IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received February 11, 2020, accepted February 17, 2020, date of publication February 19, 2020, date of current version February 27, 2020.

Digital Object Identifier 10.1109/ACCESS.2020.2975142

Security and Privacy in Smart Farming: Challenges and Opportunities

MAANAK GUPTA[1], MAHMOUD ABDELSALAM[2], SAJAD KHORSANDROO[3], AND SUDIP MITTAL[4]

[1]Department of Computer Science, Tennessee Technological University, Cookeville, TN 38501, USA
[2]Department of Computer Science, Manhattan College, Riverdale, NY 10471, USA
[3]Department of Computer Science, North Carolina A&T State University, Greensboro, NC 27411, USA
[4]Department of Computer Science, University of North Carolina Wilmington, Wilmington, NC 28403, USA

Corresponding author: Maanak Gupta (mgupta@tntech.edu)

ABSTRACT Internet of Things (IoT) and smart computing technologies have revolutionized every sphere of 21st century humans. IoT technologies and the data driven services they offer were beyond imagination just a decade ago. Now, they surround us and influence a variety of domains such as automobile, smart home, healthcare, etc. In particular, the Agriculture and Farming industries have also embraced this technological intervention. 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. However, the use of IoT and smart communication technologies introduce a vast exposure to cybersecurity threats and vulnerabilities in smart farming environments. Such cyber attacks have the potential to disrupt the economies of countries that are widely dependent on agriculture. In this paper, 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.

INDEX TERMS Security, privacy, smart farming, precision agriculture, cloud computing, edge computing, cyber physical systems, IoT, artificial intelligence (AI), machine learning, layered architecture.

I. INTRODUCTION AND MOTIVATION

According to the United Nations (UN), the world population is expected to exceed 9 billion people by 2050, growing by almost a third of the current population [1], [2]. Such an increase in the population demands a boost of almost 70 percent in the food production rate, according to the Food and Agriculture Organization of the United Nations.[1] This rapidly growing population also introduces a variety of other problems such as increasing competition and exploitation of land, water and other natural resources. These issues present an urgent need to reduce the dependence of food system on our environment. Consequently, the need for an evolutionary agricultural paradigm to keep up with growing demand of food and crop production is necessary to guarantee a sustainable development [3].

Smart farming technologies[2] and precision agriculture[3] [4] are gaining more attraction for their potential to fulfill such an increasing demand and meet global food supply needs. Smart farming technologies involve integration of technology and data driven agriculture applications to increase crop yield and quality of food products. There are numerous smart farming use cases [5]–[7] present globally indicating the impact of this new paradigm of practicing agriculture. As an example, the use of remote sensors placed in the soil for measuring blueberry irrigation in Chile has reduced the volume of water used in farming by 70 percent [8]. In India, farm data has been used to predict and prevent crop diseases, which reduced the

The associate editor coordinating the review of this manuscript and approving it for publication was Noor Zaman.

[1]Food and Agriculture Organization of the United Nations. http://www.fao.org/home/en/

[2]https://www.microsoft.com/en-us/research/project/farmbeats-iot-agriculture/

[3]In the paper, we use the term smart farming and precision agriculture interchangeably.

risk associated with the failure of crop production [9]. Similar data driven approaches have helped fruit farmers in Slovenia effectively fight against pests.[4] 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 [10] 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. Although beneficial to the productivity of the industry, the use of heterogeneous, internet-connected devices has exposed potential cyber attacks and vulnerabilities in the agriculture sector. These attacks introduce the ability to remotely control and exploit on-field sensors and autonomous vehicles (tractors, aerial vehicles, etc). Potential agricultural attacks can create an unsafe and unproductive farming environment. For example, exploits that have the ability to destroy an entire field of standing grown crops, flood the farmlands, over spray pesticides using smart drones, etc. can cause unsafe consumption as well as economic deterioration. Such attacks in a large coordinated manner, also referred to as agro-terrorism [11], also have the potential of disrupting the economy of an agriculture-dependent nation. A report [12] released by the U.S. Department of Homeland Security extensively elaborates various cyber threat scenarios in precision agriculture, further emphasizing the need for research in this critical domain.

The Agriculture industry adds 6.4 percent of the world's economic production with a total of $5,084,800 million.[5] Agriculture, food, and related industries contributed $1.053 trillion to U.S. gross domestic product (GDP) in 2017.[6] At the same time, United State's farms contributed $132.8 billion of this sum which is almost 1 percent of GDP. Agriculture contributed 1.2 % to the European Union's (EU) GDP in 2017 whereas EU's agricultural industry added gross value of EUR 188.5 billion in 2017[7] at a record high. Out of 226 countries, nine countries have agriculture sector as the dominant sector in their economy. The U.S. food and agriculture system has a total economic impact of $7.06 trillion[8] and one-fourth of the overall jobs in the country are connected to it. Most countries globally export agricultural products. As a result, cyber vulnerabilities can have a significant impact on global food security. A sophisticated agro-terrorism attack on a (large) exporting country like the U.S. could harm the health of millions of consumers

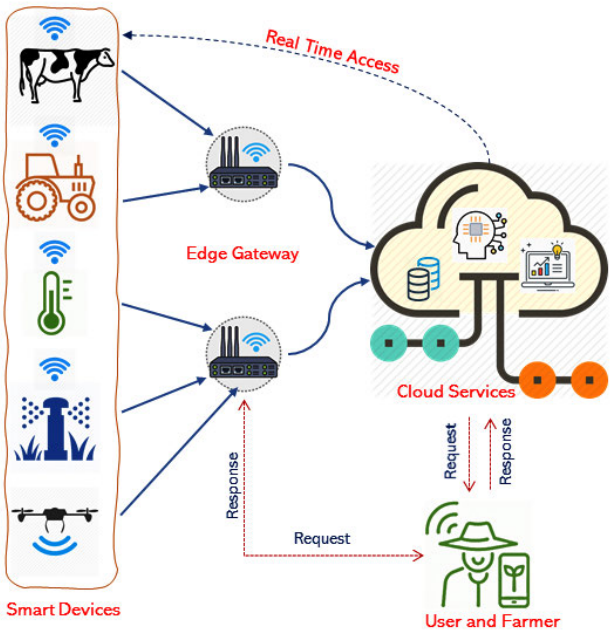

FIGURE 1. A model of end-to-end interaction between various stakeholders in smart farming.

world-wide. In addition, attacks could reduce confidence on domestic consumption and destroy the United State's status as a trusted food exporter. A report released in 2018 by the Council of Economic Advisors,[9] "The Cost of Malicious Cyber Activity to the U.S. Economy" suggests the agriculture sector as one of the 16 critical infrastructure sectors that are important to both the U.S. economy and national security for which cyber protection is particularly important. It also reported that the agriculture sector experienced 11 cyber incidents in 2016.

According to the World Health Organization,[10] 420,000 people die every year from food-related illnesses and 600 million people fall ill as a result of food contaminated with bacteria, viruses, toxins or chemicals. A cyber attack on the food ecosystem targeted at farms, transportation system, or food processing industrial control systems (ICSs) may increase these numbers exponentially. Other important industries like energy, financial or healthcare have understood the need for resilient infrastructure and have hardened their defenses. However, the food and agriculture industry is still a low hanging fruit for threat actors. Food Protection and Defense Institute (FPDI) at the University of Minnesota has discovered that food industry ICSs may be distinctly vulnerable to cyberattacks.[11] Food industry operations technology personnel, in particular, those responsible for operating and

[4]Lanner-America. https://www.lanner-america.com/blog/smart-farming-iot-5g-agriculture/

[5]http://statisticstimes.com/economy/countries-by-gdp-sector-composition.php

[6]https://www.ers.usda.gov/data-products/ag-and-food-statistics-charting-the-essentials/ag-and-food-sectors-and-the-economy

[7]https://ec.europa.eu/eurostat/statistics-explained/index.php/Performance_of_the_agricultural_sector

[8] https://feedingtheeconomy.com/

[9]https://www.whitehouse.gov/wp-content/uploads/2018/03/The-Cost-of-Malicious-Cyber-Activity-to-the-U.S.-Economy.pdf

[10]https://news.un.org/en/story/2019/06/1039901

[11]S. Streng, "Food Industry Cybersecurity Summit: Meeting Report," Food Protection and Defense Institute, Saint Paul, MN, May 2016.

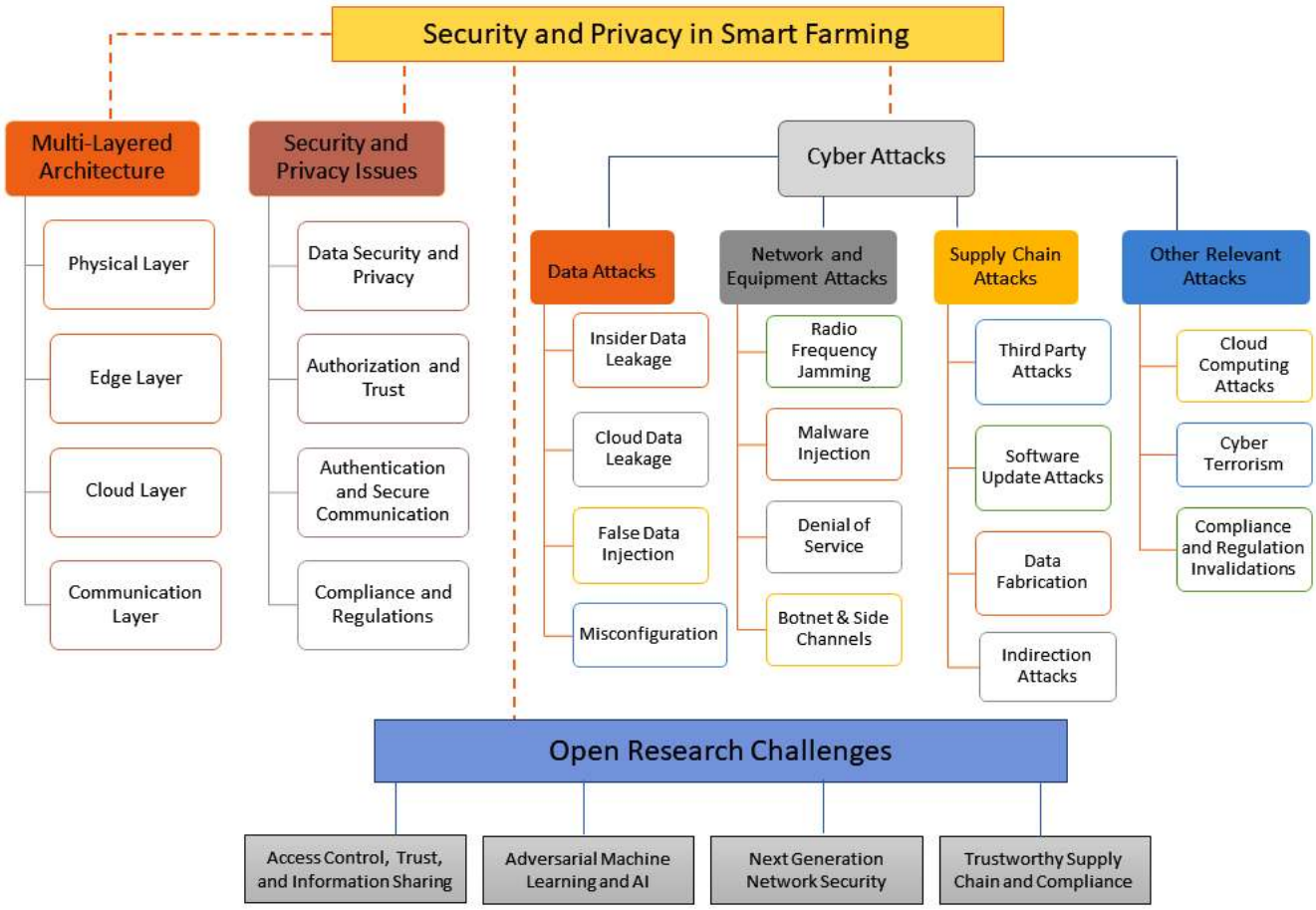

FIGURE 2. A roadmap of cybersecurity research and challenges in smart farming.

maintaining ICSs, are experts trained in food and production safety production and not in cybersecurity. This presents a huge gap between employing smart farm technology and securing it correctly and persistently. If not continuously monitored, cyber attacks on smart agriculture technologies can have grave implications on several stakeholders in the ecosystem. These groups include farmers, end consumers, food processing industries, agriculture co-operatives, livestock, government agencies and nations critically dependent on agriculture.

Figure 1, shows an end to end interaction among various entities involved in smart farming ecosystem. Physical sensors and livestock in the field generate data and receive command operations via user applications. These on-farm devices are connected to gateway supported edge nodes, which help enable in-farm device communication, filter sensor data and real time agronomy analytics. At the same time, data lakes in the cloud hold a large amount of data and information including but not limited to, environmental information (e.g. soil moisture level and fertility status), monitoring information (e.g. sensors and smart machinery status), energy management data, and other sensitive information. In terms of security and data privacy, it is needless to say that manipulation and leakage of such data, as well as the impairment of physical equipment and software systems, can induce serious consequences.

Extensive research on secure IoT devices [13]–[15], smart vehicles [16]–[19], drones [20], [21], edge cloud [22]–[24], wireless communication [25]–[27] is already available and might be extended to the smart farming ecosystem. However, most of the time, research is conducted on these technologies without consideration of the environment they are used. The dynamic smart farming environment, has unique characteristics such as farm equipment, labor sharing, and operational decisions, influenced by environmental conditions. Domain specific issues such as like location, user skill set, insider threats, generated data, need smart-farming-specific security mechanisms. The development of smart farm technologies therefore, demands further research before wide adoption in the community.

The current state of the art and our review (discussed in Section V) on smart farming, demands further research in security and privacy aspects of this evolving domain. As the research, on cybersecurity for smart farming is in its infancy, our objective in this review is to provide a holistic view of cybersecurity developments in smart farming. In this paper, we discuss current threats, analyze potential cybersecurity attacks, review the existing scattered security research, and

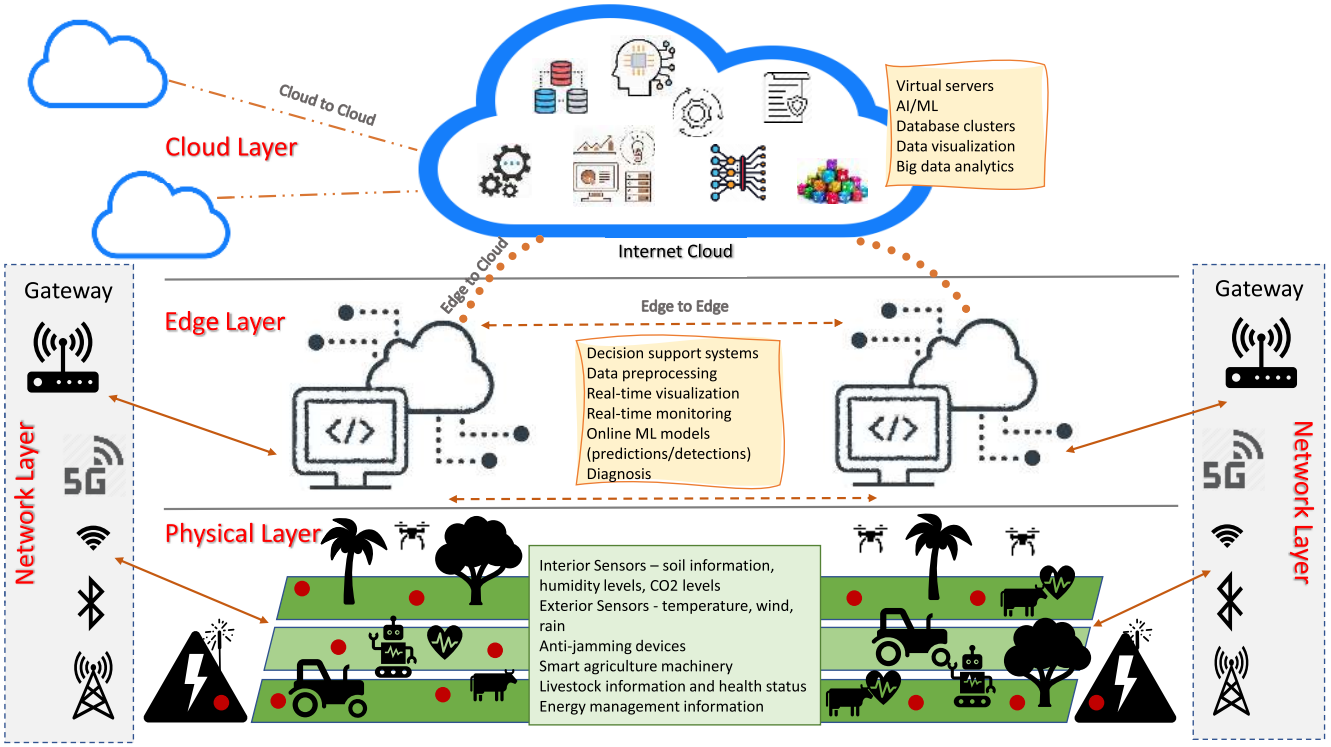

FIGURE 3. Multi layer smart farming architecture.

summarize open research challenges in the smart farming field as illustrated in Figure 2.

This paper has the following **key contributions**:

- It provides an overview of smart farming focused multi-layered architecture, highlighting multiple entry points and communication across layers.
- It identifies potential cybersecurity issues in smart farming and illustrates, scenario specific cyber attacks, which have been categorized into data, network, supply chain, and other common attacks.
- It presents an extensive evaluation of the current cybersecurity research, countermeasures in smart farming, and also enlists the focus, contributions and weaknesses of current research works.
- It provides a clear view of the open security research challenges in different areas including next generation network security, trustworthy supply chain and compliance, adversarial machine learning and AI, and access control, trust and information sharing.

The remainder of this paper is as follows. Multi-layered architecture for smart farming is discussed in Section II. Section III elaborates security and privacy issues, whereas Section IV discusses different attacks on the smart farming ecosystem including the supply chain side. Existing research and state of the art in smart farming security is discussed in Section V. Section VI highlights open research challenges and possible approaches to solutions. Finally, Section VII draws conclusion to this research paper.

II. SMART FARMING LANDSCAPE & ARCHITECTURE

Figure 3, depicts a multi layer architecture for the smart farming ecosystem. The proposed architecture adapts and extends widely discussed IoT and Cyber Physical System (CPS) multi-layer architectures [28]–[31]. These architectures recognize the use of cloud and edge services, and the infinite capabilities provided by them to fully harness the data generated from smart devices at the physical layer [32]–[37]. Our smart farming architecture, also reflects different user applications which can be envisioned at various layers. It also considers, vast amounts of data collected at edge or cloud layers, and highlights the need for various multi-cloud or edge-cloud scenarios. Overall the architecture consists of four layers: Physical layer, Edge layer, Cloud layer, and Network Communication layer. The latter spans across all three previous layers and connect them.

A. PHYSICAL LAYER

The bottom layer in the architecture comprises of real physical sensors and gateway devices which are spread across agriculture farms or in greenhouse buildings. These devices include drones flying in the air, autonomous tractors, sensors embedded in livestock, or hub devices installed to provide communication among smart objects or with a central cloud. These devices are responsible for data sensing and based on the information gathered, help in actuating other devices to realise various smart farming use cases. They collect real time information about weather conditions, soil moisture level,

or cattle's body temperature, which can be sent to the edge or cloud supported intelligent decision making systems to provide recommendations and enable automation. For example, data gathered from soil moisture sensing device in the field, after getting processed in the edge or cloud, can help in determining the amount of water needed at the farm, optimize irrigation schedule and offers a convenient experience to the end farmers.

B. EDGE LAYER

This layer is near to the end-users and end-devices for local real-time computations and decisions. It reduces the computation load off the centralized cloud layer and also the network load. Edge computing layer consists of multiple edge nodes. Each node represents a gateway that include services such as: data capturing, security monitoring and detection, prediction and real-time decision support. Data capturing services include, data aggregation, filtering, encrypting and encoding of real-time data streams.

Prediction services usually rely on machine learning models trained on the central cloud and deployed on the edge layer. They are used to predict and/or categorize certain events related to plant or livestock such as, prediction of crop yield, categorization of plants or livestock health, predictions about the amount of fertilizer and water needed for a patch of land, so as to maximize yield, or estimating soil erosion.

Security monitoring and detection mechanisms can be deployed for real-time monitoring of anomalous events and classifying these events as malicious or benign. This includes services like, anomaly detection and device failures prediction.

C. CLOUD LAYER

Precision Agriculture (PA) and cloud computing paradigms offer advances to enhance PA connectivity. The cloud layer is generally virtualized in data centers and communicates with the other layers using the Internet. Generally, these cloud layer platforms follow the Platform as a Service (PaaS) architecture model where the users can focus on running applications and importing their data.

The PaaS provider runs and maintains a data broker that collects data being pushed in from the edge layer and saves these records in a Distributed File System (DFS). This stored data is used by analytic software to mine knowledge. This data analytics component computes insights and these are pushed to the end user through a client application running on the users' machine.

Popular farm equipment manufacturers like, John Deere,[12] Farmers Business Network,[13] etc. have created several cloud based products that help users monitor various sensors and vehicles used on a farm. These PaaS systems generally run on popular cloud computing platforms like Amazon Web Services,[14] Google Cloud,[15] etc. The way these farming PaaS systems are built using these popular cloud computing platforms also introduce various security challenges in smart farming ecosystem.

D. NETWORK COMMUNICATION LAYER

The common theme for most, if not all, current technologies is ''connectivity''. With a growing need for a boundary-less Internet, the idea of a network of smart devices has become a reality. This concept, known as the Internet of Things (IoT), allows connected devices to be monitored, controlled, and shared data among each other. This data can be analyzed and used by multiple applications. In smart farming, as shown in Figure 3, the network layer not only facilitates edge and physical layer connectivity, but also provides an interface for them to interact with the cloud layer. From exchanging soil temperature through a peer-to-peer sensor communication system, to sending farm monitoring data to the cloud data stores through high speed mobile networks such as 5G [38], or updating the farmer about corp quality via a wireless adhoc topology [39], network layer offers a means of communication to bind all other layers.

Network layer has two main responsibilities in a smart farming system. Firstly, there are diverse set of heterogeneous devices in every layers of a smart farming system. The network layer provides a secure and efficient network stack where, wire, wireless and mobile sub-networks can communicate in a compatible and cross-layer manner. The second responsibility of the layer is to preserve connectivity and therefore, increase availability. From bigdata processing systems used to analyze collected data to individual sensors that collect information from the field, this layer is needed for system-wide cyber communication.

Real World Smart Farming Use Cases: The proposed smart farming architecture is constructed based on multiple literature and real world smart farming use cases. It can be viewed as a general smart farming architecture that satisfies most of the use cases. However, it should be noted that not all use cases will include all four layers as proposed in the architecture.

Blackhills Farm in New Zealand, a 400-hectare property with over 2000 cattle and 800 sheep, has adopted the use of SCADAfarm[16] system which allows the owners to remotely monitor water and energy consumption, location of irrigators, soil moisture measurements and real-time weather information. The farm uses Schneider Electrics's EcoStuxture IoT architecture[17] which corresponds to our physical layer and sensors. It also utilizes Microsoft Azure[18] IoT suite with communication provided by the Vodafone New Zealand cellular

[12] John Deere Operations Center. https://www.deere.com/en/technology-products/precision-ag-technology/data-management/operations-center/

[13] Farmer's Business Network. https://www.fbn.com/

[14] Amazon Web Services. https://aws.amazon.com/

[15] Google Cloud. https://cloud.google.com/

[16] SCADAfarm. https://www.scadafarm.com

[17] EcoStuxture IoT architecture. https://www.se.com/us/en/work/campaign/innovation/overview.jsp

[18] https://azure.microsoft.com/en-us/overview/iot/

network which corresponds to the cloud and network layer in out framework.

Similarly, a 7,000-acre farm at Beltsville Area Research Center, was developed by the United States Department of Agriculture (USDA) to act as a testbed for smart farming technologies. The farm was equipped with a physical layer including sensors, drones and IoT-enabled farm equipment for a public-private program called Farmbeats [5]. The farm adopts a two-layer hybrid network: a layer based on TV White Spaces [40] technology for connectivity over long range which connects the farmer's home Internet connection to IoT base stations on the farm, and a layer based on Wi-Fi technology which connects smart sensors to the IoT base stations. Such IoT base stations (gateways) are equivalent to the edge cloud layer (Figure 3) in our proposed general architecture. Additionally, the data collected at the IoT stations are pushed to the cloud layer which employs AI algorithms for data analysis.

Another usecase is a revolutionary step towards smart crop health monitoring. A group of researchers[19] along with local farmers are developing a distributed airborne monitoring system to detect possible zones of crop damage or nutrient deficiency at a 492-acre farm in in North Carolina, United States. In order to accommodate rapidly-growing food demands and increase the quality and quantity of agricultural production, it is necessary to improve farming management practices and technological developments in agricultural fields. Accordingly, unlike traditional crop management methods that use farmers or ground vehicles for assessing crop health status, this collaborative smart farming project is using autonomous technology to perform aerial monitoring of agricultural fields to save time and money, while preventing damage to crops. In this project, a group of drones which monitor the field are working in the physical layer, as depicted in Figure 3. Drones communicate with each other through network layer, using which they also send collected data and images to land processing bases (i.e. the edge layer in our proposed architecture) for initial data cleaning and pre-processing. Finally, pre-processed data is sent to the cloud layer for storing and knowledge extraction functionalities.

III. SECURITY & PRIVACY ISSUES

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 cyber attacks. In this section, we will elaborate these issues in detail followed by attacks in the following section.

A. 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, if such information is used by competitors or hostile actors. On a larger scale, aggregating important agricultural information on a particular country is also a potential threat. As such data security and privacy is a very important requirement and one of the primary objectives to ensure the reliable operation in a smart farming ecosystem.

Data on the Edge: Smart farms leverage Internet of Things (IoT), state-of-the-art communications (e.g., 5G), and artificial intelligence. Such systems mostly require fast response times, than those of a traditional model in which data is transmitted to a centralized data center (e.g., cloud) for processing and results are returned to a user. As such, the need of edge cloud is on the rise. Although moving data processing and analytics to the edge enhances agility and efficiency, to say the least, it also imposes huge security risks due to the increased attack surface primarily because of the highly diverse use of IoT devices which are usually not built with security in mind. This gives attackers an easy entry point to the network since remote access to the edge layer, in most cases, is essential. Additionally, finding the IP addresses of edge endpoints become an easy task especially when considering websites like Shodan,[20] a search engine for all IoT connected devices. Beside directly compromising IoT devices or edge endpoints to gain access to the smart farm network, an indirect attack to compromise third parties is also a potential risk. As an example, smart farms often use third party agronomy analytics to analyze the collected data which can be used in many research areas such as plant biology and genetics, agriculture economy, supply forecasts, and disease predictions. Those parties might be given direct access to smart farm data on the edge for real-time analytics. An attacker might phish for such third parties, compromise their systems and inject malicious software to redirect the data sent to external servers for data theft. Such attacks are very hard to detect, since attackers are using legitimate stolen third party credentials.

B. 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 (MQTT[21]),

[19] https://ncatresearch.org/2018/10/30/n-c-at-uses-drones-to-bring-smart-agriculture-to-the-aggie-farm/

[20] Shodan. https://www.shodan.io

[21] MQTT. http://mqtt.org/

Constrained Application Protocol (CoAP[22]) or other IoT communication protocols. In either case, it is essential to ensure that the messages are sent from a trusted authorized entity, rather from a malicious adversary. This exchange of information, like moisture level of soil, information about crop yield, cost of fertilizer, or sensitive data about the livestock like health, current location, breeding decision information and other farm related private data sent to the cloud or to a third-party application must be authorized by the owner of the field or a concerned party.

Livestock are important part of agriculture, and a big component of a farmer's income. Sensors can be embedded in the cattle [41]–[43] which can monitor their health and can be used to remotely inject medicines or enable preventive actions from a doctor. Even in case of livestock purchase, buyer can be given temporary access to the data of an animal they are interested in, which can help them analyse it before purchase. As these animals are kept in monitored environments, remotely controlling the temperature or making adverse conditions in barn can affect the yield of animals, and can also result in epidemics and widespread disease.

Over the air (OTA) updates for the equipment's firmware must be from a trusted party, a bad software patch received for a critical agriculture equipment can curtail a farmer from using it at the needed time of harvesting and planting. Cross cloud and multi cloud trust models [44], [45] are needed when entities associated at different cloud providers interact and access data remotely. In case of a mechanic trying to diagnose an engine of an autonomous tractor, or a doctor trying to access data of a cattle located in a private cloud, trust levels need to be established so as to enable such access. Several access control models have been proposed for IoT [46]–[58] like systems, however their feasability in dynamic smart farming is still to be investigated.

Proper authorization is needed for a farmer to issue a command, to a smart water sprinkler, or to fetch the latest readings from a soil moisture sensor. Farm rivalry can exploit such connectivity to the sensors, and may flood a farmer's field, or make it parched. Usually in farms, labor is hired on a temporary basis mostly at the time of harvesting and sowing, therefore, temporary access to smart equipment can be delegated to on field workers for non-critical operations. It may be the case that a critical operation, like running an autonomous tractor on the field, or flying a drone over the field to spray pesticides may need multi level authorization.

C. 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 (PKI) authentication mechanisms cannot be considered as feasible solutions.

Alternatively, secure lightweight multi-factor authentication protocols which are offered as a service [13], [59] are more realistic solutions in a smart farming network environment. In fact, an intermediary Certifying Authority (CA) can facilitate the authentication of a connecting device [60]. Such authentication mechanisms do not consume devices' limited resources for authentication processing, but also unauthorized devices will be prevented from connecting and accessing the network in an efficient way [61]. Moreover, devices may sometime join or leave different layers of a smart farming ecosystem. This entails dynamic authenticated mechanisms that apply authentication on demand to ensure that only legitimate devices are allowed to have access to different services spanning over different layers.

Providing end to end secure communication in a smart farming setting requires securing the communication between devices in a particular layer and also securing the inter-layer communication [62]. While cryptography-based solutions prove their effectiveness in securing both intra-layer and inter-layer communications, employing them on constrained IoT devices is a big concern. There are, however, limited attempts to apply lightweight cryptography solutions to a smart farming ecosystem [14]. Additionally, quantum-based cryptography for a secure end to end communication for IoT devices is under active investigation [63] as a futuristic solution. However, the feasibility of such solutions have not been evaluated in real world scenarios.

D. COMPLIANCE AND REGULATIONS

Smart farming and precision agriculture raises various legal issues, which remain partially unanswered. The following are some of the major issues in this area.

1) CONTRACTS AND AGREEMENTS

A smart farm involves different parties like the farmers, the cloud service providers, the networking infrastructure providers, to name a few (See Section II). These different parties need to negotiate and agree on various parts of contracts [12], [64]. These contracts include data privacy, security and intellectual property protection clauses. Data protection is essential for the development of smart farms and is a major part of these contracts. Such contracts between interested parties are crucial to protect the value and confidentiality of the data as an important asset. Farmers who use smart farming tools also need to negotiate in advance finer elements of these contracts. For example, which party shall be responsible in case data processing and analysis lead to wrong decisions affecting different downstream tasks in the pipeline. Another important contractual element example is the decision involving use of self-driving tractors, which are subject to the set of obligations applicable to self-driving cars. In this scenario, strong compensation and limitation of liability clauses may help the farmers.

[22]COAP. https://coap.technology/

2) DATA SECURITY AND PRIVACY

Farmers who deploy smart infrastructure fear that their data might be stolen by competitors or be publicly released. Hence, data security is crucial and agreements with technology providers should include specific clauses. Although most smart farming techniques process non-personal data, linking of such information to a particular personally identifiable information (PII) poses serious concerns [12], [64]. For example, data of livestock directly referring to their owner; crops conditions linked to farmers' personal details. In this case, privacy clauses should be included to prohibit personal data processing to a certain degree. Further issues may arise when smart farming equipment, such as drones or tractors, have the functionality to monitor their users [12], [64].

3) INTELLECTUAL PROPERTY (IP)

An important question from a compliance perspective is who owns the data collected on a smart farm. This is specially important as data privacy laws cannot solve this issue. As per the current regulatory setup, data itself cannot be protected, however copyright provisions can be utilized to achieve high level of safeguards. Most farmers include IP protection clauses [64] in contracts that they create with smart farming technology providers [12].

4) REGULATORY

Agriculture and livestock production is a highly regulated industry. Various countries across the globe have many laws, regulations, and supervisory authorities [65]–[67]. These touch upon specific compliance requirements for producing and selling of products. Such compliance can be achieved easier by using smart farming technology that help farmers and regulators track, audit, and inspect every step of the production pipeline.

5) CYBER INSURANCE

Cyber Insurance allows victims to protect themselves from various cyber risks. However, cyber insurance policies in agriculture have lagged in the coverage of cyber incidents and events. Most of the current available agriculture based cyber insurances are very ambiguous and limited in their coverage [64].

IV. SMART FARMING ECOSYSTEM CYBER Attacks

This section elaborates possible cyber attacks in smart farming ecosystem. We have categorized attacks into four different classes as shown in Figure 4. We have discussed data specific and network specific attacks orchestrated on smart farms including IoT based farming sensors. We have also explored cyber attacks from the supply chain side to highlight the vulnerabilities as more and more systems get connected to the internet and generating sensitive data.

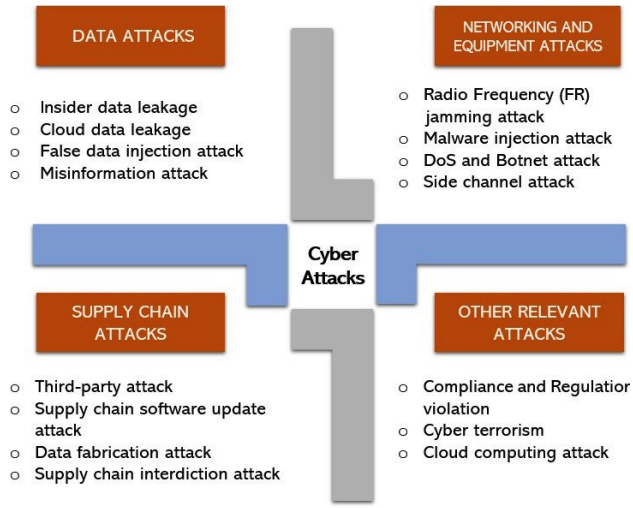

FIGURE 4. Smart farming ecosystem cyber attacks.

A. DATA ATTACKS

1) INSIDER DATA LEAKAGE

Farmers fear leakage of confidential data the most among other threats as it can be used against them in the commodity market. An insider (like a disgruntled employee) can leak such data to intentionally cause harm or sell data for money. For example, a former engineer at Allen and Hoshall was able to access the company's data over a period of two years.[23] Data this employee accessed included engineering schematic, project proposals, and marketing information which had an estimated value of $500,000.

2) CLOUD DATA LEAKAGE

Smart farming data is very sensitive and can reveal a lot of confidential agriculture and economic information about the entire country. Cloud data centers are distributed across the world and, in some instances, virtual machines might be placed in data centers located in different countries. Data might be less secure if it is stored in data centers in other countries. These countries could place less strict security requirements on companies. Additionally, their governments might also intercept or collect that data stored on servers within their own jurisdictions. For these reasons, countries have started adding laws for sensitive data localization. For instance, China has placed a new cybersecurity law[24] into effect in 2017 stating, among other things, that personal data must be stored on domestic servers. As such, companies like Microsoft, Google and Amazon started taking steps to transfer control of Chinese data to Chinese firms.

3) FALSE DATA INJECTION ATTACK

In this attack, an attacker attempts to change/falsify data that contributes to important real-time decisions, with the

[23] Department of Justice. https://www.justice.gov/opa/pr/tennessee-man-sentenced-unauthorized-access-former-employers-networks

[24] China Internet Security Law. https://en.wikipedia.org/wiki/China_Internet_Security_Law

assumption that adversary has the knowledge of the system and its configuration. For example, injecting false information about the soil moisture level will result in over watering and, in turn, damaging the crops.

4) MISINFORMATION ATTACK

In this attack, the aim is to endanger data integrity. An attacker may release false data about a smart farm claiming the outbreak of a disease in crops or livestock. Such false data reports mimic the form of an actual report released by the targeted smart farm. As a result, it will take a lot of time, effort and money to prove that the released report is false.

B. NETWORKING AND EQUIPMENT ATTACKS

1) RADIO FREQUENCY (FR) JAMMING ATTACK

In many cases, smart farming equipment rely on radio frequency communication, like cellular or satellite networks. A smart farming equipment often use global navigation satellite systems (GNSS) to improve efficiency with products and techniques such as path planning, auto steering, seeding and spray rates. GNSS is achieved by combining GPS with real time kinematics (RTK) technology to enhance the precision of real-time position data. Attackers may jam GNSS for malicious purpose by deploying many distributed low power jammers to disrupt GNSS over wide areas and, in turn, prevent smart farming equipment from functioning properly.

2) MALWARE INJECTION ATTACK

One of the most prevalent threats to smart farming is malware injection attack [68], where an attacker injects a malware into a connected smart device. Malware is a very common threat in large scale systems since, in most cases, it acts and propagates through the system automatically, hence making it a very attractive target to attackers. Precision agriculture is being adopted widely, meaning that more farms are connected to the internet. Typically, most of these farm deployments use similar software components (e.g., usage of LoRa[25] and ZigBee[26]). As a result, a malware that infects a particular smart farm will most likely infect other farms with similar deployments. The damage caused by malware comes in many shapes and types. Malware can steal information about the consumption of agricultural materials, purchase information of fruits, vegetables and livestock, data about agricultural machinery etc. It can also recruit smart devices as part of a botnet which will be used for committing malicious acts controlled by an attacker. Further, malware can hinder the functions of physical smart equipment which, in turn, can have a devastating effect on a particular crop harvest or farm area.

3) DENIAL OF SERVICE ATTACK

IoT devices used in smart farming environments can always be used to launch large scale denial of service (DoS) attacks [69] similar to what happened in 2016 using Mirai botnet [70]. In that occasion, an army of dummy CCTVs was exploited to launch one of the biggest DoS attacks that happened recently. There are usually a large number of inter-connected nodes and groups in a farm, and thus, similar type of attacks are possible in context of smart farming. These attacks not only can disrupt normal functions of different modules in an individual farm but also can be leveraged to interrupt legitimate cyber services in other domains.

4) BOTNET

With IoT everything is capable of getting connected to the internet. In smart farming ecosystem, there are many IoT related devices at each architectural layer. These devices are prone to attacks and can then be controlled by a central malicious system. This forms a so called 'Botnet of Things' [71]. A zombie army of infected farm IoT devices [72] can easily be used to infect many other networks through different mediums and hence a smart farm may turn out to be an internet of vulnerabilities for cyber criminals. Smart farm devices are not built with security as a concern and even if they do, users usually neglect the basic steps of setting adequate cybersecurity defense mechanisms.

5) SIDE CHANNEL ATTACK

Attacks which have their roots in gaining information from how a system is implemented rather than what weakness exists in the system implementation are called side channel attacks. Smart farming is one of the IoT use case and hence it inherits some common IoT vulnerabilities including side channel attacks [73]. In such attacks, there are different channels which can be exploited by attackers. In timing channel attacks, for example, computation time along with cache miss and cache hit timing patterns are among those attacks vectors which can be exploited by adversaries. Hardware glitching in forms of voltage fluctuations and variances in system clock period during execution tasks are other possible attack channels. Other channels for launching a successful attack are power consumption patterns, possible electromagnetic leaks or even sound and acoustic channels.

C. SUPPLY CHAIN ATTACKS

The entire agriculture ecosystem and the notion of 'farm to plate' involves several entities which work in tandem to provide quality food to the end consumer in a just-in time environment. This supply chain system [74] starts from the farm, which produces raw material that, in turn, is stored and processed by the food industry. The processed food is packed and sent to distribution retailer from where the end customer purchases processed goods. With IoT technology at each stage of the supply chain, it introduces potential cybersecurity threats since a security breach in just-in-time distribution system could also have a serious cascading effects on the entire supply chain. The massive scale of attacks like WannaCry[27] ransomware, and the recent spate of ransomwares

[25] https://lora-alliance.org/about-lorawan
[26] https://zigbeealliance.org/
[27] WannaCry Ransomware. https://www.symantec.com/blogs/threat-intelligence/wannacry-ransomware-attack

in cities[28] across the US, suggest that even a breach or data freeze at a single inter-dependent entity will be enough to disrupt the whole chain and possibly the economy of a country.

An attack on the agriculture equipment and fertilizer provider companies could potentially disable critical connected machinery needed at a prime time. It could manipulate the amount of nutrients in the fertilizers [64] which could seriously destroy the crops rather than nourishing them. The smart devices can be infected by malware which are controlled and commanded remotely. In such a scenario, large scale attacks can be orchestrated on all the smart farms utilizing those compromised machinery resulting in massive disruption in the sector. Needless to say that the suppliers of such machinery might loose trust and confidence of their customers. Such smart machinery needs dynamic calibration to determine the distance at which seeds need to be planted or the amount of fertilizers to be sprayed based on historical crop data. This calibration related information is uploaded in the machine software over-the-air (OTA), which suggests that deliberate uploading of false information to the machine software can have larger scale impact.

US Foods[29] has more than 250,000 customers which purchase supplies, will be affected badly if US Foods IT infrastructure is hit by a ransomware or a cyber attack disrupting its computer assisted facility and impacting critical processes. Temperature and conditions under which the produce is transferred is an important factor to maintain the freshness of the product. Smart monitors ensure that products are processed and packed at appropriate temperatures. Adversaries can manipulate these sensor readings or issue a command to change the temperature that could result in inappropriate temperature conditions for produce, which can impact the end consumers as well as the entire supply chain. These attacks are not limited to direct stakeholders, but for example, contaminated water from a compromised water treatment facility used in irrigation can destroy the whole crop field. Even attacks on smart grid due to sudden surge in demand and grid overloading can result in blackout which in-turn can spoil the stored produce in large storage houses, inducing huge losses to the supplier. Blockchain[30] based solutions have been proposed to ensure the provenance of the food products in the chain, which offers transparency and assure quality of the food. However, the entire cost to use this system will not be clear unless widely adopted [75].

Smart farming goes beyond agriculture where livestock sector is also considered an important part. An attack on this sector can also have massive disruptions, where a malicious actor can publish false data about a disease outbreaks or unapproved genetic modifications of crops. Similarly, sensors and smart devices in the buildings where these livestock are kept can be attacked or altered to change the temperature, which can put to harm the entire livestock on the farm. Also, for livestock feed products, if an IT system monitoring the ingredients of the feed is compromised, it can potentially lead to wide-spread contamination in livestock which can easily reach humans as well.

D. OTHER RELEVANT ATTACKS

1) COMPLIANCE AND REGULATION

Food production and farming are a highly regulated industry with different countries having multiple national agencies monitoring food production. In the United States, Environment Protection Agency [65] and the Department of Agriculture [66] enforce various regulations and industry standards. In the European Union, Department of Agriculture and Rural Development [67] undertakes this responsibility with similar authorities in other countries. These federal authorities issue compliance directives to ensure quality food production. With the advent of smart farming technology these agencies are relying more and more on data produced by farm based sensors.

An adversary attacking a smart farm can specifically inject false data that will then impact various compliance certification processes. This certification process if invalidated, can impact a nation's food supply, affect crop price, etc. The complex smart farming ecosystem, creates a broad attack surface that needs to be protected to ensure data integrity.

2) CYBER TERRORISM

The increased use of digital interconnected system in agriculture sector brings new opportunities for terrorists to attack places that previously were too remote or difficult to strike. Cyber terrorism is a relatively low-cost venture with high payoff potential, making the risks of agro-terrorism too large to ignore. Therefore, it is important to find solutions that guarantee trust and transparency within smart farming concept, as well as protect critical resources.

3) CLOUD COMPUTING ATTACKS

Cloud is a very diverse, decentralized, heterogeneous and powerful ecosystem. The enormous amount of distributed resources make the cloud a hard target. However, with the introduction of new cloud concepts (e.g., on-demand services, auto-scaling, and self provisioning), attackers have used such resources in their favor and, in turn, cloud has become one of the most desirable targets to attacker. For example, with the introduction of auto-scaling in cloud, a large part of the virtual machines hosted on cloud are similarly configured. If one of the virtual machines is vulnerable, it is highly likely that all auto-scaled virtual machines are vulnerable as well. As such, a malware that infected one virtual machine can propagate to other virtual machines quickly.

The infected machines can be employed as a part of global botnets which, consequently, can be used to launch a large scale distribute DoS (DDoS) attacks enough to hinder the functionality of cloud. For example, in 2018, a large scale DDoS attack was launched on github resulting in a record-breaking sudden traffic increase to 1.35 terabits

[28] 22 Texas Towns Hit With Ransomware Attack In 'New Front' Of Cyberassault. https://www.npr.org/2019/08/20/752695554/23-texas-towns-hit-with-ransomware-attack-in-new-front-of-cyberassault

[29] U.S. Foods. https://www.usfoods.com/

[30] https://www.blockchain.com/

per second. Inevitably, DDoS attacks are becoming more frequent, more powerful and more sophisticated. A large scale DDoS attack with an overwhelming number of requests, packets or messages can deny services to smart farms, thereby paralyzing the brain of smart farms. Further, DDoS attacks might not be specifically targeting smart farms' virtual machines. Even though, an attack might be directed at a different target, if virtual machines used by smart farms are on the save physical server, it will naturally block off other's traffic as well.

V. EXISTING RESEARCH

Table 1 summarizes state-of-the-art research, challenges and contributions with respect to security and privacy issues in smart farming. We have categorized the literature into different subsections based on the focus areas they address.

A. 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 U.S. Department for Homeland Security released a report [12] which emphasizes the importance of precision agriculture (PA) and associated cybersecurity threat and potential vulnerabilities. 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. Another promising work [76] highlights the vulnerabilities and risks due to introduction of technologies in the field of precision agriculture. This thesis work illustrates data collection and related empirical study, however falls short of security solutions in the domain.

The work from Jahn [64] discuss implications of using smart devices in the agriculture sector. The authors make strong argument about how the lack of a cyber insurance framework is going to have a big impact on various agribusinesses. They also highlight the fact that a regulatory response is needed to protect the interests of farmers who adopt the use of smart devices. Barreto and Amaral [77] use empirical methodology based on the analysis of information and experiences collected in the Internet Security Alliance,[31] the European Cyber Security Organization[32] and the National Institute of Standards and Technology[33] to highlight security challenges in smart farming. Some major threats discussed include security and privacy issues, social engineering, denial of service, cyber-espionage agroterrorism, ransomware etc. 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.

Peer to Peer (P2P) is a network paradigm which has use cases in smart farming communication. The device authentication methods in this type of communication, however, rely heavily on public key infrastructure. Although the system is trustworthy, it puts unnecessary computation load on resource constrained smart farm IoT devices participating in a secure P2P communication. Accordingly, authors in [78] proposed a lightweight device authentication solution in which session keys and public keys are combined to expedite the encryption/decryption tasks. It results in a fast and light-weight authentication solution which is a good fit for smart farming communication purposes. Additionally, West [79] introduced a framework to understand vulnerabilities in emerging technologies and the use of such technologies in a smart-farming-specific environment. The framework goal is to quantify the degree to which the use of smart farming new technologies are vulnerable to cyber-attacks. It uses the common vulnerability scoring system (CVSS) for the threat prediction model assessment. The work shows the trade-offs between technology maturity and adaptation in the smart farming environment which can lead to system compromise. The approach in the paper uses three parameters: basic parameters, temporal parameters and environmental parameters for constructing a CVSS score. Basic parameters indicate the intrinsic and severity of a vulnerability, whereas temporal parameters indicate how a vulnerability might change and affect the system over time due to technical changes. Environmental parameters reflect the specifications of a vulnerability present in a smart-farming-specific environment. Although CVSS score has become a standard in the industry for understanding the severity of vulnerabilities and prioritizing their patches, it has some shortcomings. Smart farming is a diverse environment with many connected devices and systems. CVSS score deals with individual vulnerabilities and fails to accurately capture impact of connections within the entire system.

B. BLOCKCHAIN RELATED RESEARCH

Recently, the usefulness of blockchain in domains other than cryptocurrency and financial transactions has been acknowledged [93]–[95]. Agriculture and food supply chain is one of the domains in which blockchain technology has shown its capabilities. Accordingly, the authors in [81] 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. Lin *et al.* [80] 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,

[31] ISA. https://isalliance.org/
[32] ECSO. https://ecs-org.eu/
[33] NIST. https://www.nist.gov/

TABLE 1. Projects and research addressing cybersecurity in smart farming.

Paper Title	Focus/Objective	Contribution	Limitation
Cyber Attacks, Threats and Proposed Solutions			
Threats to Precision Agriculture [12]	Identifies security threats, vulnerabilities, and threat scenarios in smart agriculture, crop and livestock.	• Uncovers threats using CIA model of information security. • Defines precision agriculture technologies. • Proposes security best practices.	• Lacks distinction among threats in CPS and precision agriculture. • Limited and abstract cybersecurity solutions.
Cyber Risk and Security Implications in Smart Agriculture and Food System [64]	Demonstrates the nature of modern information risk in causing "unknown unknown" risks.	• Emphasises the extent of cyber insurance coverage for the agriculture sector. • Discussion on the regulatory response to use of smart devices and its impact on smart farm security.	• Lacks clear future technological guidance for potential risks. • Incomplete arguments on future agriculture regulations and cyber insurance.
Smart Farming Cyber Security Challenges [77]	Uses empirical methodology to highlight security issues and challenges in smart farming.	• Discusses security challenges including agro-terrorism, social engineering, ransomware attacks, denial of service, and cyber-espionage. • Discusses cyber risk management framework.	• No implementation and results. • No use-cases to reflect how the attacks can be orchestrated. • Unclear distinction of cyber threat differences from other domains.
Enhanced Secure Device Authentication Algorithm in P2P-based Smart Farm System [78]	Enhances P2P communications security in smart farms through a new cryptography-based solution.	• Devises a lightweight encryption and decryption method to facilitate a robust authentication solution in smart farming P2P communications.	• It is not clear how fast and lightweight the current solution is, compared to the existing solutions. • The proposed solution has not been tested extensively in a real world scenario.
A Prediction Model Framework for Cyber Attacks to Precision Agriculture Technologies [79]	Focuses on assessing cyber-attack vulnerabilities in the technologies (e.g., sensors, transmitters and data systems) as well as in the smart farming environment.	• Constructs Common Vulnerability Scoring System (CVSS) score based on the technologies used in a smart farm with a consideration of the smart farming environmental nature.	• CVSS fails to accurately capture the impact of connections within the entire system. • Not suitable to assess vulnerability risks to highly diverse systems that use diverse protocols and network topologies.
Blockchain Related Research			
Blockchain and IoT Based Food Traceabilty System [80]	Improves the overall food safety issues by using blockchain to ensure food traceability.	• Tracks various aspects of the food production cycle using IoT sensors and blockchain technology. • Sensor based verification of the food production cycle proposed.	• The framework is constructed for a general blockchain, with specific advantages provided by a particular implementation. A generic version is missing. • Smart contracts on the blockchain are not implemented.
The Rise of Blockchain Technologies in Agriculture and Food Supply Chains [81]	Investigates the impact of Blockchain technology in agriculture and food supply chain.	• Critically reviews some of the ongoing blockchain-based projects in agriculture and food supply chain.	• There exist barriers and challenges which hinder wider popularity of Blockchain-based projects among farmers and farming systems.
Role of Internet of Things (IoT) with Blockchain Technology for the Development of Smart Farming [82]	Develops a framework based on IoT and blockchain technology for agriculture product tracking.	• Keeps track of the entire product life cycle using blockchain technology. • Builds a testbed to simulate a smart farm with 120 IoT nodes and 20 blockchain producers.	• No comparison to other work in literature. • Certain aspects of the simulation of the proposed framework is unclear such as what workload and probability distribution have been used.
Agriculture on the Blockchain: Sustainable Solutions for Food, Farmers, and Financing [83]	Explores applications of blockchain beyond the typical financial use cases in agriculture.	• Provides real world use cases of organizations using blockchain for agriculture. • Uses blockchain to provide food trace-ability across the entire supply chain.	• High Level discussion about the use cases with no implementation details or results.

TABLE 1. *(Continued.)* **Projects and research addressing cybersecurity in smart farming.**

A Framework for Blockchain Based Secure Smart Green House Farming [84]	Provides a light-weight security framework for smart greenhouse farms based on blockchain.	• Develops distributed blockchain based framework that incorporate the notion of leader elections to avoid single point of failure. • Provides threat analysis based on availability, integrity and confidentiality and their corresponding potential attacks.	• High level conceptual framework with no implementation or experiments. No related literature and no comparison to other proposed blockchain based frameworks.
AI and Machine Learning Assisted Work			
Design and Implementation of IoT based Smart Security and Monitoring for Connected Smart Farming [85]	Proposes a threshold based decision making system which focuses on soil condition information such as temperature and humidity.	• Designs and implements a low cost IoT based security monitoring system for environmental monitoring in smart farming.	• Data analysis is very limited in terms of applied methods. • Fails to address security and privacy issues in case of tampering with any smart farming component.
Security Systems for Remote Farm [86]	Focuses on the application of machine learning for pattern recognition of captured CCTV videos used in farm security.	• Security system for remote farms • Real time monitoring and notifications in smart farming • Image Processing and pattern recognition detected through surveillance system of smart farms	• The proposed solution is not scalable • It is not clear how multiple images from several cameras can be processed and analyzed in parallel in order to satisfy the real time property of the proposed system
Edge AI in Smart Farming IoT: CNNs at the Edge and Fog Computing with LoRa [87]	Expands the possibilities of smart agriculture and farming applications with Edge and Fog computing through low-power wide-area networks (LPWAN).	• Solves the problem of low-bandwidth transmissions with LPWANs. • Moves data analytic and compression toward end devices to extend the functionalities of LPWANs-based smart farming systems on the edge.	• Limited testbed and experiments. • The proposed system has no resiliency against saturation attacks which can be leveraged by attackers to seriously interrupt smart farming systems.
Big Data analysis for smart farming: results of TO2 project in theme food security [88]	Uses machine learning in big data analytic for smart farming security, with a use case in milk production chain.	• Develops a big data analytic platform for smart farming. • Works with two different machine learning techniques.	• The proposed system has been evaluated in a very limited number of use cases and its robustness in a real world scenario is unclear.
Other Relevant Literature			
A Framework for Cyber Security Approaches in Precision Farming [89]	Discusses challenges of wireless sensor network (WSN) in digital farm, and proposes a framework of security approach for data flow in precision agriculture.	• Proposes a cyber physical architecture introducing the notion of virtual farms. • Proposed cyber physical system offers real time high frequency decision systems. • Discusses security framework elements.	• High level conceptual abstract framework. • No implementation prototypes or evaluation results. • Incomplete data protection techniques.
Cyber Security in AgriFood Sector [90]	Discusses data security challenges within the agrifood sector.	• Provides use cases showing the increase of data in the agrifood sector and their need of data security measurements. • Interviewed companies about their cybersecurity concerns.	• No security solutions. • Limited scope to data security.
Cyber Security on the Farm: An Assessment of Cyber Security Practices in the United States Agriculture Industry [91]	Surveys farmers and agribusiness owners about their perceptions of cybersecurity, and how age, gender, and education might affect these perceptions.	• Quantifies levels of previous cyber-crime victimization and technology implementation. • Details how individuals react to known threats, and what motivates them to adopt protection technologies.	• A temporal analysis will further add to the understanding of how cyber threat perceptions change with more awareness.
Cyberbiosecurity: A New Perspective on Protecting US Food and Agricultural System [92]	Defines bio economy and investigates cyberbioeconomy security.	• Discusses how current and emerging data and infrastructure security issues affect the U.S. food and agricultural system and its cybersecurity.	• No feasible solution has been suggested to enhance cyberbioeconomy security.

warehousing, and selling. The system also uses various IoT based sensors to replace manual recording and verification with sensor based verification.

Other works [82], [84], [96] focused on providing case studies of using blockchain and smart contracts in smart farming. Awan *et al.* [82] proposed a framework based on IoT and blockchain technology for agriculture product tracking life cycle. They used smart contracts to eliminate the involvement of middlemen or third-party intermediaries and as such increase credibility and trust. The authors implemented a use case based on their proposed framework which included 120 IoT nodes and 20 blockchain producers. Further, they validated their system based on it's throughput considering different block sizes. However, this work has several drawbacks. Very few related works are included and comparison to other works in the literature is lacking. Additionally, the authors didn't include much details about the nature of workload used in their experiments and they failed to add a baseline benchmark for the validation results for a fair comparison. Patil *et al.* [84] proposed a light-weight security framework for smart greenhouse farms based on blockchain. Every IoT node can elect cluster head leader which helps preventing a single point of failure in case an attacker targets the leader node. Additionally, the authors provided discussion of the security threats on their proposed framework following the traditional confidentiality, integrity and availability (CIA) triad model as well as their corresponding attacks. Although, this work is interesting, the framework is conceptual with no implementation or experiments. Further, the paper didn't include related work nor a comparison to other proposed frameworks.

Besides proposing blockchain-based frameworks and implementations [97], real world use cases of blockchain in smart farming are discussed in the blockchain research institute article [83]. In this work, authors explore applications of blockchain beyond the typical financial use cases in agriculture. Accordingly, they focused on three classes of applications: food safety, sustainable agriculture and the local economy and agriculture finance. The authors accompanied each class of applications with real world use cases. However, these use cases are discussed on a very high level aspect with no implementation details or results.

C. 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. This data is sent to a controller where data is analyzed to make decisions like activating the actuators for water sprinkler in the farms. The proposed work is focused more on implementing the basic functionalities of smart farming than addressing security and privacy issues. It is very limited to simple threshold based decisions, like, if the soil temperature is above a certain threshold, then activate water sprinkler.

Real time security monitoring for a remote farm is another current application of ML in smart farming. In scenarios where real time monitoring and notifications are paramount to farm and cybersecurity, the image(s) detected through a surveillance system can be processed by open-source computer vision programming supported by AI. For example, Abuan *et al.* [86] proposed a neural based face recognition system which is able to be invariant to changes in illumination for background and illumination conditions through a neural network training.

The agricultural and farming industries have been widely influenced by the disruption of the IoT. However, the impact of the IoT is limited in countries with less penetration of mobile internet. The boom of low-power wide-area networks (LPWAN) in the last decade, with technologies such as LoRa or NB-IoT, has mitigated this by providing a relatively cheap infrastructure that enables low-power and long-range transmissions. Nonetheless, the benefits that LPWAN technologies have the disadvantage of low-bandwidth transmissions. Therefore, the integration of edge and fog computing, moving data analytics and compression near end devices, is key in order to extend functionality. By integrating AI at the local network layer, referred as edge AI, authors in [87] proposed a system architecture and implementation that expands the possibilities of smart agriculture and farming applications with edge and fog computing using LPWAN technology for large area coverage. In another research work [88], Support Vector Machines (SVM) along with Artificial Neural Networks (ANN) are used to create an integration platform for big data analysis for smart farming. Such a platform not only expedites processing huge amounts of data collected from farms and livestocks, but also gives smart farming stakeholders the ability to detect and respond against possible cyber attacks more efficiently.

D. OTHER RELEVANT LITERATURE

Chi *et al.* [89] present a framework for cybersecurity approaches in precision agriculture and discussed challenges of using Wireless Sensor Networks (WSN) in digital virtual farms. They also present a framework for secure data capture. Security challenges in agrifood sector has been extensively discussed in [90]. The report provides an overview of emerging technologies in smart farming. Most smart farms are data-driven with respect to automating agriculture processes, decision making, and predictions. It also raises important questions of how important is data security? How risk assessment is done considering the entire supply chain? Who should take responsibility and who should be involved? The report serves to raise awareness addressing the importance of cybersecurity in agrifood sector.

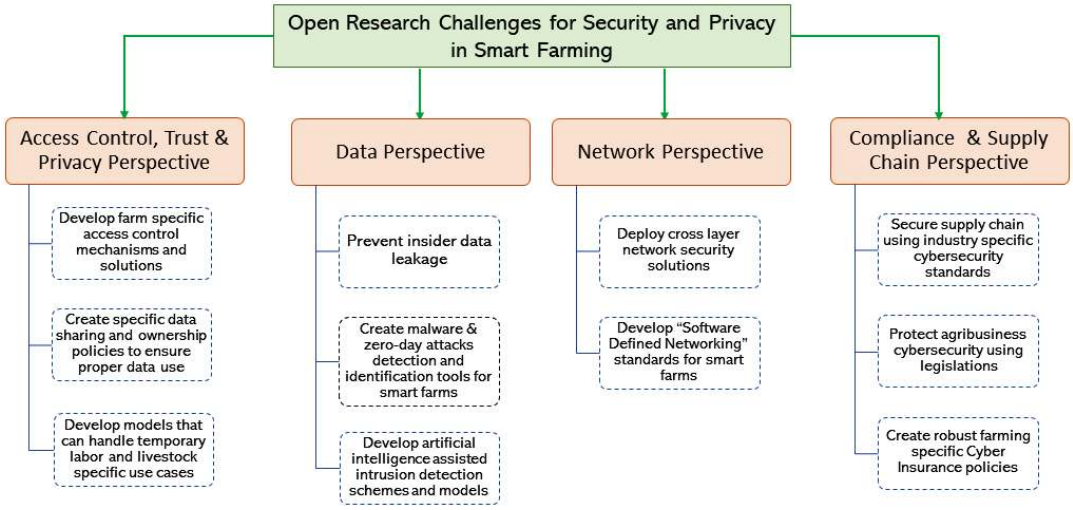

FIGURE 5. Open research challenges and future directions for cybersecurity in smart farming.

Authors in [98] provide an overview of cross-section of cybersecurity in food and agriculture sectors. They also discuss cyber-terrorism, policies, and plans. Spaulding and Wolf [99] detail the needs for educating farmers about various cybersecurity threats. Authors in [100] show the impact of cyber attacks on smart farming infrastructure via simulations using NETA with OMNET++ framework. Huning *et al.* [101] created a system to enable privacy preserving crowd sourcing techniques to estimate different smart farming parameters. Cybersecurity perception is also changing among farmers and agribusiness owners. Geil *et al.* [91] conducted an assessment of cybersecurity practices in the United States agriculture industry. Insights from their work reflect that over half of the respondents have been victims of a computer security incident, demonstrating that even individuals working in agriculture can be impacted by cybersecurity incidents. Cyberbiosecurity [92] is a multi-disciplinary domain consists of cybersecurity, bio-security, and cyber-physical security. It discusses how current and emerging information technologies affect the cybersecurity of large portion of U.S. economy which is based on food and agriculture (i.e. Bio-economy). As Peccoud *et al.* [102] discuss, food and agricultural sectors are immensely diverse and require advanced technologies and efficiencies that rely on computer technologies, big data, cloud-based data storage, and internet accessibility, at the same time are vulnerable to cybersecurity incidents.

Based on our literature review, it can be emphasised that, there is a dearth of security related research done in smart farming domain. There are numerous unanswered important security questions and open research challenges as discussed in the following section.

VI. OPEN CHALLENGES AND RESEARCH AREAS

This section discusses open research challenges for improving security and privacy in smart farming ecosystem, as well illustrated in Figure 5. These open problems have been divided into four subsections as follows.

A. ACCESS CONTROL, TRUST & PRIVACY PERSPECTIVE

The multi-layered architecture discussed in section II recognizes possibilities of cyber threat challenges, which needs to be addressed by extending and adapting current access control foundational research, as well as developing sophisticated access control solutions to assist dynamic and agile environments in cyber-physical systems like smart farms.

In-farm and cross farm operations need authorized interaction among sensors and labor/farmers working at multiple farms operating different sets of smart devices. What kind of operations they can do must be checked, which may require single level or multiple level access control depending on the risk factor associated with the operation? For example, consider sowing the field with autonomous tractor as compared to turning ON an irrigation system during the rainy season. Delegation and revocation of access rights to operate on a farm must be automatically performed based on the contract agreement, for example, in case temporary labor hired during harvesting season. Such access control requirements need further investigation to be adopted in such dynamic environment. The notion of trust can also be developed where labor who has worked earlier or an equipment borrowed from a 'known' old friend may have higher trust level as compared to machine and manpower hired from co-operative market. Self-configurable AI assisted smart access control policies need to be developed in a sharing-dominated CPS domain like smart farming.

Cyber physical systems introduce the notion of virtual objects (which can be created in cloud or edge environment) corresponding to real physical sensors. An important challenge here is the location of cyber entities created as a part of connection with cloud or edge environments, for example,

AWS device shadows[34] or Microsoft Azure device twins.[35] Research needs to determine: a) how cyber entity will move from one cloud (or edge) to another if the corresponding device is borrowed from one farmer to another? b) how the control of virtual entities will be delegated to the lending farmer, whether both the farmers need to use same application? c) how the applications will allow to delegate access for machine operation? d) Can the virtual objects or equipment across farms communicate with each other, whether at the physical level or using the virtual entities? If it is the virtual entity across different accounts in the same cloud provider, how such interaction will take place? In case it is across different cloud providers, how cross cloud and federated cloud environments will ensure such trust levels? Suppose in case a farmer has borrowed an equipment from a friend farmer, will the original owner be able to have access to it, or the access will be completely revoked? Is it possible to control a device through different remote clouds? All are relevant questions in smart farming domain. Further, how to establish trust mechanisms among different cloud service providers which the farmer is using for services and alerts? Manufacturer of the device may hold digital twin [103] and the cloud used by farmers will get data from on-field sensor and the cloud provider via pre-defined and signed negotiations. Such negotiations can also define what kind of data will be shared with required permissions of the owner farmer. Another important question is, how to establish trust between physical sensor objects? One approach is sensors at the same farm trust each other more for the shared information as compared to sensors across different farms. IoT and CPS specific cross cloud access controls and related security models are still in infancy stage and need more attention.

Livestock and animals also have sensors embedded, which require appropriate authorized access. However, current literature does not provide strong access control mechanisms that can restrict such operations and secure critical data sharing from cattle and livestock at the farm. These wearable and health monitoring devices are attached to livestock and collect sensitive data, which can be used by adversaries to control the animal or even effect the sale/purchase of a cattle, for example, having the information about which cow is having low milk production. Efficient access controls [104]–[106] are needed to safeguard such sensitive data in cloud, which needs more research considering the spate of breaches heard every now and then. Usually in case of wearable IoT devices, a human which has the device controls what kind of data he/she wants to be shared. However, it is not in case of livestock which has a master (like the owner of the farm or caretaker) to decide control. Also, as a cattle is sold/purchased and moves from one owner to another, relevant data sharing security policies need to be specified and will require automatically configured information sharing. Studies [107], [108] have shown vulnerabilities in human used fitness devices, however, such studies and research are still an open challenge in case of livestock devices.

Since data is collected from smart devices spread across farms, different applications require to access to this data. Consequentially, it is important to limit the sharing of data across applications and across nearby friend farmers, who may also get some value or receive alerts for their farms. How and when to share such information requires adaptive security policies to control and supervise data transferred by sensors to the cloud platform. Further, if data is sharing across multi cloud systems, cross cloud trust also needs to be addressed. Appropriate attribute based fine grained access controls [109], [110] and privacy preserving schemes need to be deployed to ensure confidentiality of the data. Evidently, farmers must decide the level and type of data sharing needed to ensure the privacy of critical information.

B. DATA PERSPECTIVE

The most noticeable feature of smart farming is its communication ability between the smart devices, resulting in an unprecedented amount of generated data [7], [111]. This provides many challenges as discussed in section III and open doors for several research opportunities. Machine learning is an attractive solution for processing big data, and implementing effective security solutions.

Insider data leakage detection has always been a daunting task as users already have legitimate access to the system, making it hard to detect and predict such attacks. Several research works have been conducted on insider data leakage [22], [112], [113]; however, none has been targeting smart farming settings. Further investigation is needed to understand the possibility of adopting insider data leakage defense mechanisms into smart farming and whether unique characteristics of smart farming can help to improve these mechanisms.

Smart farms are highly connected systems, which allow malware to easily propagate through the network infecting all interconnected devices. An interesting question is how to detect malware in smart farming IoT environment, especially considering all heterogeneous devices in place. For instance, a malware detection technique that works against a malware that infects smart farming equipment might not work against malware that infects edge or cloud systems since the malware's end goal is different. Many AI assisted malware detection techniques [114]–[120] are proposed and used in practice; however, there are no smart-farming-specific malware detection techniques that consider the context and environment in which smart farms reside.

Smart farms generate diverse and vast amount of unstructured data. It is almost impossible for one party to analyze and make use of the entire datasets. For this reason, threat information sharing is a viable approach for data security. For instance, each smart farm can employ a malware detection technique; however, it is guaranteed that none of these employed techniques is comprehensive enough to catch all

[34] https://docs.aws.amazon.com/iot/latest/developerguide/iot-device-shadows.html

[35] https://docs.microsoft.com/en-us/azure/iot-hub/iot-hub-devguide-device-twins

types of malware. Information sharing between smart farms can prove very useful. It can be used as an asset to share threat information about attack patterns or malware that was detected by collaborating smart farms. In a similar case, if a deployed detection technique in a farm detected supplied water with high toxin content, it is relevant to share that information with nearby farms who may also be impacted by similar issue. This can save analysis cost and money for every participating smart farm as it prevents doing work that someone else already did before. What kind of data, meta-data or analysis can be shared remains an open question and what kind of threat information sharing process can be used remain an open question for resource constrained farmers.

Smart farming is an emerging field, so it is highly likely to encounter zero-day attacks which have not been detected before. Anomaly detection [121]–[125] is a very appealing solution against such attacks. Anomaly detection techniques look for any abnormal behavior that deviates from the pre-established database of normal behavior. These normal behaviour profiles are constructed based on collection of historical observations and patterns. Building smart farms behavior profiles is a challenging task since their behaviors are so dynamic in nature. External factors are a major reason for this dynamism. For example, less irrigation is needed during a rainy weather than dry weather which will cause a different behavior for irrigation systems. Can weather forecast information be used as an indication of such change of behavior? What kind of data contribute to building smart farms behavior profiles? Do some data fields weigh more than others? These are all open research questions that need to be investigated.

Detection mechanisms are used to detect faulty and compromised sensors by monitoring the data sent for any tampered or abnormal values. Employing a simple threshold based mechanism can easily be bypassed by an attacker, so in most cases, more sophisticated machine learning based mechanisms need to be deployed. However, smart attackers can still bypass these models by (1) exploiting the sensors and a little tweaking of data sent by these sensors just to lead the machine learning model in place to misclassify/mispredict the outcome (such attack is called adversarial machine learning attack), and (2) poisoning the model during training phase by injecting bad data into the model's training database, and in turn get it to learn something it shouldn't. Some research addressed mitigation against adversarial attacks; however, it is not clear whether these technologies can be adopted to smart farming domain which is very dominant on changing environment conditions.

Another open research challenge is to create various artificial intelligence systems that collect and parse Cyber Threat Intelligence (CTI[36]) about smart devices, software, cloud systems etc. used in the smart farming ecosystem. These systems have been developed to collect CTI in other areas [126]–[129] and need to be extended to ensure coverage of various smart farming devices, equipment and software.

[36]https://www.cisecurity.org/blog/what-is-cyber-threat-intelligence/

C. NETWORK PERSPECTIVE

Cybersecurity threats to smart farming and its devices include a diverse range of security risks due to certain characteristics of the underlying networking and communication technologies which are used in the domain.

First, both virtual and physical communication environments get connected. Many IoT devices in a smart farm system are capable of functioning on the data they receive from their respective environments which shortens the distance between virtual and physical systems. While convenient for the users, it allows cyber threats to convert to physical consequences more quickly, thereby having a bigger impact. Second, devices and layers involved in a smart farm system create a complex communication environment. Hyper connected farming environments exist due to the growing availability and diversity of IoT devices. 'Complex' in this context means that large number of devices are working in a single smart farm environment such that dynamic interactions between them are possible. This complexity expands the capabilities of an environment, but at the cost of a wider attack surface.

Smart farming like other emerging technologies is embracing new networking paradigms to tackle today's sophisticated attacks. Software defined network (SDN) [130]–[132] is one such promising networking revolution. Through decoupling control plane from data plane and giving credit to network programmable, it offers interesting technical capabilities to network providers. This causes an intense adaption of SDN in almost every fields of networking, from data center networks to WANs, wireless, 5G and recently IoT. Using SDN in smart farm networking is attracting to both academia and industry for certain reasons. SDN supports both physical and virtual networking scenarios very well. It also offers a reliable way of practicing networking in highly diverse and naturally heterogeneous smart farms networking environment. Moreover, using SDN, smart farms are able to form a holistic view of all the connected devices along with how they interact in a near real time manner. Such a holistic view not only improves agility, scalability, and manageability of smart farm networking but also empowers a large smart farm network to enforce robust security counter measure against possible sophisticated cyber attacks.

It is important to research further the adaptability of SDN and other 5G related next generation communication technologies in smart farming and precision agriculture domain. SDN can enable smart farms to get the most benefit out of complex machine learning and AI algorithms to automate network management of large number of sensors, wireless and wired networks used in a smart farming ecosystem. It also facilitates implementing advanced, cross-layer network security solutions which are very time and resource consuming,

if not impossible, otherwise. Finally, SDN expedites edge networking and hence cloud-based security-as-a-service delivery model becomes a more approachable solution in large smart farming deployments.

D. COMPLIANCE AND SUPPLY CHAIN PERSPECTIVE

With the ubiquitous use of sensors, automated drones, blockchain, artificial intelligence integration, different agricultural businesses are falling back on compliance, regulation and cyber insurance to protect themselves [64]. With the development of targeted malware and other cyber threats, the entire food supply chain is at risk [12], [64]. A hostile actor specifically interested in disrupting the supply chain can target various organizations and companies that supply raw material to farms or process food for the end user. A potential solution to this problem is to develop industry standards that enable trust between various raw material suppliers and downstream food processors [64].

The development of these standards enforced by national governments through regulation, has been slow. One example of such a shortcoming, is the existence of a few cybersecurity standards for the many smart devices used in the food supply chain. Various legislation are being introduced to set 'minimal cybersecurity operational standards for internet connected devices'. In specific cases where various governments do not wish to regulate these interactions, it is up to various agriculture businesses to protect themselves by asking their supply chain to 'self-regulate' cybersecurity best practices [64]. Such developments can be pushed through market demands, competitive pressure, etc.

The food supply chain also lacks robust cyber insurance policies. With the constant development of smart applications, AI, smart farming equipment, etc. cyber insurance providers are unable to predict and quantify various cyber risks involved in these systems. Specific research needs to be done so as to develop standard legal jargon and metrics to quantify cyber risk in smart farming. These will help create robust cyber insurance markets for precision agriculture. Various systems [133]–[136] also need to be built to make it easier for the end users to understand and parse these complex legal documents, cyber insurance policies, agreements, contracts, etc. Research on these open challenges will help wide adoption of precision agriculture technologies.

VII. CONCLUSION

The proliferation 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. This paper discusses such cybersecurity challenges in smart farming and elaborates open research questions. The paper first outlines a multi-layer smart farming architecture illustrating different entities pertinent to real time use-cases supported by edge and cloud environments. Based on the architecture, the paper outlines security and privacy issues and highlights different attacks scenarios in smart farms as well as scenarios affecting the entire food supply chain. Thereafter, this article surveys the state-of-the-art research and acknowledges important works related to cybersecurity in the domain. Finally, the paper illustrates several open challenges and research problems pertinent to security and privacy aspects in precision agriculture. We envision this paper will simulate research to solve platitude of security and data privacy issues in fast growing and economically important smart farming sector.

ACKNOWLEDGMENT

The authors would like to thank Dr. B. Leckie, Associate Professor in the School of Agriculture at Tennessee Technological University, for his domain expertise, insightful comments, and suggestions, to make this manuscript more comprehensible. *(All authors contributed equally to this work.)*

REFERENCES

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

[2] H. C. J. Godfray, J. R. Beddington, I. R. Crute, L. Haddad, D. Lawrence, J. F. Muir, J. Pretty, S. Robinson, S. M. Thomas, and C. Toulmin, "Food security: The challenge of feeding 9 billion people," *Science*, vol. 327, no. 5967, pp. 812–818, Jan. 2010.

[3] D. Gollin, S. Parente, and R. Rogerson, "The role of agriculture in development," *Amer. Econ. Rev.*, vol. 92, no. 2, pp. 160–164, 2002.

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

[5] D. Vasisht, Z. Kapetanovic, J. Won, X. Jin, R. Chandra, 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, pp. 515–529.

[6] A. Kamilaris, F. Gao, F. X. Prenafeta-Boldu, and M. I. Ali, "Agri-IoT: A semantic framework for Internet of Things-enabled smart farming applications," in *Proc. IEEE 3rd World Forum Internet Things (WF-IoT)*, Dec. 2016, pp. 442–447.

[7] S. Wolfert, L. Ge, C. Verdouw, and M.-J. Bogaardt, "Big data in smart farming—A review," *Agricult. Syst.*, vol. 153, pp. 69–80, May 2017.

[8] A. Alvino and S. Marino, "Remote sensing for irrigation of horticultural crops," *Horticulturae*, vol. 3, no. 2, p. 40, Jun. 2017.

[9] E.-C. Oerke and H.-W. Dehne, "Safeguarding production—Losses in major crops and the role of crop protection," *Crop Protection*, vol. 23, no. 4, pp. 275–285, 2004.

[10] A. Walter, R. Finger, R. Huber, and N. Buchmann, "Opinion: Smart farming is key to developing sustainable agriculture," *Proc. Nat. Acad. Sci. USA*, vol. 114, no. 24, pp. 6148–6150, Jun. 2017.

[11] O. S. Cupp, D. E. Walker, and J. Hillison, "Agroterrorism in the U.S.: Key security challenge for the 21st century," *Biosecur. Bioterrorism, Biodefense Strategy, Pract., Sci.*, vol. 2, no. 2, pp. 97–105, 2004.

[12] A. Boghossian, "Threats to precision agriculture," U.S. Dept. Homeland Secur., Washington, DC, USA, Tech. Rep., 2018.

[13] M. Wazid, A. K. Das, V. Odelu, N. Kumar, M. Conti, and M. Jo, "Design of secure user authenticated key management protocol for generic IoT networks," *IEEE Internet Things J.*, vol. 5, no. 1, pp. 269–282, Feb. 2018.

[14] M. S. Henriques and N. K. Vernekar, "Using symmetric and asymmetric cryptography to secure communication between devices in IoT," in *Proc. Int. Conf. IoT Appl. (ICIOT)*, May 2017, pp. 1–4.

[15] Z.-K. Zhang, M. C. Y. Cho, C.-W. Wang, C.-W. Hsu, C.-K. Chen, and S. Shieh, "IoT security: Ongoing challenges and research opportunities," in *Proc. IEEE 7th Int. Conf. Service-Oriented Comput. Appl.*, Nov. 2014, pp. 230–234.

[16] J. P. Hubaux, S. Capkun, and J. Luo, "The security and privacy of smart vehicles," *IEEE Secur. Privacy Mag.*, vol. 2, no. 3, pp. 49–55, May 2004.

[17] H. Li, R. Lu, J. Misic, and M. Mahmoud, "Security and privacy of connected vehicular cloud computing," *IEEE Netw.*, vol. 32, no. 3, pp. 4–6, May 2018.

[18] A. Dorri, M. Steger, S. S. Kanhere, and R. Jurdak, "BlockChain: A distributed solution to automotive security and privacy," *IEEE Commun. Mag.*, vol. 55, no. 12, pp. 119–125, Dec. 2017.
[19] R. M. Noor, R. H. Khokhar, R. Jabbarpour, S. Khorsandroo, N. Khamis, and O. Michael, "Using VANET to support green vehicle communications for urban operation rescue," in *Proc. 12th Int. Conf. ITS Telecommun.*, Nov. 2012, pp. 324–328.
[20] C. 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.*, vol. 56, no. 1, pp. 64–69, Jan. 2018.
[21] D. He, Y. Qiao, S. Chan, and N. Guizani, "Flight security and safety of drones in airborne fog computing systems," *IEEE Commun. Mag.*, vol. 56, no. 5, pp. 66–71, May 2018.
[22] M. B. Mollah, M. A. K. Azad, and A. Vasilakos, "Secure data sharing and searching at the edge of cloud-assisted Internet of Things," *IEEE Cloud Comput.*, vol. 4, no. 1, pp. 34–42, Jan. 2017.
[23] S. N. Shirazi, A. Gouglidis, A. Farshad, and D. Hutchison, "The extended cloud: Review and analysis of mobile edge computing and fog from a security and resilience perspective," *IEEE J. Sel. Areas Commun.*, vol. 35, no. 11, pp. 2586–2595, Nov. 2017.
[24] S. Yi, Z. Qin, and Q. Li, "Security and privacy issues of fog computing: A survey," in *Proc. Int. Conf. Wireless Algorithms, Syst., Appl.* Springer, 2015, pp. 685–695.
[25] N. Yang, L. Wang, G. Geraci, M. Elkashlan, J. Yuan, and M. D. Renzo, "Safeguarding 5G wireless communication networks using physical layer security," *IEEE Commun. Mag.*, vol. 53, no. 4, pp. 20–27, Apr. 2015.
[26] M. Strohmeier, M. Schäfer, R. Pinheiro, V. Lenders, and I. Martinovic, "On perception and reality in wireless air traffic communication security," *IEEE Trans. Intell. Transp. Syst.*, vol. 18, no. 6, pp. 1338–1357, Oct. 2016.
[27] M. Ahmed, M. R. J. Sattari, M. K. Nasir, S. Ghahremani, S. Khorsandroo, S. A. S. Ali, and R. M. Noor, "Vehicle adhoc sensor network framework to provide green communication for urban operation rescue," *Lect. Notes Inf. Theory*, vol. 1, no. 2, pp. 77–82, 2013.
[28] M. Gigli and S. Koo, "Internet of Things: Services and applications categorization," *Adv. Internet Things*, vol. 01, no. 02, pp. 27–31, 2011.
[29] A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, and M. Ayyash, "Internet of Things: A survey on enabling technologies, protocols, and applications," *IEEE Commun. Surveys Tuts.*, vol. 17, no. 4, pp. 2347–2376, 4th Quart., 2015.
[30] L. Atzori, A. Iera, and G. Morabito, "The Internet of Things: A survey," *Comput. Netw.*, vol. 54, no. 15, pp. 2787–2805, Oct. 2010.
[31] J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, "Internet of Things (IoT): A vision, architectural elements, and future directions," *Future Gener. Comput. Syst.*, vol. 29, no. 7, pp. 1645–1660, Sep. 2013.
[32] A. R. Biswas and R. Giaffreda, "IoT and cloud convergence: Opportunities and challenges," in *Proc. IEEE World Forum Internet Things (WF-IoT)*, Mar. 2014, pp. 375–376.
[33] R. Lea and M. Blackstock, "City hub: A cloud-based IoT platform for smart cities," in *Proc. IEEE 6th Int. Conf. Cloud Comput. Technol. Sci.*, Dec. 2014, pp. 799–804.
[34] A. Botta, W. de Donato, V. Persico, and A. Pescape, "On the integration of cloud computing and Internet of things," in *Proc. Int. Conf. Future Internet Things Cloud*, Aug. 2014, pp. 23–30.
[35] M. Aazam, I. Khan, A. A. Alsaffar, and E.-N. Huh, "Cloud of things: Integrating Internet of Things and cloud computing and the issues involved," in *Proc. IBCAST*, Jan 2014, pp. 414–419.
[36] M. Díaz, C. Martín, and B. Rubio, "State-of-the-art, challenges, and open issues in the integration of Internet of Things and cloud computing," *J. Netw. Comput. Appl.*, vol. 67, pp. 99–117, May 2016.
[37] A. Botta, W. de Donato, V. Persico, and A. Pescapé, "Integration of cloud computing and Internet of Things: A survey," *Future Gener. Comput. Syst.*, vol. 56, pp. 684–700, Mar. 2016.
[38] A. Y. Ding and M. Janssen, "Opportunities for applications using 5G networks: Requirements, challenges, and outlook," in *Proc. 7th Int. Conf. Telecommun. Remote Sens. (ICTRS)*, 2018, pp. 27–34.
[39] M. López, S. Martínez, J. M. Gómez, A. Herms, L. Tort, J. Bausells, and A. Errachid, "Wireless monitoring of the pH, NH4+ and temperature in a fish farm," *Procedia Chem.*, vol. 1, no. 1, pp. 445–448, Sep. 2009.
[40] P. Bahl, R. Chandra, T. Moscibroda, R. Murty, and M. Welsh, "White space networking with Wi-Fi like connectivity," *ACM SIGCOMM Comput. Commun. Rev.*, vol. 39, no. 4, pp. 27–38, Aug. 2009.
[41] 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 *Adv. Agronomy*, vol. 133, pp. 71–112, Jan. 2015.
[42] A. R. Frost, C. P. Schofield, S. A. Beaulah, T. T. Mottram, J. A. Lines, and C. M. Wathes, "A review of livestock monitoring and the need for integrated systems," *Comput. Electron. Agricult.*, vol. 17, no. 2, pp. 139–159, May 1997.
[43] D. Berckmans, "Automatic on-line monitoring of animals by precision livestock farming," in *Livestock Production and Society*, vol. 287. Wageningen, The Netherlands: Wageningen Academic Publishers, 2006.
[44] B. Tang and R. Sandhu, "Cross-tenant trust models in cloud computing," in *Proc. IEEE 14th Int. Conf. Inf. Reuse Integr. (IRI)*, Aug. 2013, pp. 129–136.
[45] N. Pustchi, R. Krishnan, and R. Sandhu, "Authorization federation in IaaS multi cloud," in *Proc. 3rd Int. Workshop Secur. Cloud Comput. (SCC)*, 2015, pp. 63–71.
[46] A. Ouaddah, H. Mousannif, A. A. Elkalam, and A. A. Ouahman, "Access control in the Internet of Things: Big challenges and new opportunities," *Comput. Netw.*, vol. 112, pp. 237–262, Jan. 2017.
[47] L. Seitz, G. Selander, and C. Gehrmann, "Authorization framework for the Internet-of-Things," in *Proc. IEEE 14th Int. Symp. 'World Wireless, Mobile Multimedia Networks' (WoWMoM)*, Jun. 2013, pp. 1–6.
[48] V. G. Cerf, "Access control and the Internet of Things," *IEEE Internet Comput.*, vol. 19, no. 5, p. 96-c3, Sep. 2015.
[49] G. Zhang and J. Tian, "An extended role based access control model for the Internet of Things," in *Proc. Int. Conf. Inf., Netw. Autom. (ICINA)*, Oct. 2010, pp. 319–323.
[50] N. Ye, Y. Zhu, R.-C. Wang, R. Malekian, and L. Qiao-min, "An efficient authentication and access control scheme for perception layer of Internet of Things," *Appl. Math. Inf. Sci.*, vol. 8, no. 4, pp. 1617–1624, Jul. 2014.
[51] S. Kaiwen and Y. Lihua, "Attribute-role-based hybrid access control in the Internet of Things," in *Proc. APWeb*. Springer, 2014, pp. 333–343.
[52] J. L. Hernandez-Ramos, A. J. Jara, L. Marın, and A. F. Skarmeta, "Distributed capability-based access control for the Internet of Things," *J. Internet Services Inf. Secur.*, vol. 3, nos. 3–4, pp. 1–16, Nov. 2013.
[53] S. Gusmeroli, S. Piccione, and D. Rotondi, "A capability-based security approach to manage access control in the Internet of things," *Math. Comput. Model.*, vol. 58, nos. 5–6, pp. 1189–1205, Sep. 2013.
[54] M. Gupta and R. Sandhu, "Authorization framework for secure cloud assisted connected cars and vehicular Internet of Things," in *Proc. 23nd ACM Symp. Access Control Models Technol. (SACMAT)*, 2018, pp. 193–204.
[55] M. Gupta, J. Benson, F. Patwa, and R. Sandhu, "Dynamic groups and attribute-based access control for next-generation smart cars," in *Proc. 9th ACM Conf. Data Appl. Secur. Privacy (CODASPY)*, 2019, pp. 61–72.
[56] M. Gupta, J. Benson, F. Patwa, and R. Sandhu, "Secure cloud assisted smart cars using dynamic groups and attribute based access control," 2019, *arXiv:1908.08112*. [Online]. Available: http://arxiv.org/abs/1908.08112
[57] 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.
[58] 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/2001.04041
[59] Y. Wei Law, M. Palaniswami, G. Kounga, and A. Lo, "WAKE: Key management scheme for wide-area measurement systems in smart grid," *IEEE Commun. Mag.*, vol. 51, no. 1, pp. 34–41, Jan. 2013.
[60] X. Fan, L. Liu, R. Zhang, Q. Jing, and J. Bi, "Decentralized trust management," *ACM Comput. Surv.*, vol. 53, no. 1, pp. 1–33, Feb. 2020.
[61] A. Bothe, J. Bauer, and N. Aschenbruck, "RFID-assisted continuous user authentication for IoT-based smart farming," in *Proc. IEEE Int. Conf. RFID Technol. Appl. (RFID-TA)*, Sep. 2019, pp. 505–510.
[62] E. Bou-Harb, C. Fachkha, M. Pourzandi, M. Debbabi, and C. Assi, "Communication security for smart grid distribution networks," *IEEE Commun. Mag.*, vol. 51, no. 1, pp. 42–49, Jan. 2013.
[63] S. K. Routray, M. K. Jha, L. Sharma, R. Nyamangoudar, A. Javali, and S. Sarkar, "Quantum cryptography for IoT: APerspective," in *Proc. Int. Conf. IoT Appl. (ICIOT)*, May 2017, pp. 1–4.
[64] M. M. Jahn. (2019). *Cyber Risk and Security Implications in Smart Agriculture and Food Systems*. Accessed: Nov. 14, 2019. [Online]. Available: https://jahnresearchgroup.webhosting.cals.wisc.edu/wp-content/uploads/sites/223/2019/01/Agricultural-Cyber-Risk-and-Security.pdf

[65] (2019). *United States, Environment Protection Agency*. Accessed: Dec. 15 12, 2019. [Online]. Available: https://www.epa.gov/agriculture/laws-and-regulations-apply-your-agricultural-operation-farm-activity

[66] (2019). *United States, Department of Agriculture*. Accessed: Dec. 12, 2019. [Online]. Available: https://www.usda.gov/our-agency/about-usda/laws-and-regulations

[67] (2019). *European Union, Department of Agriculture and Rural Development*. Accessed: Dec. 12, 2019. [Online]. Available: https://ec.europa.eu/info/publications/regulations-food-and-agricultural-products_en

[68] N. Gruschka and M. Jensen, "Attack surfaces: A taxonomy for attacks on cloud services," in *Proc. IEEE 3rd Int. Conf. Cloud Comput.*, Jul. 2010, pp. 276–279.

[69] C. Kolias, G. Kambourakis, A. Stavrou, and J. Voas, "DDoS in the IoT: Mirai and other botnets," *Computer*, vol. 50, no. 7, pp. 80–84, 2017.

[70] 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 Secur. Symp. (USENIX Secur.)*, 2017, pp. 1093–1110.

[71] T. Tyagi, "Botnet of things: Menace to Internet of Things," in *Proc. 3rd Int. Conf. Comput., Commun., Netw. Secur.*, 2018, pp. 1–5.

[72] G. Kambourakis, C. Kolias, and A. Stavrou, "The Mirai botnet and the IoT zombie armies," in *Proc. IEEE Mil. Commun. Conf. (MILCOM)*, Oct. 2017, pp. 267–272.

[73] A. Ukil, J. Sen, and S. Koilakonda, "Embedded security for Internet of Things," in *Proc. 2nd Nat. Conf. Emerg. Trends Appl. Comput. Sci.*, Mar. 2011, pp. 1–6.

[74] M. M. Aung and Y. S. Chang, "Traceability in a food supply chain: Safety and quality perspectives," *Food Control*, vol. 39, pp. 172–184, May 2014.

[75] P. Santhana and A. Biswas. (2017). *Blockchain Risk Management–Risk Functions Need to Play an Active Role in Shaping Blockchain Strategy*. Accessed: Dec. 7, 2019. [Online]. Available: https://www2.deloitte.com/content/dam/Deloitte/us/Documents/financial-services/us-fsi-blockchain-risk-management.pdf

[76] M. Window, "Security in precision agriculture: Vulnerabilities and risks of agricultural systems," Dept. Comput. Sci., Elect. Space Eng., Luleå Univ. Technol., Luleå, Sweden, Tech. Rep., 2019.

[77] L. Barreto and A. Amaral, "Smart farming: Cyber security challenges," in *Proc. Int. Conf. Intell. Syst. (IS)*, Sep. 2018, pp. 870–876.

[78] C.-J. Chae and H.-J. Cho, "Enhanced secure device authentication algorithm in P2P-based smart farm system," *Peer-to-Peer Netw. Appl.*, vol. 11, no. 6, pp. 1230–1239, Jan. 2018.

[79] J. West, "A prediction model framework for cyber-attacks to precision agriculture technologies," *J. Agricult. Food Inf.*, vol. 19, no. 4, pp. 307–330, Feb. 2018.

[80] J. Lin, Z. Shen, A. Zhang, and Y. Chai, "Blockchain and IoT based food traceability system," *Int. J. Inf. Technol.*, vol. 24, no. 1, pp. 1–16, 2018.

[81] A. Kamilaris, A. Fonts, and F. X. Prenafeta-Boldú, "The rise of blockchain technology in agriculture and food supply chains," *Trends Food Sci. Technol.*, vol. 91, pp. 640–652, Sep. 2019.

[82] S. H. Awan, S. Ahmed, N. Safwan, Z. Najam, M. Z. Hashim, and T. Safdar, "Role of Internet of Things (IoT) with blockchain technology for the development of smart farming," *J. Mech. Continua Math. Sci.*, vol. 14, no. 5, pp. 170–188, Sep./Oct. 2019.

[83] H. M. Kim and M. Laskowski, "Agriculture on the blockchain: Sustainable solutions for food, farmers, and financing," in *Supply Chain Revolution*. Barrow Books, 2018.

[84] A. S. Patil, B. A. Tama, Y. Park, and K.-H. Rhee, "A framework for blockchain based secure smart green house farming," in *Advances in Computer Science and Ubiquitous Computing*. Springer, 2017, pp. 1162–1167.

[85] L. S. Shabadi and H. B. Biradar, "Design and implementation of IOT based smart security and monitoring for connected smart farming," *Int. J. Comput. Appl.*, vol. 179, no. 11, pp. 1–4, Jan. 2018.

[86] D. D. Abuan, A. C. Abad, J. B. Lazaro, Jr., and E. P. Dadios, "Security systems for remote farm," *J. Autom. Control Eng.*, vol. 2, no. 2, pp. 115–118, 2014.

[87] T. N. Gia, L. Qingqing, J. P. Queralta, Z. Zou, H. Tenhunen, and T. Westerlund, "Edge AI in smart farming IoT: CNNs at the edge and fog computing with LoRa," in *Proc. IEEE AFRICON*, Sep. 2019.

[88] C. Kempenaar, C. Lokhorst, E. Bleumer, R. Veerkamp, T. Been, F. V. Evert, M. Boogaardt, L. Ge, J. Wolfert, and C. Verdouw, "Big data analysis for smart farming: Results of To$_2$ project in theme food security," Wageningen Univ. Res., Tech. Rep. 655, Wageningen, The Netherlands, 2016.

[89] H. Chi, S. Welch, E. Vasserman, and E. Kalaimannan, "A framework of cybersecurity approaches in precision agriculture," in *Proc. 5th Int. Conf. Manage. Leadership Governance (ICMLG)*, Reading, U.K., 2017, pp. 90–95.

[90] M. Bogaardt, K. Poppe, V. Viool, and E. V. Zuidam, "Cybersecurity in the Agrifood sector," Capgemini Consulting, Paris, France, Tech. Rep., 2016.

[91] A. Geil, G. Sagers, A. D. Spaulding, and J. R. Wolf, "Cyber security on the farm: An assessment of cyber security practices in the united states agriculture industry," *Int. Food Agribusiness Manage. Rev.*, vol. 21, no. 3, pp. 317–334, Mar. 2018.

[92] S. E. Duncan, R. Reinhard, R. C. Williams, F. Ramsey, W. Thomason, K. Lee, N. Dudek, S. Mostaghimi, E. Colbert, and R. Murch, "Cyber-biosecurity: A new perspective on protecting U.S. food and agricultural system," *Frontiers Bioeng. Biotechnol.*, vol. 7, p. 63, Mar. 2019.

[93] S. Underwood, "Blockchain beyond bitcoin," *Commun. ACM*, vol. 59, no. 11, pp. 15–17, Oct. 2016.

[94] M. Crosby, P. Pattanayak, S. Verma, and V. Kalyanaraman, "Blockchain technology: Beyond bitcoin," *Appl. Innov.*, vol. 2, nos. 6–10, p. 71, 2016.

[95] M. Pilkington, "Blockchain technology: Principles and applications," in *Research Handbook on Digital Transformations*, vol. 225. Cheltenham, U.K.: Edward Elgar Publishing, 2016.

[96] Y.-P. Lin, J. Petway, J. Anthony, H. Mukhtar, S.-W. Liao, C.-F. Chou, and Y.-F. Ho, "Blockchain: The evolutionary next step for ICT E-agriculture," *Environments*, vol. 4, no. 3, p. 50, Jul. 2017.

[97] Y. Voutos, G. Drakopoulos, and P. Mylonas, "Smart agriculture: An open field for smart contracts," in *Proc. 4th South-East Eur. Design Autom., Comput. Eng., Comput. Netw. Social Media Conf. (SEEDA-CECNSM)*, Sep. 2019, pp. 1–6.

[98] C. Cooper, "Cybersecurity in food and agriculture," *Protecting Our Future*, vol. 2, 2015.

[99] A. D. Spaulding and J. R. Wolf, "Cyber-security knowledge and training needs of beginning farmers in Illinois," Dept. Agricult., Illinois State Univ., Normal, IL, USA, Tech. Rep., 2018.

[100] S. Linsner, R. Varma, and C. Reuter, "Vulnerability assessment in the smart farming infrastructure through cyberattacks," in *Proc. GIL Annu. Conf., Digitization Agricult. Enterprises Small Struct. Regions Contradiction Terms*, 2019, pp. 119–124.

[101] L. Huning, J. Bauer, and N. Aschenbruck, "A privacy preserving mobile crowdsensing architecture for a smart farming application," in *Proc. 1st ACM Workshop Mobile Crowdsensing Syst. Appl. (CrowdSenSys)*, New York, NY, USA, 2017, p. 62–67.

[102] J. Peccoud, J. E. Gallegos, R. Murch, W. G. Buchholz, and S. Raman, "Cyberbiosecurity: From naive trust to risk awareness," *Trends Biotechnol.*, vol. 36, no. 1, pp. 4–7, Jan. 2018.

[103] A. El Saddik, "Digital twins: The convergence of multimedia technologies," *IEEE MultimediaMag.*, vol. 25, no. 2, pp. 87–92, Apr. 2018.

[104] M. Gupta, F. Patwa, and R. Sandhu, "Object-tagged RBAC model for the Hadoop ecosystem," in *Proc. DBSec*. Springer, 2017, pp. 63–81.

[105] M. Gupta, F. Patwa, J. Benson, and R. Sandhu, "Multi-layer authorization framework for a representative Hadoop ecosystem deployment," in *Proc. SACMAT*, 2017, pp. 183–190.

[106] F. M. Awaysheh, M. Alazab, M. Gupta, T. F. Pena, and J. C. Cabaleiro, "Next-generation big data federation access control: A reference model," 2019, *arXiv:1912.11588*. [Online]. Available: http://arxiv.org/abs/1912.11588

[107] W. Zhou and S. Piramuthu, "Security/privacy of wearable fitness tracking IoT devices," in *Proc. 9th Iberian Conf. Inf. Systems Technol. (CISTI)*, Jun. 2014, pp. 1–5.

[108] S. Siboni, A. Shabtai, N. O. Tippenhauer, J. Lee, and Y. Elovici, "Advanced security testbed framework for wearable IoT devices," *ACM Trans. Internet Technol.*, vol. 16, no. 4, pp. 1–25, Dec. 2016.

[109] M. Gupta and R. Sandhu, "The GURA$_G$ administrative model for user and group attribute assignment," in *Proc. NSS*. Springer, 2016, pp. 318–332.

[110] M. Gupta, F. Patwa, and R. Sandhu, "An attribute-based access control model for secure big data processing in Hadoop ecosystem," in *Proc. the 3rd ACM Workshop Attribute-Based Access Control (ABAC)*, 2018, pp. 13–24.

[111] M. V. Schönfeld, R. Heil, and L. Bittner, "Big data on a farm—Smart farming," *Big Data Context*, pp. 109–120, 2018.

[112] S. Alneyadi, E. Sithirasenan, and V. Muthukkumarasamy, "A survey on data leakage prevention systems," *J. Netw. Comput. Appl.*, vol. 62, pp. 137–152, Feb. 2016.

[113] Z. A. Baig, P. Szewczyk, C. Valli, P. Rabadia, P. Hannay, M. Chernyshev, M. Johnstone, P. Kerai, A. Ibrahim, K. Sansurooah, N. Syed, and M. Peacock, "Future challenges for smart cities: Cyber-security and digital forensics," *Digit. Invest.*, vol. 22, pp. 3–13, Sep. 2017.
[114] J. Saxe and K. Berlin, "Deep neural network based malware detection using two dimensional binary program features," in *Proc. 10th Int. Conf. Malicious Unwanted Softw. (MALWARE)*, Oct. 2015, pp. 11–20.
[115] J. Demme, M. Maycock, J. Schmitz, A. Tang, A. Waksman, S. Sethumadhavan, and S. Stolfo, "On the feasibility of online malware detection with performance counters," *ACM SIGARCH Comput. Archit. News*, vol. 41, no. 3, p. 559, Jul. 2013.
[116] A. Shabtai, R. Moskovitch, Y. Elovici, and C. Glezer, "Detection of malicious code by applying machine learning classifiers on static features: A state-of-the-art survey," *Inf. Secur. Tech. Rep.*, vol. 14, no. 1, pp. 16–29, Feb. 2009.
[117] M. R. Watson, N.-U.-U. Shirazi, A. K. Marnerides, A. Mauthe, and D. Hutchison, "Malware detection in cloud computing infrastructures," *IEEE Trans. Depend. Sec. Comput.*, vol. 13, no. 2, pp. 192–205, Apr. 2016.
[118] H. E. Merabet and A. Hajraoui, "A survey of malware detection techniques based on machine learning," *Int. J. Adv. Comput. Sci. Appl.*, vol. 10, no. 1, pp. 366–373, 2019.
[119] M. Abdelsalam, R. Krishnan, and R. Sandhu, "Online malware detection in cloud auto-scaling systems using shallow convolutional neural networks," in *Proc. IFIP Annu. Conf. Data Appl. Secur. Privacy* Cham, Switzerland: Springer, 2019, pp. 381–397.
[120] M. Abdelsalam, R. Krishnan, Y. Huang, and R. Sandhu, "Malware detection in cloud infrastructures using convolutional neural networks," in *Proc. IEEE 11th Int. Conf. Cloud Comput. (CLOUD)*, Jul. 2018, pp. 162–169.
[121] M. Abdelsalam, R. Krishnan, and R. Sandhu, "Clustering-based IaaS cloud monitoring," in *Proc. IEEE 10th Int. Conf. Cloud Comput. (CLOUD)*, Jun. 2017, pp. 672–679.
[122] V. Chandola, A. Banerjee, and V. Kumar, "Anomaly detection: A survey," *ACM Comput. Surv.*, vol. 41, no. 3, p. 15, 2009.
[123] C. Wang, V. Talwar, K. Schwan, and P. Ranganathan, "Online detection of utility cloud anomalies using metric distributions," in *Proc. IEEE Netw. Oper. Manage. Symp. (NOMS)*, 2010, pp. 96–103.
[124] C. Wang, K. Viswanathan, L. Choudur, V. Talwar, W. Satterfield, and K. Schwan, "Statistical techniques for online anomaly detection in data centers," in *Proc. 12th IFIP/IEEE Int. Symp. Integr. Netw. Manage. (IM) Workshops*, May 2011, pp. 385–392.
[125] F. Azmandian, M. Moffie, M. Alshawabkeh, J. Dy, J. Aslam, and D. Kaeli, "Virtual machine monitor-based lightweight intrusion detection," *ACM SIGOPS Oper. Syst. Rev.*, vol. 45, no. 2, pp. 38–53, Jul. 2011.
[126] S. Mittal, P. K. Das, V. Mulwad, A. Joshi, and T. Finin, "CyberTwitter: Using Twitter to generate alerts for cybersecurity threats and vulnerabilities," in *Proc. IEEE/ACM Int. Conf. Adv. Social Netw. Anal. Mining (ASONAM)*, Aug. 2016, pp. 860–867.
[127] A. Piplai, S. Mittal, A. Joshi, T. Finin, J. Holt, and R. Zak, "Creating cybersecurity knowledge graphs from malware after action reports," Univ. Maryland Baltimore County, Baltimore, MD, USA, Tech. Rep., Nov. 2019.
[128] S. Mittal, A. Joshi, and T. Finin, "Thinking, fast and slow: Combining vector spaces and knowledge graphs," 2017, *arXiv:1708.03310*. [Online]. Available: http://arxiv.org/abs/1708.03310
[129] L. Neil, S. Mittal, and A. Joshi, "Mining threat intelligence about open-source projects and libraries from code repository issues and bug reports," in *Proc. IEEE Int. Conf. Intell. Secur. Inform. (ISI)*, Nov. 2018, pp. 7–12.
[130] S. Khorsandroo and A. S. Tosun, "Time inference attacks on software defined networks: Challenges and countermeasures," in *Proc. IEEE 11th Int. Conf. Cloud Comput. (CLOUD)*, Jul. 2018, pp. 342–349.
[131] S. Khorsandroo and A. S. Tosun, "An experimental investigation of SDN controller live migration in virtual data centers," in *Proc. IEEE Conf. Netw. Function Virtualization Softw. Defined Netw. (NFV-SDN)*, Nov. 2017, pp. 309–314.
[132] S. Khorsandroo and A. Saman Tosun, "White box analysis at the service of low rate saturation attacks on virtual SDN data plane," in *Proc. IEEE 44th LCN Symp. Emerg. Topics Netw. (LCN Symposium)*, Oct. 2019, pp. 100–107.
[133] K. Joshi, K. P. Joshi, and S. Mittal, "A semantic approach for automating knowledge in policies of cyber insurance services," in *Proc. IEEE Int. Conf. Web Services (ICWS)*, Jul. 2019, pp. 33–40.
[134] K. P. Joshi, A. Gupta, S. Mittal, C. Pearce, and T. Finin, "Alda: Cognitive assistant for legal document analytics," in *Proc. AAAI Fall Symp. Ser.*, 2016, pp. 149–152.
[135] S. Mittal, K. P. Joshi, C. Pearce, and A. Joshi, "Automatic extraction of metrics from SLAs for cloud service management," in *Proc. IEEE Int. Conf. Cloud Eng. (IC2E)*, Apr. 2016, pp. 139–142.
[136] K. P. Joshi, A. Gupta, S. Mittal, C. Pearce, A. Joshi, and T. Finin, "Semantic approach to automating management of big data privacy policies," in *Proc. IEEE Int. Conf. Big Data (Big Data)*, Dec. 2016, pp. 482–491.

MAANAK GUPTA received the B.Tech. degree in computer science and engineering from Kuruskhetra University, India, the M.S. degree in information systems from Northeastern University, Boston, and the M.S. and Ph.D. degrees in computer science from The University of Texas at San Antonio (UTSA). He has worked as a Postdoctoral Fellow with the Institute for Cyber Security (ICS), UTSA. He is currently an Assistant Professor in computer science with Tennessee Technological University, Cookeville, TN, USA. His primary area of research includes security and privacy in cyber space focused in studying foundational aspects of access control and there application in technologies, including cyber physical systems and cloud computing. He is also interested in malware analysis and AI assisted cyber security solutions. He is a Reviewer and a Technical Committee Member for several IEEE journals and conferences.

MAHMOUD ABDELSALAM received the B.Sc. degree from the Arab Academy for Science and Technology and Maritime Transportation (AASTMT), in 2013, and the M.Sc. and Ph.D. degrees from the University of Texas at San Antonio (UTSA), in 2017 and 2018, respectively. He was working as a Postdoctoral Research Fellow with the Institute for Cyber Security (ICS), UTSA. He is currently an Assistant Professor with the Department of Computer Science, Manhattan College. His research interests include computer systems security, anomaly and malware detection, cloud computing security and monitoring, cyber physical systems security, and applied machine learning.

SAJAD KHORSANDROO received the B.S. degree in computer engineering from the University of Applied Science and Technology, Iran, in 2006, the M.S. degree from the University of Malaya, Malaysia, in 2013, and the Ph.D. degree from the University of Texas at San Antonio, in 2019. He joined the School of Information, University of California Berkeley, and the Department of Computer Science, North Carolina A&T State University, in 2019. He is currently a Lecturer with the School of Information, University of California Berkeley, and an Assistant Professor with the Department of Computer Science, North Carolina A&T State University. His research interests include cyber security, cloud computing, and software defined networks.

SUDIP MITTAL received the B.Tech. and M.Tech. degrees in computer science from IIIT Delhi, and the Ph.D. degree in computer science from the University of Maryland–Baltimore County. He has worked with the Accelerating Cognitive Cyber Security Research Laboratory (ACCL), the Ebiquity Research Lab, the Center for Hybrid Multicore Productivity Research (CHMPR), and the Cybersecurity Education and Research Centre (CERC@IIITD). His goal is to develop the next generation of cyber defense systems that help protect various organizations and people. He is currently an Assistant Professor of computer science with the University of North Carolina Wilmington (UNCW). His primary research interests are cybersecurity and artificial intelligence.