efficacy of pesticides and fertilizers and use them more selectively by specifically measuring different parameters within a field and adapting the strategy.

Similarly, farmers can use smart farming techniques to better track individual animal needs and change feed accordingly, preventing disease and improving herd health. [44-51]

Agriculture has benefited from technological advancements in recent years. Task-specific sensors are used to collect this data. The Internet of Things (IoT) plays an important role in precision agriculture because it collects data that is used to make decisions. Farming processes will become increasingly data-driven and data-enabled as smart machines and sensors appear on farms and farm data grows in quantity and scope.

The phenomenon of Smart Farming is being driven by rapid advances in the Internet of Things and Cloud Computing (Sundmaeker et al., 2016). Although Precision Agriculture only considers in-field variability, Smart Farming goes a step further by basing management tasks on data as well as location, with background and situation knowledge triggered by real-time events (Wolfert et al., 2014).

To carry out agile actions, real-time assisting reconfiguration features are needed, particularly in cases of suddenly changed operating conditions or other circumstances (e.g., weather or disease alert). These features usually provide intelligent assistance with technology deployment, maintenance, and use.61-68] Smart devices enhance traditional tools (e.g., rain gauges, tractors, and notebooks) by incorporating autonomous context-awareness through various sensors, built-in intelligence, and the ability to perform autonomous actions or do so remotely.

While it is already implied in this illustration that robots will play an important role in management, it is likely that the role of humans in analysis and planning will be increasingly supported by machines, resulting in the cyber-physical cycle becoming nearly autonomous. [59-65]

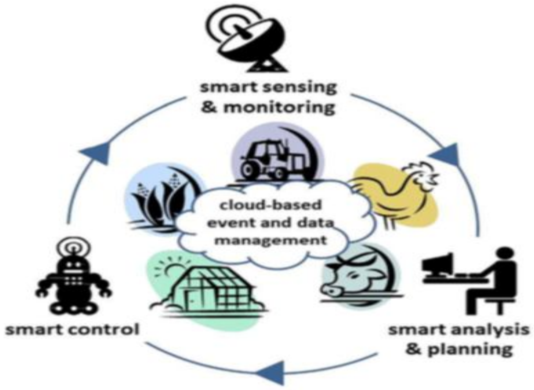


Figure 1 summarizes the concept of Smart Farming along the management cycle as a cyber-physical system [11]

Smart devices enhance traditional tools (e.g., rain gauges, tractors, and notebooks) by incorporating autonomous context-awareness through various sensors, built-in intelligence, and the ability to perform autonomous actions or do so remotely. While it is already implied in this illustration that robots will play an important role in management, it is likely that the role of humans in analysis and planning will be increasingly supported by machines, resulting in the cyber-physical cycle becoming nearly autonomous.

Recently, innovations such as ubiquitous computing, cloud computing, fog computing, and remote sensing have been involved. Smart farming at fog locations with the assistance of downstream computing presents new problems and testing opportunities for future risks. To optimize the benefits of precision farming and its stability, it's crucial to build a complete system with sensor deployment. In addition, in most situations, the sensors are used as relay nodes in addition to gathering data at regular intervals. The more data that passes through a sensor, the more resources it consumes, shortening the network's lifespan and rendering it vulnerable to security threats [2]. As a result, an educated sensor implementation is critical to solving the efficiency and security issues for smart farming applications.

The majority of current smart farming strategies are implemented with no prior knowledge of whether they can result in the most efficient use of available resources. There are no simulator toolkits built for configuring the network of smart farming in the literature. However, there are a few studies that use models in which the data used to make decisions is collected through sensors [3]. Core network properties such as network interference caused by overlapping sensor areas, packet error rate, and energy consumption of the underlying communication model are totally overlooked in such simulations. These properties have an impact on the architecture's security in a noticeable way. According to the analysis of the literature, no such strategy exists that enables data processing at shared fog locations in order to mitigate or eliminate security risks.

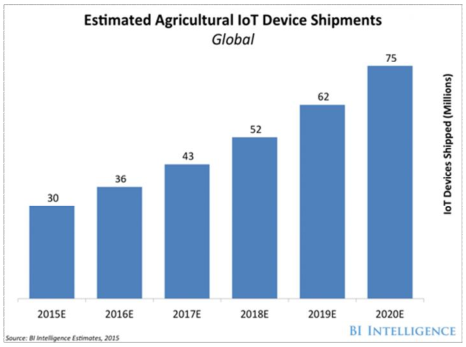
The aim of this paper is to discuss various security issues and threats that have been encountered with smart agricultural devices and to suggest a solution based on fog computing. The remainder of this paper is structured in the following manner. Section II discusses the Internet of Things architecture for smart agriculture and farming. Section III discusses the many security concerns and obstacles that smart farming faces. The suggested solution and its execution are highlighted in Section VI. Section V summarizes the test findings, and Section VI brings the paper to a close by shedding light on future research in smart farming and its security implications.

II. STATISTICAL VIEW ON PRECISION FARMING

Agriculture is the economic backbone of India. It accounts for nearly 66% of total employment opportunities in the region. However, conventional agricultural methods are not sustainable and cannot ensure the sector's survival and development.

The Indian Precision Agriculture Market was worth over $ 57 million in 2019 and is expected to expand at a CAGR of over 10% to reach $ 99 million by 2025, owing to growing knowledge about precision agriculture's applications and the the need to maximize yield from small farms. [70-71]

Additionally, the application of advanced analytics, the adoption of the Internet of Things (IoT) in agriculture, and the expansion of supporting government initiatives for the adoption of modern agriculture technologies are all driving the Indian Precision Agriculture Market. Additionally, the demand for data on crop health, local weather forecasts, and soil is expected to drive demand for precision agriculture during the forecast era. However, high costs and a lack of knowledge about innovations and their benefits are major roadblocks for India's precision agriculture industry. [61-59]



Source: BI Intelligence Estimates, 2015

Figure 2 gives an estimate of the agricultural IoT device shipments globally [60]

Agriculture technology is also receiving funding from India's central government, which is aiming to double farmers' incomes by 2022. To this end, the NITI Aayog is partnering with companies such as IBM to pilot technology-enabled agricultural solutions. This is in order to provide farmers with real-time advice. For example, artificial intelligence is being used to build models of crop yield defence. [60-59]

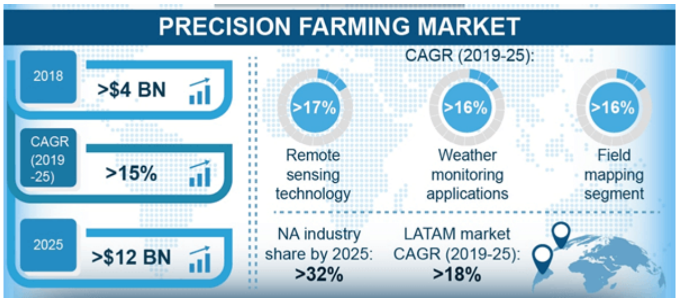


Figure 3 gives an estimate of the growth of precision farming from 2019-2025in terms of market size [59]

Additionally, the Government of India intends to computerize the Primary Agricultural Credit Society (PACS) with a grant of nearly INR 2,000 crore to benefit cooperatives. Additional government initiatives to promote smart farming in India include the establishment of the National Centre for Management of Agricultural Extension (MANAGE) in Hyderabad, the launch of the Pradhan Mantri Krishi Sinchayee Yojana (PMKSY), One Nation One Market, and mentoring agriculture-technology start-ups.

Farmers in the southern states of Andhra Pradesh, Telangana, and Tamil Nadu are increasing crop yields through a variety of precision agricultural methods. Precision agriculture enables farmers to raise their income per acre by 35% to 60%. It can also help mitigate agricultural water pollution, Accenture Interactive India's Achal Sharma said recently on the side-lines of the World AgTech Congress in Delhi. [58–61]

III. TRADITIONAL IOT ARCHITECTURE

The word "Internet of Things" was coined in 1999 by Kevin Ashton, executive director of MIT's Auto-ID Center, and has since taken on many slightly different meanings. There is no universally accepted concept of IoT at the moment, though many formalizations are available on the web and in the literature [21]–[24]. The International and Telecommunication Union's (ITU) concept is used in this work: "Internet of Things" is "a global infrastructure for the information society that enables advanced services through the interconnection of (physical and virtual) things using existing and emerging interoperable information and communication technologies (ICT). [25]

A thing is defined in this context as "an object of the physical world (physical things) or the information world (virtual things) that is capable of being identified and integrated into communication networks", while a device is defined as "a piece of equipment with mandatory communication capabilities and optional sensing, actuation, data capture, data storage, and data processing capabilities". [25.]

In a nutshell, the Internet of Things is a set of computing devices (specifically, things) that are connected through the Internet and designed to provide services for a variety of applications while meeting security requirements. [25]

Three layers comprise the IoT architecture: device layer, network layer, and perception layer. This section discusses these strategies in detail:

A. *Application Layer*

This layer is responsible for providing the customer with application-specific services. Additionally, it specifies applications for the Internet of Things. [4, 5, 6] It is the layer from which cloud applications store, manage, and access or retrieve data as required for processing.

B. *Network Layer*

This layer is in charge of linking intelligent objects, network devices, and servers. Additionally, it is used to transmit and process sensor data. It links sensors to the server in smart farming to relay data upward for further processing. [6,7].

C. *Perception Layer*

This layer is where sensors detect and collect data about the environment. It detects and recognizes physical parameters or other artifacts in the world. For instance, relative humidity, temperature, and precipitation conditions. [8]

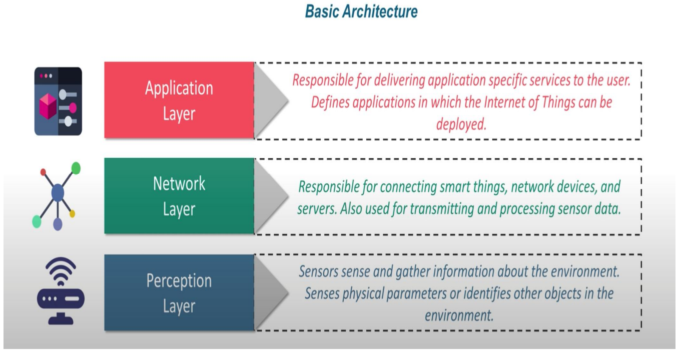

Basic Architecture
Application Layer
Responsible for delivering application specific services to the user. Defines applications in which the Internet of Things can be deployed.
Network Layer
Responsible for connecting smart things, network devices, and servers. Also used for transmitting and processing sensor data.
Perception Layer
Sensors sense and gather information about the environment. Senses physical parameters or identifies other objects in the environment.

Figure 4: showing the basic architecture of IOT using application layer, network layer and, perception layer with the detailed description of their functions [9]

More recently, innovations such as ubiquitous computing, cloud computing, fog computing, and remote sensing have been incorporated. Smart farming with backend computing help at fog locations creates new challenges and avenues for research into possible threats.

D. *Essential Characteristics Of Internet Of Things*

The following sections summarize the major characteristics of the Internet of Things [24], [25], [32]:

1) *Interconnectivity*: Anything in the Internet of Things is capable of being linked to the global networking and knowledge infrastructure;
2) *Things-related services*: The Internet of Things enables the provision of thing-related services within the constraints of things, such as private security and semantic continuity between physical and virtual things;
3) *Heterogeneity*: devices in the Internet of Things may be built on a variety of different networks and hardware platforms. Additionally, they can communicate with various service platforms and devices through various networks;
4) *Constrained resources*: The Internet of Things usually requires devices that face energetic and technological constraints;
5) *Dynamic changes & the uncontrolled environment*: in the Internet of Things, the state of the system (e.g., sleeping/awake, connected/disconnected) and context (e.g., position, speed) change dynamically. As a result, IoT devices operate in an unregulated environment characterized by chaotic surroundings and unreliable user-device interactions caused by unstable network access and complex device state changes. Additionally, the number of devices will fluctuate dynamically;
6) *Huge scale*: the number of devices that must be handled and communicate with one another is enormous and will continue to grow in the future. Additionally, the proportion of communications caused by machines will continue to increase at the expense of human-triggered communications. Perhaps more important would be the management and analysis of data provided by such devices in order to facilitate the exchange of knowledge.

IV. SMART FARMING ECOSYSTEM CYBER ATTACKS

One such device is an Internet of Things (IoT) device used in smart farming and agriculture. The proliferation of sensor-based technology has increased the risk of cyberattack. It is critical to consider the numerous security concerns associated with the implementation of smart applications; if any of them are compromised, they can have a detrimental effect on the agricultural economy.

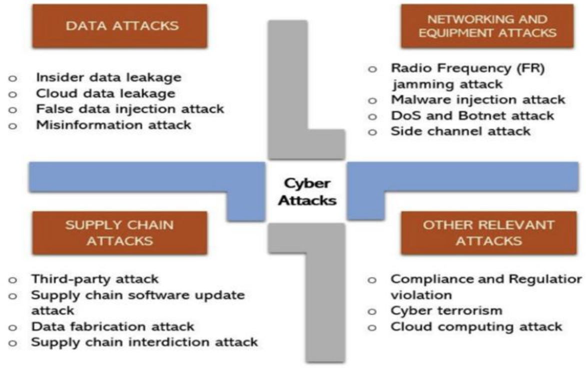


Figure 5: summarizes the various cyber-attacks that occur in a smart farming ecosystem [30]

A. *Data Attacks*

1) *Insider Data Leakage:* At the perception or physical layer of smart farming, a large amount of complex and dynamic data is produced. This information is derived from environmental variables such as soil moisture content, relative humidity, water level, and temperature. When this data is transferred to the upper layers for further processing, it becomes vulnerable. Leakage or breach of such data, whether by a hacker or an insider, will result in financial loss to farmers. For instance, the disclosure of land, crop, and agriculture purchasing information will result in significant economic losses for farmers. Farmers also employ third-party analytics to analyze data that can be used to forecast supply and the agricultural economy. An attacker can attempt to phish for such third parties in order to steal their data. [10-12]
2) *Misinformation Attack:* Farmers usually fear data leakage in smart farming because it can be used against them and has a negative impact on the economy as a whole. Smart farming has been affected by big data, and it now encompasses the whole supply chain, which is supposed to be kept secret. Smart sensors and devices generate massive amounts of data that assist farmers in making crop and plant selection decisions. If an insider sells this data for profit, it can have a detrimental impact on the farmer's economy. [13-16]
3) *Cloud Data Leakage:* Data is stored on a trusted cloud provider such as google, amazon web services, or azure in IoT devices. Smart farming also makes use of such clouds to store data from the IoT architecture's lower layers. If sensitive agricultural data is stored in a foreign country's cloud, it can be easily manipulated. It is important to make a judgement call on the location of sensitive data. For example, in Spain, there is a law requiring data users to obtain consent from each individual employee and then exercise discretion in terms of cloud storage. [17]
4) *False Data Injection Leakage:* This is the type of attack that compromises sensors and actuators at the physical or perception layer. In smart farming, an attacker may forge sensors to provide an incorrect reading of the humidity or soil moisture content. This, in turn, would influence farmers' decisions and wreak havoc on their crops and seeds. [17]

B. *Network And Equipment Attacks*

1) *Malware Injection Attack:* This is an attack in which an attacker infects a linked smart device with malware. The majority of farmers in smart farming are linked to the Internet. Malware is capable of stealing all sensitive information about the consumption of agricultural products, the procurement of fruits, vegetables, and livestock, as well as information about agricultural machinery. Additionally, malware can impair the functionality of intelligent physical equipment, which can have a detrimental effect on a specific crop. [18]
2) *Denial Of Service Attack:* IoT devices used in smart farming environments are vulnerable to Denial-of-Service Attacks, in which an attacker sends a large number of garbage requests to the server, causing it to hang. In this case, the server refuses the user any operation. If this occurs, any individual farmer can have trouble logging into their account to collect critical field data [19-20].

3) *Radio Frequency (FR) Jamming Attack:* In many cases, intelligent farming equipment communicates through radio frequency networks, such as cellular or satellite networks. Global navigation satellite systems (GNSS) are often used by smart farming equipment to increase productivity with products and techniques such as route planning, auto-steering, seeding, and spray speeds. GNSS is accomplished by fusing GPS and real-time kinematics (RTK) technology in order to improve the pre-vision of real-time position data. Attackers can jam GNSS for malicious purposes by deploying a large number of distributed low-power jammers to disrupt GNSS signals over a large region, preventing smart farming equipment from operating properly.

4) *BOTNET:* All is capable of being linked to the Internet through IoT. At each architectural layer of a smart farming ecosystem, there are numerous IoT-enabled devices. These devices are vulnerable to attack and can then be taken over by a malicious central machine. This results in the creation of a so-called 'Botnet of Things' [71]. A zombie horde of infected field workers IoT devices [72] may easily be used to infect numerous other networks through a variety of different mediums, and thus a smart farm can become a cybercriminal's internet of vulnerabilities. Security is not a priority when designing smart farm devices, and even when it is, users often overlook the fundamental steps involved in establishing adequate cybersecurity protection mechanisms.

5) *Side Channel Attack:* Side-channel attacks are those that are motivated by obtaining knowledge about how a system is implemented rather than by identifying weaknesses in the system's implementation. As an IoT use case, smart farming inherits many common IoT vulnerabilities, including side-channel attacks [73]. There are numerous channels that attackers can manipulate in such attacks. For instance, in timing channel attacks, adversaries can exploit computation time as well as cache miss and cache hit timing patterns. Other potential attack vectors include hardware glitches in the form of voltage fluctuations and variations in the device clock time during execution tasks. Other potential attack vectors include power consumption patterns, electromagnetic leaks, and even sound and acoustic networks.

C. *Other Relevant Attacks*

1) *Compliance And Regulation:* Food processing and farming are highly regulated sectors, with various national authorities regulating food production in different countries. The Environmental Protection Agency [65] and the Department of Agriculture [66] also enact different legislation and industry standards in the United States. In the European Union, this role is shared by the Department of Agriculture and Rural Development [67] and similar authorities in other countries. These federal agencies issue enforcement orders to ensure the production of safe food. These agencies are increasingly relying on data produced by farm-based sensors as a result of the advancement of smart farming technology. An adversary attacking a smart farm may inject false data with the intent of interfering with various compliance certification processes. If this certification procedure is invalidated, it can have a negative effect on a nation's food supply, crop prices, and so on. The intricate smart farming ecosystem generates a large attack surface that must be covered in order to maintain data integrity.

2) *Cyber Terrorism:* Increased use of modern, integrated networks in agriculture provides terrorists with new opportunities to target locations that were previously too distant or difficult to attack. Since cyber terrorism is a low-cost endeavour with a high payoff potential, the risks of agro-terrorism are too great to ignore. As a result, it is crucial to develop solutions that ensure confidence and accountability within the smart farming concept, while also protecting critical resources.

3) *Cloud Computing Attacks:* The cloud ecosystem is extremely diverse, decentralized, heterogeneous, and strong. Due to the massive amount of dispersed capital, the Cloud is a difficult objective. However, with the advent of new cloud concepts (e.g., on-demand services, auto-scaling, and self-provisioning), attackers have taken advantage of such capabilities, and the cloud has become one of the most attractive targets for attackers. For instance, since the advent of auto-scaling in the Cloud, a sizable proportion of virtual machines hosted on the Cloud are configured similarly. If one virtual machine is compromised, it is highly likely that all auto-scaled virtual machines are compromised as well. As a result, malware that infects a single virtual machine can easily spread to other virtual machines. The infected machines can be used as part of global botnets, which can then be used to conduct large-scale distributed denial of service (DDoS) attacks, crippling the Cloud's functionality. For instance, in 2018, a large-scale DDoS attack on GitHub resulted in an unprecedented spike in traffic to 1.35 terabits per second. Inevitably, DDoS attacks would increase in frequency, power, and sophistication. A large-scale DDoS attack with an enormous volume of requests, packets, or messages will disable smart farms' services, effectively paralyzing their brains. Additionally, DDoS attacks may not be directed directly at smart farm virtual machines. Even if an attack is aimed at a different goal, if the virtual machines used by smart farms are located on a secure physical server, they would automatically block off traffic from other sources.

D. Supply Chain Attacks

A supply chain attack, also known as a value chain or third-party attack, happens when an outside partner or vendor with access to your infrastructure and data infiltrates your system. Through the use of IoT technology at each point of the supply chain, a possible vulnerability to the system's critical data is introduced. In agriculture, the supply chain is comprised of producers, auctions, wholesalers, importers, and exporters. An assault on agricultural equipment and fertilizer manufacturers could potentially disable vital linked machinery at a critical time. It has the potential to exploit the amount of nutrients in fertilizers, thus destroying crops rather than nourishing them [21].

V. USE CASE DIAGRAM FOR SMART FARMING

Use case diagrams are used to collect information about a system's specifications, including internal and external factors. There are mostly design specifications. Thus, when a system's functionalities are gathered, use cases are created and actors are defined. To comprehend a system's dynamics, we must employ a variety of diagram forms. One of them is the use case diagram, which is used to collect system specifications and actors. [57 and 58]

Use case diagrams depict the system's events and their sequences. However, the use case diagrams never explain the implementation process. A use case diagram can be thought of as a black box with only its input, output, and function understood.

These diagrams are used at the most advanced stages of design. This high-level design is iterated upon in order to obtain a complete and functional representation of the method. Additionally, a well-structured use case outlines the pre- and post-conditions, as well as any exceptions. These additional elements are used to create test cases during the testing process. [58 and 59]

After completing the initial mission, use case diagrams are created to depict the external view.

In summary, use case diagrams are used to

1) Collect specifications for a system.
2) Used to provide an external perspective on a device.
3) Determine the external and internal influences that have an impact on the system.
4) Demonstrate the relationship between the criteria and the actors.

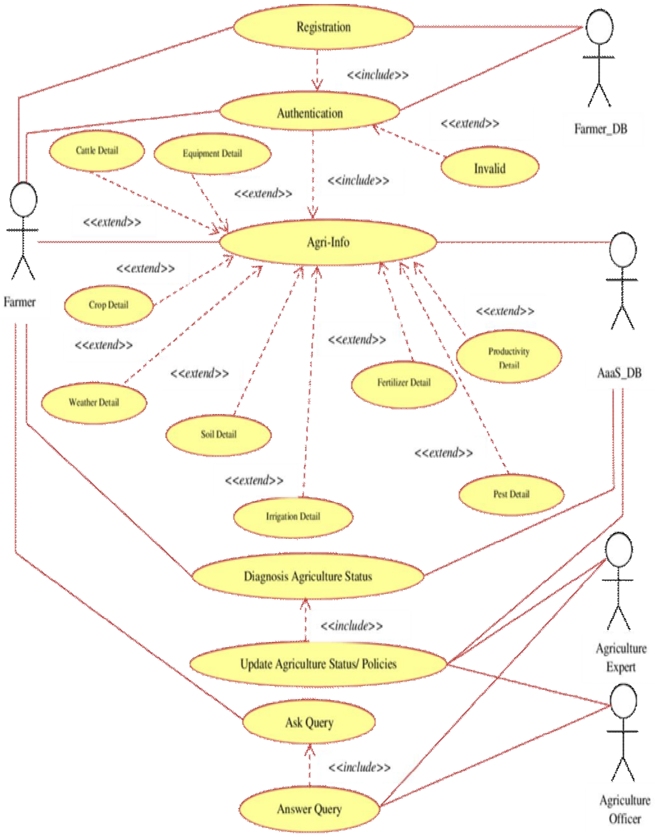


Figure 6: shows the flow of basic activities in smart farming ecosystem [58]

Farmers, farmer DB, agriculture specialist, agriculture officer, and Aaas DB are all involved in this case. The farmer can communicate with a variety of use cases, including registration, authentication, agri info, agriculture status diagnosis, and query. Via the two use cases of registration and authentication, a farmer DB is maintained. The use cases that provide necessary information about crop-suitable field parameters are cattle detail, equipment detail, weather detail, soil detail, fertilizer detail, pest detail, productivity detail, and irrigation detail. Each of these use cases has an extended relationship with the agri info use case, which is used to further define the various activities of the agri info. This agriculture data is stored in an Aaas DB database for the purpose of diagnosing the state of agriculture. Additionally, as shown in the diagram, only agriculture experts are allowed to update agriculture policies. Additionally, the Update Agriculture Status use case has an include relationship with Diagnosis Agriculture Status, indicating that the status can be modified only after the diagnosis is complete. The actor above the Agriculture officer is available to answer any questions a farmer might have about the system's operation at any time.

VI. USE CASE DIAGRAM FOR SECURITY CHALLENGES IN SMART FARMING

The use case diagram provides an overview of how a danger can affect both the farmer who is the system's user and the administrator who maintains the system on a daily basis. The actor administrator will take part in use cases such as backing up the system, configuring the system, inspecting the operation log, and updating virus security. If the Admin actor in the diagram takes an insecure backup of data, a threat to the agriculture system would result. [58]

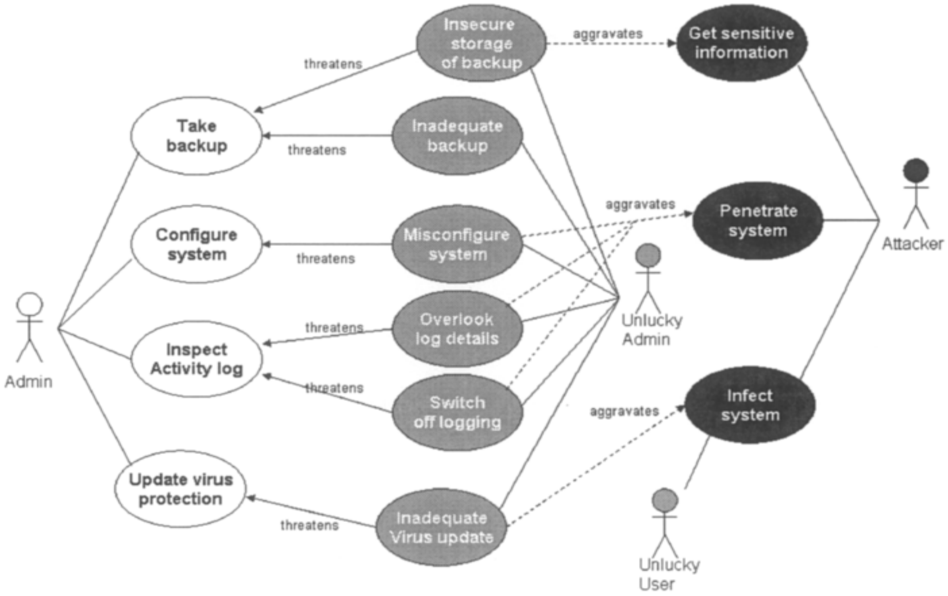


Figure 7: shows the various use cases that might lead to a threat in smart farming ecosystem [58]

Similarly, if the administrator does not perform appropriate backups, misconfigures the system, overlooks log details/switches off logging, or performs insufficient virus updates, a vulnerability to the system is possible. The intruder can obtain confidential information, penetrate the system, or infect the system, resulting in an attack on the system, which results in the farmer and administrator becoming unfortunate and losing control of the system.

VII. FOG, EDGE AND CLOUD COMPUTING:

Realizing the promise of the Internet of Things cloud computing was undeniably the dominant computing model over the last decade and would continue to be a focus of research for many years. Nonetheless, the IoT's rapid spread has eroded its power. Indeed, there are many IoT-related problems that cloud computing is ill-equipped to solve. As a result, interest in Edge computing has grown, as it aims to address IoT problems by relocating computation to the network's edge. Fog computing found its way through this transition, encapsulating the emerging paradigm that completely crosses the divide between Cloud computing and IoT. [70-71]

Cloud computing, as defined by NIST, [18] is a model for enabling universal, easy, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, software, and services) that can be rapidly provisioned and released with little management effort or service provider involvement.

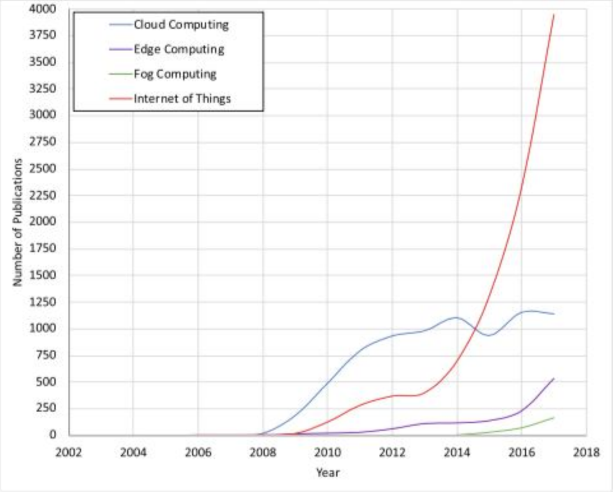


Figure 8: shows the relationship trend of Cloud, Edge, Fog and Internet of Things [68]

Cloud computing has been the dominant standard for the last decade. Computing, power, and data storage have all been centralized and transferred to the Cloud in response to this trend [20]. On the other hand, the Internet of Things (IoT) is gaining traction. There were approximately 20 billion IoT-connected devices in 2017, which will increase to approximately 30 billion in 2020 and more than double by 2025. The emerging IoT introduces a slew of new problems that Cloud computing struggles to address due to its own limitations. The emergence of IoT signals the start of the post-Cloud period. While the majority of IoT data is currently stored in the Cloud, the close relationship between Cloud and IoT poses many new problems that Cloud computing alone cannot completely solve. Edge computing, as the highest development of the Edge computing concepts, has become feasible and extremely interesting in this sense, as has Fog computing.

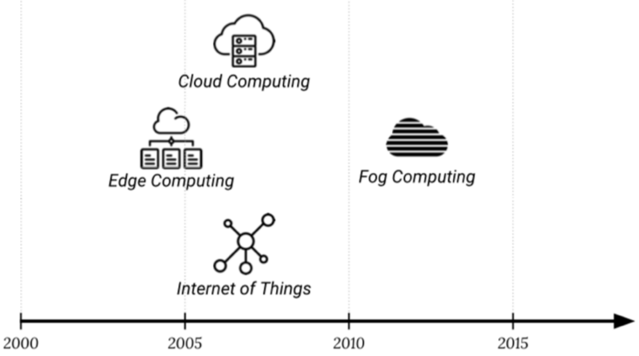


Figure 9: shows the growth of the various technologies over a period of 2000-2015

Edge computing is a new paradigm born of the need to transfer computation to the network's edge. While the term "Edge computing" first appeared in the literature prior to the Cloud, the growing interest in Edge computing coincides with the emergence of IoT and associated new challenges.

Fog computing is frequently regarded as a type of edge computing [3], [38], [39], [42], [45]. Indeed, fog computing enables the user to interact with distributed computing, storage, power, and networking capabilities [46]. However, the literature review indicates that Fog computing is not just another implementation of Edge computing; rather, it is the pinnacle of the Edge computing concepts. Indeed, fog computing is not restricted to the network's edge; it integrates the idea of Edge computing, creating a standardized intermediate layer that fully crosses the divide between IoT and Cloud computing. Indeed, since Fog nodes can be placed anywhere between end devices and the Cloud, they are not necessarily directly connected to them. Additionally, fog computing is not limited to the "stuff" side, but also offers services to the Cloud. Fog computing, in this vision, is not simply an extension of the Cloud to the network's edge, nor is it a substitute for the Cloud; rather, it is a new entity that works between the Cloud and the IoT to completely help and enhance their relationship, incorporating IoT, Edge, and Cloud computing.

VIII. PROPOSED SOLUTION

To combat cybercrime through multiple layers of the IoT architecture, we integrated fog computing into our smart devices in the farming ecosystem. Fog computing is critical for enabling reliable, accurate, and manageable communication between a large number of intelligent IoT devices. With its unique characteristics such as low latency, security, location awareness, and a large number of server nodes, it enables real-time connectivity and mobility. Through offering Network Level Virtualization (NLV) and real-time data services, fog computing enables users to take complete control and management of the network. Open pipe implements NLV through a hybrid model that includes a virtual Software Defined Network (SDN) controller (located in the cloud), virtual local controllers (located in the fog), virtual radio resources (for wireless communication), and a virtual cloud server. [22-24]

Now, for field implementation, we'll assume a Farm F with dimensions (length. Width=law) and sensors denoted by S. The system is capable of supporting an infinite number of heterogeneous sensors with varying transmission energies Es and transmission times Ts. Static/mobile sensors are installed at locations S_{xy}. These sensors aid in the exchange of information between farms.

There is support for unmanned ground-based controllers (UAVs) to collect data from sensors and/or to forward data to a backend server for data analytics and real-time decision making. Each UAV is equipped with a contact range Ru and an energy capacity Eu. [25]

The sensors in this case work in two modes: sleep and active. Between deployed sensors and UAVs, communication is accomplished through an orthogonal frequency-division multiple access uplink. Distributed environment with UAVs collaborating with nearby fog locations to share data. Fog nodes are computational tools that are used to receive, process, and temporarily store incoming UAV streams. Line of sight (LoS) must be formed between the Fog nodes in order for communication to be efficient. The probability of LoS occurring is computed using the formula P_{LoS} as described in [26].

$$p_{\mathrm{LoS}} = \frac{1}{1+\rho \times \exp(\sigma[\Phi - \mu])} \qquad (1)$$

where φ is the elevation angle between the location of sensor Sxy and the UAV Uxy, and ρ and σ are constants based on communication frequency and type of area (rural or urban).

Noting that the probability increases with increasing UAV altitude, deployed sensors can be allocated to the jth UAV only if the LoS probability is closer to 1, or pLoS. As a result, the condition that exists between the sensor and the UAV is specified as

$$d_{ij} \leq \frac{h_j}{\sin(p_{\mathrm{LoS}})} \qquad (2)$$

where *dij* represents the distance between the i_{th} sensor node and the j_{th} UAV, and *hj* is the altitude of the UAV. Assuming *m*×*n* sensors deployed across the farm then the coverage time *tc* of UAVs is computed as

$$t_c = \sum_m \sum_n T_{mn} + \frac{2}{M} \sum_k \sum_j S_{kj} \qquad (3)$$

where *Tmn* represents the time to move UAV from one sensor to another, *Skj* represents the number of sensors traversed, and *M* represents the total number of UAVs used during the data gathering process.

We use a collection of brokers B to handle fog locations in order to analyze data. A broker node is responsible for the efficient use of fog services available to users.

The broker distributes the resource to other brokers in the vicinity. This contributes to the reduction of contact delays. The network delay td is proportional to the distance between nodes, as follows: td = da +db, where db is the delay between the UAV and the assigned fog spot, and da is the network delay between the sensor and the UAV. By contrast, the network cost C is a linear function of distance denoted by

$$C = \varphi \cdot \left(d_{i,j} + \sum_{k \in B \& j \neq k} d_{j,k} \right) \qquad (4)$$

Where φ is a constant, *di,j* is the distance between the *i*th UAV and its local broker *j*, and *dj,k* is the distance of the local broker *j* to brokers leasing compute resources *j* ∈ *B*.

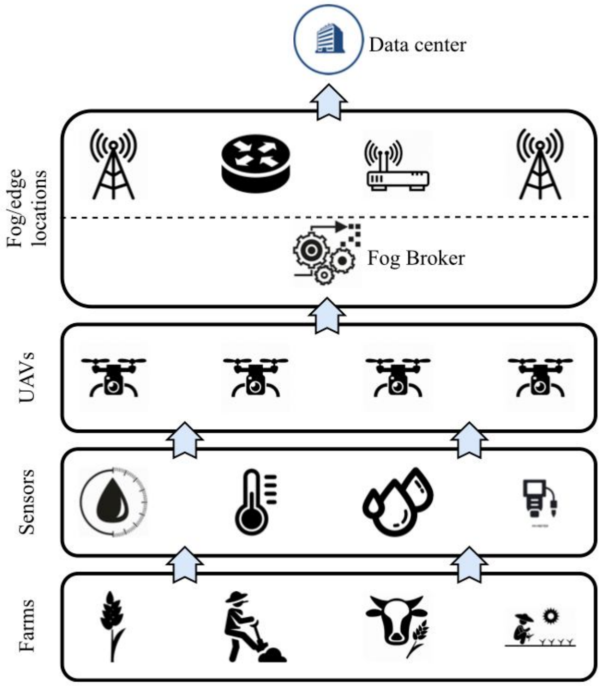


Figure 10: represents Smart farming toolkit layered architecture.

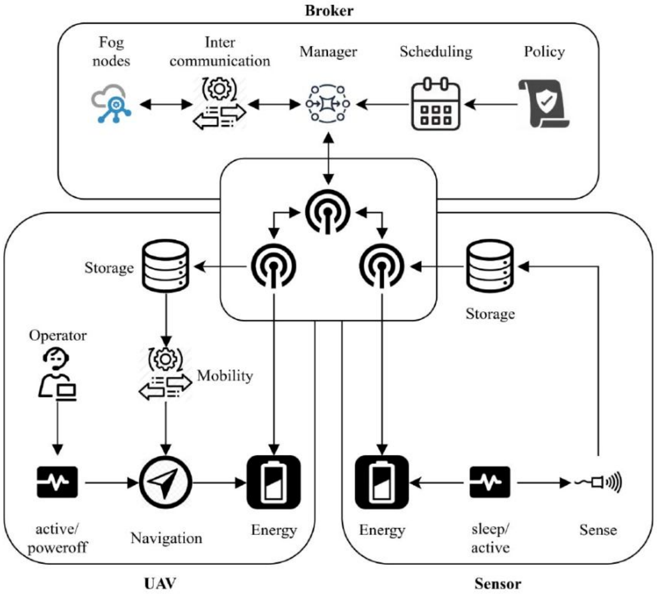


Figure 11: Internal architecture of the proposed framework

Each fog location contains M fog resources. We use a series of broker B to control fog positions in order to process the gathered data. A broker node is responsible for optimizing the use of fog services located near end users. The UAVs have prior knowledge of the sensors deployed and their specific identifiers. The UAVs sequentially call out the sensors and only request that they respond to this call.

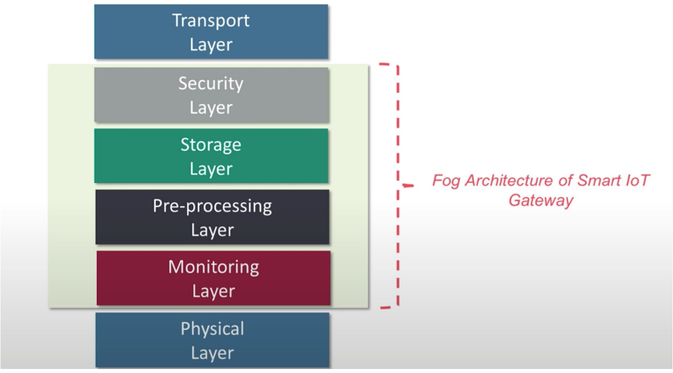


Figure12: Represents Fog computing architecture with layered approach, which inserts monitoring, preprocessing, storage, and security layers between physical and transport layers.

The following algorithm illustrates how UAVs operate. The UAVs gather data from deployed sensors and forward it to fog nodes for further processing in the upper layers of the fog computing architecture, ultimately sending it to the cloud, where semantic tagging and classification of data takes place in the fog layer, providing refined data to the cloud system. The virtual cloud server's SDN controller satisfies the requirement for real-time, low-latency data collection. To bind SDN and local controllers, the Extended Open Flow protocol is used. Load balancing, handover events without losing Quality of Service, low energy consumption, and low network overhead are all advantages of using SDN controllers. Additionally, the device provides a reduction capability for reducing data exchange with Fog nodes, concentrating on the preservation of personal and sensitive data during transmission. Additionally, since sensors relay data only when they are involved, the proposed framework would never risk crashing the underlying fog system.

Algorithm 1 UAV Execution

```
    Input B: list of fog brokers; S: list of sensor nodes;
          t: advertisement interval
    Output status message
while true do
    broadcast()                     ▷ UAV advertises after every interval t
    connect(B)                 ▷ Connect to nearby fog locations or brokers
    (id,data) ← recv(S)                   ▷ Receive data from sensors
    if data ALREADY Received then
        ignore()                              ▷ Discard received data
        broadcast(S,IGNORE)
  ▷ Broadcast to all sensors not to relay data or send to UAVs
    else
        b ← getbroker(B)
        send((id,data),b)               ▷ Forward data to nearby fog node
    end if
end while
```

The AES encryption algorithm can be used to bolster the fog platform's security. The size of the encryption key is critical for encryption power. The fog network requires a significant amount of energy. The encryption algorithm chosen (symmetric, asymmetric, or hybrid) should be compatible with the infrastructure requirements.

IX. CONCLUSION

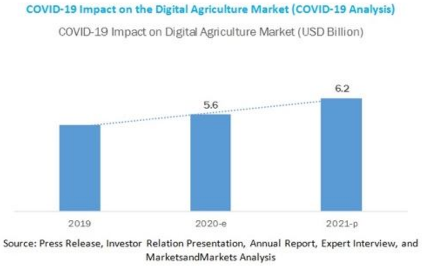
The majority of work in smart farming is focused on real sensor nodes that are linked to end systems for monitoring. We give a complete farming ecosystem in the proposed solution, which includes sensors, UAVs, and fog locations. Additionally, the device contains a cloud-based SDN controller for load balancing. In summary, the solution enables the user to deploy sensors, collect data via unmanned aerial vehicles, and support cloud server computing via fog computing for refined data transmission. In the future, AES encryption can be used to further secure data at the cloud level by combining it with a suitable machine learning algorithm, thus creating a platform for big data analytics and an intelligent framework for smart farming.

X. FUTURE OF PRECISION

The global influence of the raging COVID-19 pandemic has been felt. It has had a major effect on any sector across sectors and has significantly hindered economic growth. Its presence can be felt in India's industrial sectors as a result of the nationwide lockdown enforced to contain the virus' spread. The agricultural sector appears to be the silver lining, as it expanded by 5.9 percent in the January to March quarters, despite the COVID-19 crisis, while the Indian economy expanded by just 3.1 percent. According to Crisil's forecast, agriculture will expand by 2.5 percent, while GDP can contract. [52-55]

Technological agricultural systems are critical to sustaining the agricultural sector's development. **Kisan Suvidha**, a free Android application produced by the Indian government, now has approximately 100 million registered users. This app provides farmers with pertinent information about the current day's and five-day forecasted weather, market rates, dealers, agro advisories, and plant safety.[51-55]

By digitizing the farm and the farmer, it is possible to maximize the use of data and information derived from these tools. With the coronavirus outbreak and the social-distancing procedure affecting the supply of labour and agricultural inputs, smart agricultural technology such as precision agriculture and unmanned aerial vehicles (UAVs) can be used effectively to control agricultural fields.


COVID-19 Impact on the Digital Agriculture Market (COVID-19 Analysis)

COVID-19 Impact on Digital Agriculture Market (USD Billion)

Source: Press Release, Investor Relation Presentation, Annual Report, Expert Interview, and MarketsandMarkets Analysis

Figure13: Represents Fog computing architecture with layered approach, which inserts monitoring, preprocessing, storage, and security layers between physical and transport layers.[55]

Following COVID-19, the global digital agriculture market is expected to expand from USD 5.6 billion in 2020 to USD 6.2 billion in 2021, growing at a 9.9 percent compound annual growth rate. Demand for agricultural food products is increasing, consumer preferences are shifting toward higher standards of food safety and quality, and labor is scarce during COVID-19.

Farm mechanization and the creation of a digital agriculture infrastructure are expected to increase farmers' adoption of digital agriculture. COVID-19 is expected to have a positive effect on the market. Globally, labor shortages and supply chain disruptions are expected to drive an increase in demand for digital agriculture.

Precision farming is likely to grow in the long term following the COVID-19 outbreak, as precision farming enables crop monitoring when not physically present by the use of automation, reducing the need for human interaction, which is critical during these periods. This farming method entails the precise application of inputs in order to achieve higher average yields than conventional cultivation techniques. COVID-19, on the other hand, would impact the demand in the short term, and market growth would be slower in the first and second quarters of 2020 due to economic slowing and inflation.[55-61]

These activities save time and money by lowering the cost of fertilizer and chemical application and by reducing emissions caused by the use of chemicals. Additionally, they aid in the monitoring of soil and plant physiochemical conditions by placing sensors to measure electrical conductivity, nitrates, temperature, evapotranspiration, radiation, and leaf and soil moisture, in order to achieve the optimal conditions for plant development. These factors contribute to increased productivity with a small labor force during a pandemic situation with a labor shortage, ensuring a consistent supply of food and therefore food security.[52-58]

REFERENCES

[1] K. A. Kumar and K. Ramudu, “Precision agriculture with IoT and wireless sensor networks,” Precision Agriculture, vol. 7, no. 3, pp. 1255–1258, 2019.

[2] M. Mukherjee, L. Shu, R. V. Prasad, D. Wang, and G. P. Hancke, “Sleep scheduling for unbalanced energy harvesting in industrial wireless sensor networks,” IEEE Communications Magazine, vol. 57, no. 2, February 2019, pp. 108–115.

[3] J. Muangprathub, N. Boonnam, S. Kajornkasirat, N. Lekbangpong, A. Wanichsombat, and P. Nillaor, “IoT and agriculture data analysis for smart farms,” Comput. Electron. Agricult., vol. 156, no. 1, January 2019, pp. 467–474.

[4] Taiwanese authors: Wu-Chun Chung, Po-Chi Shih, Kuan-Chou Lai, Kuan-Ching Li, Che-Rung Lee, Jerry Chou, Ching-Hsien Hsu, and Yeh-Ching Chung. UniCloud: A Cloud Testbed for Collaborative Cloud Services, IEEE International Conference on Cloud Engineering (IC2E) Proceedings, 107–116 (2014).

[5] Lidong Zhang, Yongwei Wu, Ruini Xue, Tse-Chuan Hsu, Hongji Yang, and Yeh-Ching Chung, HybridFS - A Scalable and Balanced File System Framework with Multiple Distributed File Systems, To be published in the IEEE Computer Software and Applications Conference (COMPSAC) Proceedings (2017).

[6] Gregor Broll, Massimo Paolucci, and Matthias Wagner, Perci: Pervasive Service Interaction with the Internet of Things, Internet of Things Research Institute. (2009) IEEE Internet Computing, pp. 74–81.

[7] Sharief M.A. Oteafy and Hossam S. Hassanein, Towards a Global Internet of Things: Resource Re-utilization in Wireless Sensor Networks, IEEE International Conference on Computing, Networking, and Communications, 2012, pp. 617–622.
[8] Which third-party vendors and service providers do you use? Synergy.
[9] https://www.synoval.com/blogs/news/who-is-your-third-party-service-provider suppliers-and-providers
[10] Architecture for the Internet of Things (IoT)
[11] https://www.youtube.com/watch?v=FRxRT0DjE7A&t=260s http://www.youtube.com/watch?v=FRxRT0DjE7A&t=260s
[12] J. R. Rosell-Polo, F. A. Cheein, E. Gregorio, D. Andujar, L. Puigdomenech, J. Masip, and A. Escolà, ‘‘Advances in structured light sensors applications in precision agriculture and livestock farming," in Advances in Agronomy, vol. 133, no. 1, pp. 71–112, Jan. 2015.
[13] A. R. Frost, C. P. Schofield, S. A. Beaulah, T. T. Mottram, J. A. Lines, and C. M. Wathes, "A study of livestock control and the need for integrated systems,"' Comput. Electron. Agricult., vol. 17, no. 2, May 1997, pp. 139–159.
[14] D. Berckmans, "Automatic on-line control of livestock by precision livestock farming," in Livestock Production and Society, vol. 287. Wageningen Academic Publishers, Wageningen, The Netherlands, 2006.
[15] A. Boghossian, "Threats to precision agriculture "United States Department of Homeland Security Secur., Washington, DC, USA, Tech. Rep., 2018. Secur., Washington, DC, USA, Tech. Rep., 2018.
[16] Jahn, M. M. (2019). Cybersecurity Risks and Consequences of Smart Cities Agriculture and Food Systems.
[17] Agriculture and Food Systems. Date accessed: November 14, 2019. [Accessed online]. Agricultural Cyber Risk and Security: https://jahnresearchgroup.webhosting.cals.wisc.edu/wp-content/uploads/sites/223/2019/01/Agricultural-Cyber-Risk-and-Security.pdf
[18] (2019). Environmental Protection Agency of the United States. Accessed: 12 December 2015. [Accessed online]. https://www.epa.gov/agriculture/laws-and-regulations-that-apply-to-your-agricultural-operation-farm-activity
[19] (MAANAK GUPTA, 2020) Smart Farming Security and Privacy: Challenges and Opportunities
[20] N. Gruschka and M. Jensen, "Attack surfaces: A taxonomy for cloud service attacks," in Proc. IEEE 3rd Int. Conf. Cloud Comput., Jul. 2010, pp. 276–279.
[21] C. Kolias, G. Kambourakis, A. Stavrou, and J. Voas, "DDoS attacks in the Internet of Things: Mirai and other botnets," Computer, vol. 50, no. 7, pp. 80–84, 2017.
[22] M. Antonakakis, T. April, M. Bailey, M. Bernhard, E. Bursztein, J. Cochran, Z. Durumeric, J. A. Halderman, L. Invernizzi, and M. Kallitsis, "Understanding the Mirai botnet," in Proc. 26th USENIX Security Symposium (USENIX Security), 2017, pp. 1093–1110.
[23] M. M. Aung and Y. S. Chang, "Traceability in a food supply chain: Safety and quality perspectives," Food Control, vol. 39, no. 5, May 2014, pp. 172–184.
[24] M. M. Aung and Y. S. Chang, "Traceability in a food supply chain: Safety and consistency considerations," Food Control, vol. 39, no. 1, May 2014, pp. 172-184.
[25] K. Liang, L. Zhao, X. Chu, and H.-H. Chen (2017) A unified architecture for software-defined and virtualized radio access networks that incorporates fog computing. IEEE Network, 31(1), pp. 80–87.
[26] S. Clinch, J. Harkes, A. Friday, N. Davies, and M. Satyanarayan (2012) How close is too close? Recognize the role of cloudlets in facilitating smartphone users' display appropriation. In: IEEE International Conference on Pervasive Computing and Communications (PerCom), 2012 IEEE International Conference on. IEEE. pp. 122–127.
[27] T. Bouguera, J.-F. Diouris, J.-J. Chaillout, R. Jaouadi, and G. Andrieux, “Energy consumption model for LoRa and LoRaWAN sensor nodes,” Sensors, vol. 18, no. 7, p. 2104.
[28] M. Mozaffari, W. Saad, M. Bennis, and M. Debbah, "Mobile Internet of Things: Can Unmanned Aerial Vehicles Have an Energy-Efficient Mobile Architecture?" IEEE Global Communications Conference (GLOBECOM), Dec. 2016, pp. 1–6.
[29] R. Buyya and A. Dastjerdi, The Internet of Things: Fundamental Concepts and Paradigms, Morgan Kaufmann, #a
[30] [2] W. Shi and S. Dustdar, "The Promise of Edge Computing,"' Computer, vol. 49, no. 5, 2016, pp. 78–81.
[31] W. Shi and S. Dustdar, "The Promise of Edge Computing,"' Computer, vol. 49, no. 5, 2016, pp. 78–81.
[32] K. Dolui and S. K. Datta, "Comparing edge computing implementations: fog computing, cloudlet computing, and mobile edge computing," in Proc. Global Internet Things Summit (GIoTS), Jun. 2017, pp. 1–6.
[33] Y. Liu, J. E. Fieldsend, and G. Min, "A Fog Computing Framework: Architecture, Problems, and Optimization," IEEE Access, vol. 5, pp. 25445–25454, 2017. IEEE Access, vol. 5, pp. 25445–25454, 2017.
[34] OpenFogConsortium (http://www.openfog.org/) (2018). GlossaryofFogComputingTerms. Accessed: 10 July 2018. [Accessed online]. https://goo.gl/cS7un3
[35] IEEE Xplore Digital Library (http://xplore.ieee.org/). Accessed: 10 July 2018. [Accessed online]. Available at the following address: https://ieeexplore.ieee.org/Xplore/home.jsp
[36] American Computer Society's Digital Library. Accessed on 1 July 2018. [Accessed online]. Disponible à l'adresse suivante: https://dl.acm.org/
[37] H. H. Pang and K. L. Tan, "Authenticating query outcomes in edge computing," in Proceedings of the 20th International Conference on Data Engineering, Mar. 2004, pp. 560–571.
[38] R. Grieco, D. Malandrino, and V. Scarano, "SEcS: Scalable edge-computing services," in 2005 ACM Symposium on Applied Computing (SAC), New York, NY, USA, pp. 1709–1713.
[39] (2006). GooglePressCenter. Google. Accessed: 10 Feb 2021. [Accessed online].
[40] Available at the following link: https://www.google.com/press/podium/ses2006.html
[41] (2006). Website of Amazon Web Services. Accessed: 10 Feb 2021. [Accessed online]. https://goo.gl/gU82sF
[42] Hayes, B., "Cloud computing," ACM Communications, vol. 51, no. 7, july 2008, pp. 9–11.
[43] R. Buyya, C. S. Yeo, and S. Venugopal, "Market-oriented cloud computing: Vision, hype, and truth for providing it services as computing utilities," in Proc. 10th IEEE Int. Conf. High Perform. Comput. Commun., September 2008, pp. 5–13.
[44] K. Ashton, "That'InternetofThings'thing," RFIDJ., forthcoming. [15] R.A. Dolin, "Deployingthe'InternetofThings,"' in Proc. Int. Symp. Appl.SAINT, January 2006, pp. 219–223.
[45] "The Internet of Things," J. P. Conti Engineer, Commun., vol. 4, no. 6,
[46] Dec. 2006, pp. 20–25.

[47] F. Bonomi, R. Milito, J. Zhu, and S. Addepalli, "Fog computing and its applications".position in the Internet of Things," in Proceedings of the MCC Workshop on Mobile Computing, 1st Ed. Cloud Computing (MCC), 2012, New York, NY, USA, p. 13.
[48] [45] P. Mell and T. Grance, "The National Institute of Standards and Technology's concept of cloud computing," Technical Report, 2011.
[49] D. Leaf, F. Liu, J. Tong, J. Mao, R. Bohn, J. Messina, L. Badger, and F. Liu, "The National Institute of Standards and Technology's cloud computing reference architecture," National Institute of Standards and Technology, Special Publication, Technical Report, 2011.
[50] https://www.researchgate.net/publication/224230457 Embedded Security for Internet of Things Embedded Security for Internet of Things Embedded Security for Internet of Things Embedded Security for
[51] Schuttelaar Partners, https://schuttelaar-partners.com/news/2017/smart-farming-is-critical-for-agriculture's-future.
[52] Alexandre Pujol et al., “Metadata Collection on an Instant Messaging Server.” Academic Conferences International Limited, European Conference on Cyber Warfare and Security, June 2017, p. 741.
[53] https://www.dqindia.com/aggressive-growth-smart-farming-agri-tech-india/
[54] https://finance.yahoo.com/news/2019-114000282-india-precision-agriculture-market.html
[55] dtu.dk/orbit/files/199445663/08869772.pdf
[56] https://www.ijert.org/a-review-paper-on-iot-and-its-data-protocol-a-review-paper-on-iot-and-its-data-protocol
[57] ScienceDirect.com, https://www.sciencedirect.com/science/article/pii/S0308521X16303754.
[58] https://www.computerworld.com/article/2859496/are-you-aware-of-the-legislation-governing-personal-information-in-the-cloud.html
[59] https://www.coursehero.com/file/p15eik70/A-smart-farming-equipment-that-frequently-makes-use-of-global-navigation-satellite-systems-GNSS/
[60] https://dataprotectioncenter.com/cybercrime/what-is-a-supply-chain-attack-and-why-should-you-be-aware-of-third-party-providers/
[61] TutorialsPoint.com, http://www.tutorialspoint.com/uml/uml use case diagram.htm
[62] http://www.embedded-computing.com/guest-blogs/how-fog-computing-can-solve-the-internet-of-things-challenges
[63] Safety in fog computing: a study of existing applications.... 10.1186/s13677-017-0090-3 https://link.springer.com/article/10.1186/s13677-017-0090-3
[64] W. Z. Khan, M. Y. Aalsalem, M. K. Khan, and Q. Arshad, "Enabling customer confidence in IoT technology via a security and privacy model," in Proc. Adv. Multimedia Ubiquitous Engineering and FutureTech (MUE), Springer, 2016, pp. 111–117.
[65] International Telecommunication Union, International Telecommunication Union, Recommendation ITU-T Y.2060 Overview of the Internet of Things, paper, June 2012, Art. no. E 38086.
[66] Z. Abbas and W. Yoon, "A study of energy-saving mechanisms for the Internet of Things: Wireless networking considerations," Sensors, vol. 15, no. 10, pp. 24818–24847, 2015.
[67] P. Kamalinejad, C. Mahapatra, Z. Sheng, S. Mirabbasi, V. C. M. Leung, and Y. L. Guan, "Wireless energy harvesting for the Internet of Things," IEEE Communications Magazine, vol. 53, no. 6, June 2015, pp. 102–108.
[68] V. Adat and B. B. Gupta, "Internet of Things Security: Issues, Challenges, Taxonomy, and Architecture," Telecommun. Syst., vol. 67, no. 3, pp. 423–441, 2018.
[69] M. Conti, A. Dehghantanha, K. Franke, and S. Watson, "Internet of Things security and forensics: Challenges and Opportunities," Future Generation Computer Systems, vol. 78, no. 1, pp. 544–546, Jan. 2018.
[70] B. N. Silva, M. Khan, and K. Han, "Internet of Things: A Systematic Overview of Enabling Technology, Design, and Challenges," IETE Tech. Rev., vol. 35, no. 2, 2018, pp. 205–220.
[71] M. Noura, M. Atiquzzaman, and M. Gaedke, "Interoperability in the Internet of Things: Taxonomies and Unresolved Issues," Mobile Networks and Applications, vol. 24, no. 3, pp. 796–809, 2019.
[72] H. Li, G. Shou, Y. Hu, and Z. Guo, "Mobile edge computing: Progress and challenges," in Proc. 4th IEEE International Conference on Mobile Cloud Computing, Services, and Engineering (MobileCloud), Mar. 2016, pp. 83–84.
[73] I. Bouzarkouna, M. Sahnoun, N. Sghaier, D. Baudry, and C. Gout, ‘‘Problems confronting industrial fog computing implementation," in Proc. IEEE 6th Int. Conf. Future Internet Things Cloud (FiCloud), Aug. 2018, pp. 341–348.
[74] C. Mouradian, D. Naboulsi, S. Yangui, R. H. Glitho, M. J. Morrow, and P. A. Polakos, "A systematic study of fog computing: State-of-the-art and analysis challenges," IEEE Communications Surveys Tutorials, vol. 20, no. 1, pp. 416–464, 1st Quarter, 2018.