IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received January 17, 2020, accepted February 7, 2020, date of publication February 11, 2020, date of current version February 24, 2020.

Digital Object Identifier 10.1109/ACCESS.2020.2973178

Security and Privacy for Green IoT-Based Agriculture: Review, Blockchain Solutions, and Challenges

MOHAMED AMINE FERRAG[1], LEI SHU[2,3], (Senior Member, IEEE), XING YANG[2], ABDELOUAHID DERHAB[4], AND LEANDROS MAGLARAS[5], (Senior Member, IEEE)

[1]Department of Computer Science, University of Guelma, Guelma 24000, Algeria
[2]College of Engineering, Nanjing Agricultural University, Nanjing 210013 , China
[3]School of Engineering, University of Lincoln, Lincoln LN6 7T, U.K.
[4]Center of Excellence in Information Assurance (CoEIA), King Saud University, Riyadh 11451, Saudi Arabia
[5]School of Computer Science and Informatics, De Montfort University, Leicester LE1 9BH, U.K.

Corresponding author: Lei Shu (lei.shu@ieee.org)

This work was supported by the NAU-Lincoln Joint Research Center of Intelligent Engineering, Nanjing Agricultural University, Nanjing, China.

ABSTRACT This paper presents research challenges on security and privacy issues in the field of green IoT-based agriculture. We start by describing a four-tier green IoT-based agriculture architecture and summarizing the existing surveys that deal with smart agriculture. Then, we provide a classification of threat models against green IoT-based agriculture into five categories, including, attacks against privacy, authentication, confidentiality, availability, and integrity properties. Moreover, we provide a taxonomy and a side-by-side comparison of the state-of-the-art methods toward secure and privacy-preserving technologies for IoT applications and how they will be adapted for green IoT-based agriculture. In addition, we analyze the privacy-oriented blockchain-based solutions as well as consensus algorithms for IoT applications and how they will be adapted for green IoT-based agriculture. Based on the current survey, we highlight open research challenges and discuss possible future research directions in the security and privacy of green IoT-based agriculture.

INDEX TERMS Security, privacy, authentication, blockchain, smart agriculture, greenhouse.

I. INTRODUCTION

The Internet of Things (IoT) has been applied in many areas, such as smart farming [1], smart home [2], wearables [3], smart city [4], connected health [5], connected car [6], connected drones [7], among other areas. The IoT allows physical objects to communicate together, share information and coordinate decisions. The IoT transforms traditional objects into intelligent objects by exploiting its enabling technologies such as communication technologies, Internet protocols, application, and sensor networks [8], [9].

The global smart agriculture market is expected to reach $15.3 billion by the end of 2025 compared to $5 billion in the year 2016 [10]. Smart agriculture will become an important IoT application area in agri-products exporting countries. Recently, the IoT application has been deployed for smart agriculture using wireless sensor networks (WSNs) such as irrigation sensor network [11], prediction of frost events [12], precision soil farming [13], blind entity identification [14], smart farming [15], and precision agriculture [16].

To develop a green IoT-based agriculture solution, there are six main challenges, including, hardware, data analytics, maintenance, mobility, infrastructure, data security, and privacy [17]. The hardware challenges concern the choice of sensors and meters for IoT devices. Therefore, there are various kinds of sensors types that can be used in IoT application (e.g., temperature sensor, proximity sensor, pressure sensor, water quality sensor, chemical sensor, gas sensor, humidity sensor...etc.). The data analytics challenge concern the application of predictive algorithms and machine learning (e.g., deep learning approaches) in IoT data to obtain a nutritive solution for smart agriculture. The maintenance challenge concerns regular sensors checks of all IoT devices since they can be easily damaged in the agriculture field. The mobility

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

TABLE 1. Related surveys on green IoT-based agriculture.

Year	Author	Main focus/contributions
2017	Brewster et al. [20]	A review on developing IoT-based large-scale pilots in agriculture
2017	Ray [21]	A systematic survey that covers the IoT deployment for improved farming
2017	Tzounis et al. [38]	Review of embedded platforms and technologies in agriculture along with the main agriculture applications
2018	Elijah et al. [9]	An overview and detailed investigation of IoT and data analytics in agriculture
2019	Khanna and Kaur [22]	Fundamental structures of IoT and its impact in the field of precision agriculture
2019	Ruan et al. [23]	A brief survey on the applications of green IoT-based agriculture

challenge concerns the type of wireless communication (e.g., 4G, 5G, WiFi, 6LowPan, LoRa) that can connect sensors distributed over a large area in the agriculture field. The infrastructure challenges concern the installation and development of IoT networking architecture using new technologies such as fog computing, cloud computing, network virtualization...etc. The main problem in the development of green IoT-based agriculture is not located at the physical support but mainly in reassuring both security and privacy. With the adaption of green IoT-based agriculture, an adversary may find more ways to penetrate into the system (e.g., via a false data injection attack), raising new security and privacy issues and asking for more secure communications in the smart agriculture filed.

According to Cha *et al.* [18], privacy-enhancing technologies in IoT application can be classified into seven categories, including, enforcement, control over data, personal data protection, anonymization or pseudonymization, partial data disclosure, anonymous authorization, and holistic privacy preservation. Therefore, security requirements [19] in IoT application can be classified into authentication, confidentiality, non-repudiation, integrity, and access control. These security and privacy requirements should be achieved by the security protocols for green IoT-based agriculture.

There are related survey papers [9], [20]–[23] that focused on various aspects of IoT-based agriculture, as presented in Tab. 1. Brewster *et al.* [20] presented a review on developing IoT-based large-scale pilots in agriculture. Ray [21] presented a systematic survey that covers the IoT deployment for improved farming. Recently, the surveys [22], [23] discussed the fundamental structures of IoT and its impact in the field of green IoT-based agriculture. However, these surveys are very limited regarding research challenges on security and privacy.

In the literature, there are different related surveys that deal with IoT security. As shown in Table 2, we classify the IoT security surveys with respect to the following criteria:

- *Threat model:* It indicates whether the survey considered the threats against the IoT network.
- *Security & Privacy:* It indicates whether the survey focused considered the security and privacy countermeasures to protect the IoT network.
- *Blockchain:* It indicate whether the survey considered bloackanin-based solution for IoT security.
- *Target IoT application:* It indicates whether the survey focused on specific or general IoT applications.

Most of the IoT security surveys [24]–[31] describe the required security and privacy countermeasures and target without focusing on any particular application. Some of them restrict their covered countermeasures to IoT security taxonomy [26], IoT frameworks [27], [30], security communication protocols [24], [25], or trust-based solutions [31]. Some of the surveys describe the threat models that could comprise the security of IoT networks [26], [28], [29], [31]–[33]. Recently, blockchain-based solutions for IoT security have attracted more attention in [29], [34]–[36]. Kouicem *et al.* [35] present their security solutions and blockchain-based security solutions with respect to five IoT applications: Smart Grid, EHealth, Transportation, Smart city, and Manufacturing. Other surveys focused on industrial IoT [32], Smart Grid [37], or Smart Home [34]. To the best of our knowledge, our survey is the first that thoroughly covers threats models, secuirty and privacy countermeasures, blockchain-based solutions for IoT security, and focuses only on Green IoT-based agriculture applications.

Our contributions in this work are:

- We present a four-tier green IoT-based agriculture architecture.
- We present the threat models against green IoT-based agriculture and provide a classification into five categories, including, attacks against privacy, authentication, confidentiality, availability, and integrity properties.
- We review the security and privacy solutions for IoT applications and how they will be adapted for green IoT-based agriculture.
- We analyze the privacy-oriented blockchain-based solutions for IoT applications and how they will be adapted for green IoT-based agriculture.
- We provide the consensus algorithms for blockchain-based solutions and how they will be adapted for green IoT-based agriculture.
- We emphasize the security and privacy challenges solutions for green IoT-based agriculture.

The rest of this paper is organized as follows. Section II presents the four-tier green IoT-based agriculture architecture. In Section III, we present the threat models against green IoT-based agriculture and provide a classification into five categories. In Section IV, we provide the new trends of security and privacy solutions for green IoT-based agriculture. In Section V, we clearly highlight the pros and cons of the existing privacy-oriented blockchain-based solutions. Then, we discuss the security and privacy challenges solutions in Section VI. Lastly, Section VII presents conclusions.

TABLE 2. Related surveys on IoT security.

Reference	Threat model	Security & Privacy	Blockchain	Target IoT application
Nguyen et al. (2015) [24]	NO	Security communication protocols	NO	General
Granjal et al. (2015) [25]	NO	Security communication protocols	NO	General
Sadeghi et al. (2015) [32]	YES	YES	NO	Industrial IoT
Dalipi et al. (2016) [37]	NO	YES	NO	Smart Grid
Alab et al. (2017) [26]	YES	IoT security Taxonomy	NO	General
Baig et al. (2017) [33]	YES	NO	NO	Smart city
Lin et al. (2017) [27]	NO	IoT frameworks	NO	General
Yang et al. (2017) [28]	YES	YES	NO	General
Dorri et al. (2017) [34]	NO	NO	YES	Smart Home
Kouicem et al. (2018) [35]	NO	YES	YES	Smart Grid EHealth Transportation system Smart city Manufacturing
Khan and Salan (2018) [29]	YES	YES	YES	General
Ammar et al. (2018) [30]	NO	IoT frameworks	NO	General
Panarello et al. (2018) [36]	NO	NO	YES	General
Ferrag et al. (2019) [39]	NO	NO	YES	General
Altaf et al. (2019) [31]	YES	Trust-based	NO	General
Our survey	YES	YES	YES	Green IoT-based agriculture

II. GREEN IoT-BASED AGRICULTURE

Smart agriculture based on IoT technology has enabled farmers to improve crop yields, optimize irrigation efficiency, and reduce farming costs. It is an intelligent agricultural solution combining agriculture with modern information technology. The IoT technology has contributed to the emergence of the three aspects:

- *Precision agriculture :* is a technology which uses advanced technology to improve crop yield, among them, Wireless Sensor Network (WSN) is the main driver for the development of it [40]. It effectively reduces the potential risks in the production process and helps farmers making accurate and controlled farming practices by deploying a large number of low-power, multi-function, wireless communication sensors in environments (such as fields and open poultry and livestock breeding) and collecting relevant data in agricultural production (such as environment data, crop growth data, livestock health data [41]–[44]).
  The main modern information technology used in precision agriculture is "3S" technology, including Remote Sensing (RS), Geographic Information System (GIS) and Global Positioning System (GPS). The most remarkable application of GPS in precision agriculture is agricultural drones, they are used in the agriculture industry to enhance the different farming practices [45]. The ground and aerial drones are used for assessment of crop health, crop monitoring, planting, crop spraying, and field analysis. Furthermore, with the integration of IoT and "3S" technology in open poultry and livestock breeding, it is possible to collection information about the location and health of cattle by attaching sensors to them, which allows to identify sick cattle and isolated them. The farmers can also reduce time and effort needed to locate their animals [46]. Generally, Precision agriculture constructs an expert decision system for agriculture production management to replace the subjective traditional agricultural production management method, thereby, (1) reasonable using of pesticides to reduce environmental pollution; (2) improving the efficiency of agricultural irrigation and reducing the waste of resources; (3) Planting crops in an environment suitable for their growth, improving the land usage; (4) analyzing the growth law of crops and livestock, maintaining their best growth state and greatly improving the output and quality of agricultural products.
- *Facility agriculture :* is an industrialized agricultural production mode that aims at good quality and high yield, belongs to a high-input, high-output, capital-intensive, technology-intensive and labor-intensive industry [47]. It provides a crop production protection facility created by engineering technology to achieve the goal that agricultural production is not restricted by environmental factors and automatic and efficient; frees traditional agriculture from the shackles of nature; breaks the seasonal characteristics of traditional agricultural products; meets the multi-level consumption demand derived from social development [48]. Facility agriculture can be divided into facility horticulture and farming in terms of types, they mainly use biotechnology, engineering, meteorological environment, IoT, computer technology and other technologies. Its core lies in the prediction model and decision management control system based on the historical data collected by IoT sensors.
  Facility agriculture has become a mainstay industry in some developed countries such as America, Netherlands and Japan, the most prominent example is the intelligent greenhouse. IoT sensors can be used to automatically monitor and control the internal climate parameters of

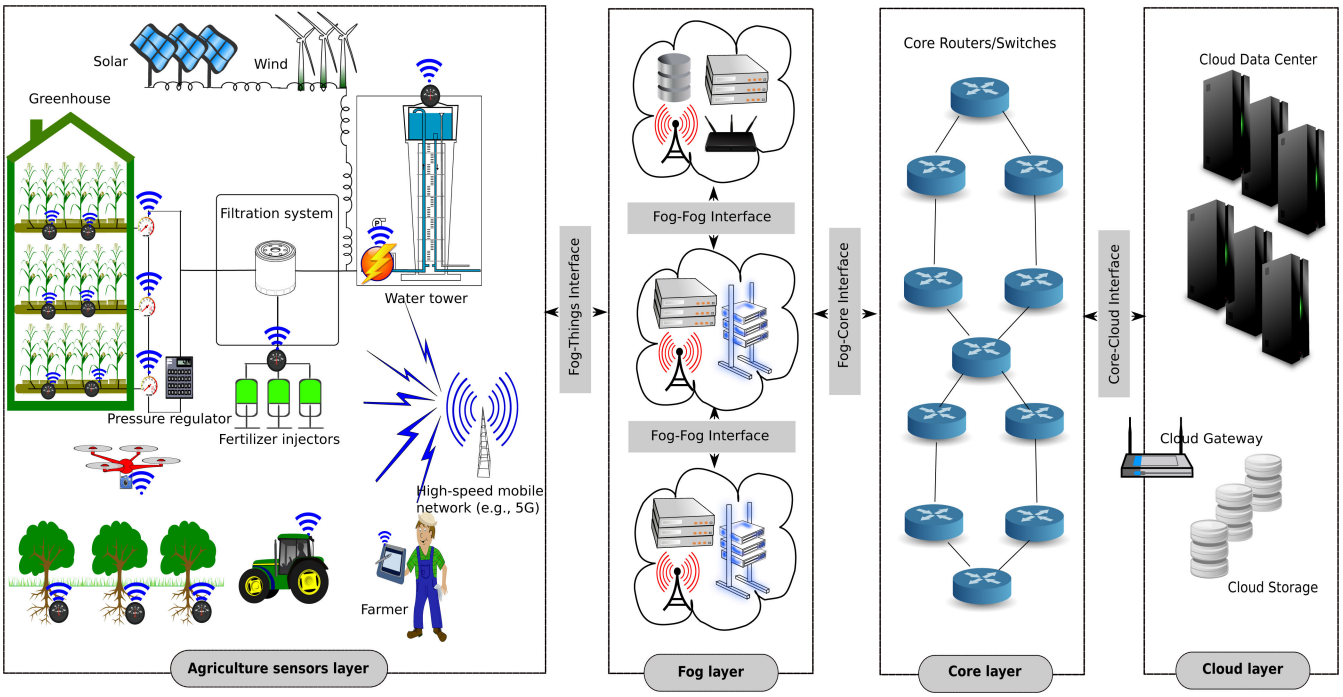


FIGURE 1. Four-tier green IoT-based agriculture architecture.

the greenhouse [49]. The sensors collect and transmit real-time data to the farmer. If the values of parameters deviate from normal condition, some actions like automatic irrigation can be performed without, which helps in reducing the labor cost as no human intervention is needed. Aquaculture, poultry and livestock farming are similar with it, the difference is different environment factors require deployment of different IoT sensors and set up specific computer control cultivation schemes. The current development goal of facility agriculture is intelligent plant factory, it enables continuous and efficient crop production under fully enclosed and intelligent control conditions. Moreover, it frees crop growth from geographical constraints, shortens the production cycle of agricultural products and improves product quality and yield. It is one of the symbols of the combination of agriculture and industry, and also the development direction of agriculture in the future.

- *Contract farming :* is a new model of agricultural production and management. With the advancement of Urbanization in the world, the gap between rural and urban development is gradually widening. According to the statistics, 80% of the extreme poor and 75% of the moderate poor live in rural areas [50]. Relatively backward agricultural infrastructure, hidden dangers in the quality and safety of agricultural products and information isolation in agricultural products trading are the main reasons. To solve these problems, contract farming emerges as the times require. It outsources the production demand of some agricultural products to farmers in advance through customers, reduces the planting and breeding risks of growers and avoid blind production, is an effective market-oriented production and marketing model [51].
  Contract farming includes supply chain management of agricultural products, traceability of agricultural products safety, agricultural products trading system, agricultural products logistics and the like. The IoT technology has been used in tracking the food supply chain (i.e., farm-to-fork traceability) [52]. For example, it has been employed to provide information about the product to the final consumer [53]. An IoT framework is proposed in [] to assess the freshness of fruits in e-commerce deliveries. In [54], IoT is used to monitor food safety throughout the product life cycle, in order to help consumers in making better purchase decisions. In [55], an early-warning system, which monitors food safety and warns about deterioration of product quality, is proposed. An IoT-based monitoring system is developed in [56] to provide geo-location information about food storage and transportation.

Fig. 1 illustrates the four-tier green IoT-based agriculture architecture, which is based on the following four layers: 1) Agriculture sensors layer; 2) Fog layer; 3) Core layer; 4) and Cloud layer. The layers are discussed as follows:

A. AGRICULTURE SENSORS LAYER

This layer consists of IoT-enabled devices (e.g., sensor nodes, smartphones, ...etc.) equipped with Global Positioning System for creating different types IoTs for smart agriculture,

including, IoTs for field agriculture, IoTs for the greenhouse, IoTs for the photovoltaic farm, IoTs for the solar insecticidal lamp, and others. Therefore, the integration and adaptation of IoT devices into various levels of agriculture aim to provide two goals. The first goal is to provide the reliability of manufacture as well as the distribution of the nutrient solution. The second goal is to provide better control in term of consumption, which gives the costs low and reduces losses in term of solution. In addition to the economic impact, the environmental impact will be significantly reduced. The farmer in the green IoT-based agriculture uses a digital control system (e.g., Supervisory Control And Data Acquisition (SCADA)) for process control to meet agriculture control requirements.

To integrate IoTs for greenhouse, we propose the sensor and meters nodes for each equipment as follows:

- IoT devices for the water pumping system which takes into consideration the surfaces to be irrigated, the pressures to be expected, and the flow rates of drippers.
- Water meters for water storage in order to show real-time updates.
- IoT devices adapted for each filtering equipment (e.g., sand filter) which takes into consideration the physical properties of water as well as drippers.
- Fertilizers meters for the storage and injectors of fertilizers (e.g., NPK fertilizers) in order to provide real-time updates.
- IoT devices for controlling the pH and electrical conductivity to meet the desired value in term of nutrient solution.
- Small solar panels with IoT sensors for controlling moisture levels and temperature.

These IoT devices and meters communicate via 5G cellular and satellite communication networks with the fog computing layer.

B. FOG COMPUTING LAYER

Since some agriculture IoT data need to be processed closer to IoT devices and meters, the fog computing layer is proposed especially for this task, which can significantly reduce the processing time. This layer is also termed as Edge computing layer. The fog nodes receive agriculture IoT data via geo-distributed devices that are managed in a distributed network, including, access points, gateway, router, and switch. The fog computing layer provides several advantages, such as reduces the traffic overhead and reinforcement of agriculture IoT data security [57]. Therefore, there are three hierarchical architectures [58] that can be used for fog computing layer in the green IoT-based agriculture. The first hierarchical architecture is three-tier (including, Tier 1-Things/End Devices, Tier 2-Fog, Tier 2-Cloud), which is the basic architecture of fog computing. The second hierarchical architecture is four-tier combined fog-cloud architecture [59]. The last hierarchical architecture is based on Software-Defined Networking (SDN) [60].

For example in the IoT use case in greenhouse, the nutrient solution can be processed and calculated at the fog computing layer. This nutrient solution uses the IoT data (e.g., the composition of water, temperature, and humidity) captured from the agriculture sensors layer.

C. CORE NETWORK LAYER

The core layer is responsible for the transport of data over green IoT-based agriculture from fog computing layer to cloud computing layer. This layer is also termed as the foundation or backbone network. To ensure that packets are securely routed over the network, the core layer includes high-speed cables (e.g., fiber optic cables) and high-end switches (e.g., Cisco switches 12000) [61]. In addition, the core network layer is responsible for routing by delivering a strategies-based network interconnection such as strategy of QoS, strategy of control broadcast and multicast...etc.

D. CLOUD COMPUTING LAYER

This layer is a centralized system consists of data centers and traditional cloud servers, which they have sufficient computing resources and sufficient storage. The cloud computing layer is responsible for delivering storage, data access, and synchronization [62].

III. THREAT MODELS

Generally, the classification of attacks for IoT application is done using the following two criteria: 1) Internal or external and 2) Passive or active, as discussed in [19]. Therefore, according to the property that the attack trying to compromise nodes in green IoT-based agriculture (i.e., IoT devices, Fog nodes, and Cloud nodes), we classify the threat models into the following five main categories, attacks against privacy, authentication, confidentiality, availability, and integrity properties, as presented in Fig. 2.

A. ATTACKS AGAINST PRIVACY

This category of attacks is based on learning the precise location and identity of IoT devices at agriculture sensors layer to get privacy data and compromise the privacy of the system. In green IoT-based agriculture, the IoT data (e.g., the composition of water, temperature, and humidity) is collected multiple times per hour by IoT devices and smart meters at agriculture sensors layer to obtain fine-grained information about the plants status and improve nutrient solution efficiency. The detailed analysis of this IoT data may easily reveal farmers' physical activities and the nutrient solution adopted. For example, in pH settings, if the pH rises excessively indicates that the farmer will increase the ammonium supply, and if the pH falls indicates that the farmer will reduce the ammonium supply. Using this information, an adversary can plan physical attacks (e.g., sending a drone) to disrupt pH settings. Obviously, this private information (i.e. pH settings) must be protected from unauthorized access.

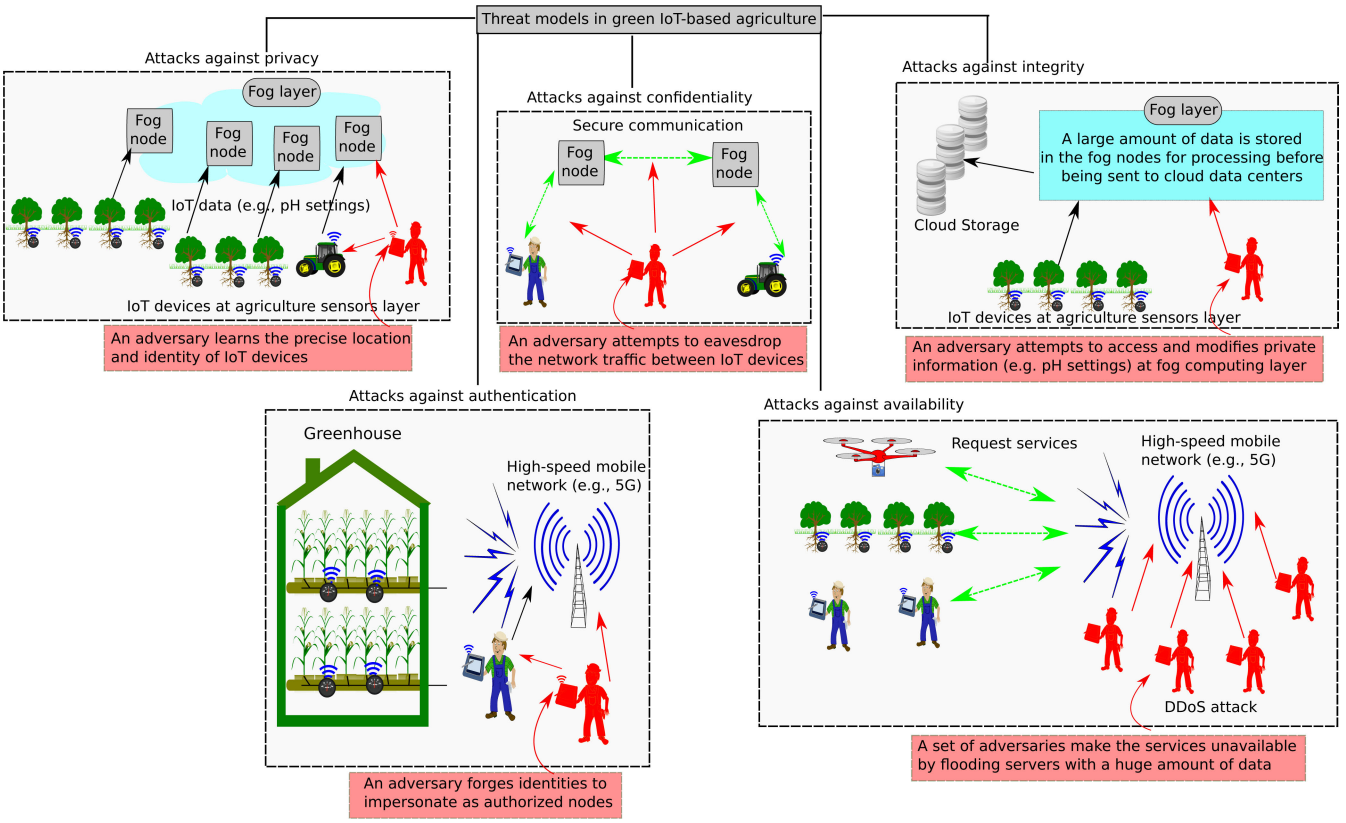


FIGURE 2. Threat models in green IoT-based agriculture.

B. ATTACKS AGAINST AUTHENTICATION

This category of attacks forges identities to impersonate as authorized nodes (i.e., IoT device, fog node, or cloud node) in order to gain access to the green IoT-based agriculture. For example, an adversary may lunch the following identity-based attacks for forge identities, namely, replay attack, masquerade attack, spoofing attack, and impersonation attack.

- A *replay attack* takes place in the form of man-in-the-middle attack (MITM). Its objectives in the green IoT-based agriculture are to intercepting data packets between IoT devices or an IoT device with an access point at agriculture sensors layer and then relaying them to their destinations without modification. The authentication protocols for securing IoT networks use three techniques against replay attacks, namely, pairing-based cryptography, hash functions, and timestamp in the encrypted data, as discussed in [19].
- A *masquerade attack* aims to masquerade as a legitimate node to log into the server at agriculture sensors layer (i.e., log into the access point) or fog computing layer (i.e., log into the fog node). The authentication protocols for securing IoT networks use three techniques against masquerade attacks, namely, 1) behavioral features-based biometric (e.g., keystroke, signature, gait, or voice), 2) human physiological-based biometric (e.g., fingerprint palm, electrocardiogram, eyes, or face), 3) hashing functions, 4) Elliptic curve cryptosystem, and 5) pairing-based cryptography [63].

C. ATTACKS AGAINST CONFIDENTIALITY

This category of attacks attempts to adversarially eavesdrop the network traffic between IoT devices or an IoT device with an access point at agriculture sensors layer so as to mislead the green IoT-based agriculture to compromise the confidentiality and make wrong decisions/actions. For example, an adversary may lunch the following Eavesdropping-based attacks to compromise the confidentiality, including, tracing attack, brute force attack, and known-key attack.

- A *tracing attack* aims to collect enough privacy information from IoT devices at agriculture sensors layer to link data with a particular real identity. To resist this attack, security solutions based on random numbers in commitments and proofs ought to be developed [64].
- A *brute force attack* aims to produce a list of all possible passwords that can be used by IoT devices at agriculture sensors layer, then to exhaust them one by one until the correct password can be identified [65].
- A *known-key attack* aims to generate new session keys based on compromising past session keys. To resist this attack, security solutions that integrate random nonce in session key ought to be developed.

D. ATTACKS AGAINST AVAILABILITY

This category takes the form of Denial of Service (DoS) attacks. Its goals are to make the services in green IoT-based agriculture (e.g., authentication for IoT devices) are unavailable either by (1) flooding servers with a huge amount of data to make it busy and unable to provide a service to IoT devices; (2) updating with false data injection attacks; or (3) attack on accurate localization for UAV with a malicious 5G station.

E. ATTACKS AGAINST INTEGRITY

This category of attacks implies an unauthorized party to accessing and modifying private information (e.g. pH settings). Under this category, we can find the following attacks: forgery attack, man-in-the-middle (MITM) attack, biometric template attack, and trojan horse attack. To resist this attack, the data aggregation schemes based on homomorphic encryption and hash functions ought to be developed.

IV. SECURITY AND PRIVACY SOLUTIONS

Table 3 summarizes research for security and privacy solutions for IoT applications and how they will be adapted for green IoT-based agriculture.

A. PRIVACY-PRESERVING SOLUTIONS

1) PRIVACY-PRESERVING DATA AGGREGATION

During running the aggregation at the network edge in green IoT-based agriculture, the fog devices cannot see each green product data. The privacy-preserving data aggregation solution is very important to protect each green IoT device's data. To resist against inject false data, Lu *et al.* [70] proposed a lightweight privacy-preserving data aggregation solution, named LDPA, for IoT applications, which can be applied in green IoT-based agriculture. The LDPA combines three cryptographic techniques, namely, the homomorphic Paillier encryption Chinese Remainder Theorem, and one-way hash chain. The Chinese remainder theorem is used by the control center for computing the mean and variance after collecting, aggregating, and forwarding IoT devices' data from the network edge to the control center. The homomorphic Paillier encryption is used for encryption the report of each sensing data from each IoT device. The one-way hash chain technique is used for achieving lightweight authentication among IoT devices. Therefore, the LDPA solution can resist against the false data injection since the one-way hash chain technique as well as the time slot are adapted in authentication phase between the fog device and IoT device. In addition, the LDPA solution can achieve differential privacy since some noises are added in the aggregated data.

Guan *et al.* [75] introduced an anonymous and privacy-preserving data aggregation protocol, named APPA, for IoT application. The system model considers Fog-enhanced IoT, which contains three layers, namely, the lower layer (smart devices), middle layer (Fog nodes), and Upper layer (Cloud Computing). To archives anonymity and unforgeability, the APPA protocol uses two cryptographic techniques, namely, signature-of-knowledge and paillier cryptosystem. The APPA protocol can resist eavesdropping attack and false data injection attack, but the availability is not considered.

2) LOCATION PRIVACY

Location-based services (LBS) in green IoT-based agriculture will have a very important area for research with the rapid development of smart agriculture. Therefore, an adversary can track IoT devices in smart agriculture, which may cause problems of loss of privacy. Sun *et al.* [69] proposed a location privacy algorithm for IoT application, which can be adapted for green IoT-based agriculture. To protect location privacy, the study uses a dummy location privacy algorithm, which consists of finding an optimal set of dummy locations using a greedy approach. The proposed algorithm can resist two attacks categories, namely, inference attacks and colluding attacks, but the data integrity and authentication are not considered.

3) CONTENT-ORIENTED PROTECTION

The content-oriented protection solution is very important against the violation of a farmer's privacy when different IoT data are collected and combined from agriculture sensors layer. Gai *et al.* [72] proposed a dynamic privacy protection model, named DPP, for ensuring mobile device user privacy in IoT application. The idea of DPP model is based on the classification of the privacy protection levels. Specifically, the DPP model uses three main phases, including, (1) security classifications for the definition of the privacy weight; (2) content-oriented data pairs identification of content-oriented data pairs based on the security classifications; and (3) the input data table. The evaluation performance in term of plan generation and timing constraints show that the DPP's average time consumption is 1.2% shorter than other related works.

4) ANONYMITY

One of the important security properties in green IoT-based agriculture is strong anonymity, which means that except for the fog nodes, the agriculture IoT data identity cannot be revealed. The CPAL solution proposed by Lai *et al.* [66] archives user anonymity in IoT application using the hybrid linear combination encryption. The CPAL solution defined the privacy-preservation with three levels, including, authorized anonymous user linking, anonymity, and authentication. Therefore, the CPAL solution can be adapted for green IoT-based agriculture by applying the hybrid linear combination encryption between the IoT devices communications at agriculture sensors layer. In addition, the CPAL solution is robust against impersonation attack and DoS attack.

5) PRIVACY-PRESERVING TRUST EVALUATION

Privacy-preserving trust evaluation is an important role to ensures trust relationships among green IoT-based agriculture entities. Yan *et al.* [68] proposed two schemes of privacy-preserving trust evaluation that can be adapted for green

TABLE 3. Summary of security and privacy solutions for IoT applications and how they will be adapted for green IoT-based agriculture.

Solution	Year	Network model	Threat models	Countermeasures	Performance (+) and Limitation (-)	How can be adapted for green IoT-based agriculture
Lai et al. [66]	2014	Roaming network architecture	- Impersonation attack - DoS attack	- Hybrid linear combination encryption - Hash function	+ Authorized anonymous user linking, anonymity, and authentication - Location tracking attack	- Applying the hybrid linear combination encryption between the IoT devices communications at agriculture sensors layer
Yao et al. [67]	2015	The network model consists of group of IoT devices with a control center	- Chosen plaintext attack - Attribute-set attack	- Lagrange secret sharing - Elliptic curve cryptosystem - HMAC method	+ Data confidentiality with integrity - Identity and location privacy are not considered	- The message exchanged between IoT devices at agriculture sensors layer is encrypted by a secure symmetric cryptographic algorithm. In addition, the elliptic curve cryptosystem is used to derives the encryption key
Yan et al. [68]	2016	Trust management system with three entities, including, nodes, evaluation party, and authorized proxy	- Conflict behavior attack - On-off attack	- Homomorphic encryption	+ Privacy-preserving trust evaluation - False data injection attack	- Applying additive homomorphism with proxy-based re-encryption between IoT devices and an access point at agriculture sensors layer
Sun et al. [69]	2017	The network model consists of two parts, namely, the LBS server and LBS users	- Inference attacks - Colluding attacks	- Dummy-location selection algorithm	+ Location privacy - Data integrity and authentication	- Adapt a dummy-location selection algorithm at agriculture sensors layer to protect location privacy
Lu et al. [70]	2017	Fog computing-enhanced IoT contains four entities, including, a trusted authority, group of IoT devices, a fog device, and a control center	- Differential attacks - False data injection attack - Denial of Service (DoS) attacks	- Chinese remainder theorem - Homomorphic Paillier encryption - One-way hash chain	+ Resist against the false data injection attack + Achieve privacy-preserving - Availability is not considered	- Enable a fog device at fog computing layer to filter injected false data using three techniques, namely, the one-way hash chain technique, homomorphic Paillier encryption, and Chinese Remainder Theorem
Song et al. [2]	2017	The network model consists of four groups, including, home appliances (e.g., TV), sensors group, control center, and hand-held devices	- Eavesdropping attack	- Chaos-based cryptography - Message authentication codes	+ Data integrity and authentication + Key update and management - The communication between sensors group and fog device is not considered	- Access point and fog node add a MAC to the original data to verify, the integrity of the transmitted data among IoT devices
Wang et al. [71]	2017	The network model consists of a 5G system with three groups, service users, caching fog nodes, and caching server	- Disturbing attack - Ignoring attack	- Label-based authentication - Hash function	+ Ensure reliability + Data integrity - Privacy preserving is not provided	- Apply a lightweight label-based access control scheme to authenticates the fog nodes at fog computing layer
Gai et al. [72]	2018	Internet-connected devices	- Privacy leakage attack	- Optimal data alternatives algorithm	+ Content-oriented protection - Anonymity, availability, and scalability are not considered	- Modeling hardware/software conditions at the agricultural sensor layer as constraints before data transmission
Gope et al. [73]	2018	The network model consists of four entities, including, two servers (i.e., an authenticated cloud and a backend database), a reader, and an RFID-tag	- Replay attack - Forgery attack - Cloning attack - DoS attack - Location tracking attack	- Unlinkable pseudo-identity - Emergency key - One-way hash chain	+ Mutual authentication + Tag anonymity, availability, and scalability - False data injection attack and DDoS attack are not considered	- Divide the agriculture sensors layer into several RFID clusters - An RFID-tag reader is integrated with each cluster - Apply a mutual authentication between an RFID-tag and reader
Zhang et al. [74]	2018	The network consists of an IoT system with a large number of storage devices, servers, user devices, IoT gateways	N/A	- Blockchain technology - Multiple access control contracts	+ Distributed and trustworthy access control - Robustness against network attack is not provided	- Apply the following three access control contracts at agriculture sensors layer: access control contract, judge contract, and register contract
Guan et al. [75]	2019	Fog-enhanced IoT contains three layers, namely, the lower layer (smart devices), middle layer (Fog nodes), and Upper layer (Cloud Computing)	- Eavesdropping attack - False data injection attack	- Signature-of-knowledge - Paillier cryptosystem	+ Anonymity and unforgeability + Data authentication and integrity - Availability is not considered	- Adapt the pseudonym certificates for IoT devices at agriculture sensors layer in order to provide the anonymity and unforgeability
Fan et al. [76]	2019	Cloud-fog computing consists of five entities, including, a cloud service provider, fog nodes, data owners, a certificate authority, and IoT devices	- Collision attack	- Linear secret sharing scheme - Hash function	+ Revocation and data confidentiality + Verifiability - Threat model is not defined	- Deploy proxy servers at fog computing layer - Adapt the one-way anonymous key agreement protocol at agriculture sensors layer
Zhang et al. [77]	2019	IoT application with three components, including, data center, public (untrusted) clouds, and IoT devices	- Chosen ciphertext attack	- Elliptic curve cryptography - Hash function	+ Authentication, confidentiality, and integrity - The communication between fog computing and cloud computing are not considered	- Adapt the one-way (non-interactive) authentication based on the elliptic curve cryptography between IoT devices and fog nodes
Li et al. [78]	2019	IoT network model with three entities, i.e., the data owner, cloud server, and data user	- Chosen-plaintext attack - Chosen keyword-file feature level pair attack	- Searchable encryption scheme - Symmetric encryption scheme - Collision-resistant hash function	+ Trapdoor indistinguishability and index indistinguishability - False data injection attack and DDoS attack are not considered	- Adapt a searchable encryption scheme based on the following five functions: Setup, KeyGen, Store, Trapdoor, and Search
Jiang et al. [79]	2019	Traditional public key infrastructure system	- 51% attack - Sybil attack, - Eclipse attack	- Blockchain technology	+ Decentralization, non-modifiability, unforgeability, and anonymity - The communication between sensors group and fog device is not considered	- Adapting the idea of private information retrieval at agriculture sensors layer to protect IoT devices privacy

IoT-based agriculture. These two schemes use additive homomorphic encryption for providing trust evaluation. The first scheme considers that authorized proxy is a fully trusted and collusion does not exist between evaluation party and authorized proxy. The second scheme considers that authorized proxy is not fully trusted and evaluation party and authorized proxy don't collude. In both schemes, there is a trust evaluation phase, which after receiving the encrypted evidence, a node decrypts data and then evaluates the trust of the result using a trust evaluation algorithm.

6) PERSONALIZED PRIVACY

Personalized privacy consists of providing trapdoor indistinguishability and index indistinguishability. The work by Li *et al.* [78] proposed a searchable encryption scheme for personalized privacy in IoT application, which can be adapted for green IoT-based agriculture. The proposed scheme considers an IoT network model that includes three entities, i.e., the data owner, cloud server, and data user. The cloud server is used to stores and retrieves the encrypted file features, which it received the encrypted file features from the data owner. Based on the specific keyword, the data user queries the encrypted file features. The proposed scheme is proven using two challenge-response games that it satisfies trapdoor indistinguishability and index indistinguishability under chosen keyword-file feature level pair attack. Therefore, the proposed scheme can be adapted for green IoT-based agriculture by adapting a searchable encryption scheme using the following five functions: 1) Setup for performing the security parameters; 2) KeyGen for generating the private and public keys; 3) Store for creating the index table and user authorization; 4) Trapdoor for creating the trapdoor query; and 5) Search. The Setup and Store functions are run by the fog node. The KeyGen function is run by the fog node and the IoT device. The Trapdoor function is run by the IoT device. The Search function is performed interactively between the IoT device and the cloud server.

B. DATA INTEGRITY SOLUTIONS

To protect data integrity and authentication for IoT applications, Song *et al.* [2] proposed a privacy-preserving protocol that uses message authentication codes (MAC). The MAC solution is added to the original IoT data, which the sender can verify that the IoT data has not tampered during communication. This solution can be applied in green IoT-based agriculture (i.e., between a group of IoT devices and fog device) in order to protect the integrity of the green IoT device's data. Wang *et al.* [71] proposed a lightweight label-based access control scheme, named LACS, for IoT-based 5G network, which can be adapted for green IoT-based agriculture. The LACS scheme uses two parts, including, the prover (caching fog node) and the verifier (caching server). The user authentication is achieved using verifying data integrity. The label-based authentication is used against two attacks, namely, disturbing attack and ignoring attack. The performance evaluation shows that the MD5 is more efficient than the SHA-1 in the IoT environment that uses LACS scheme.

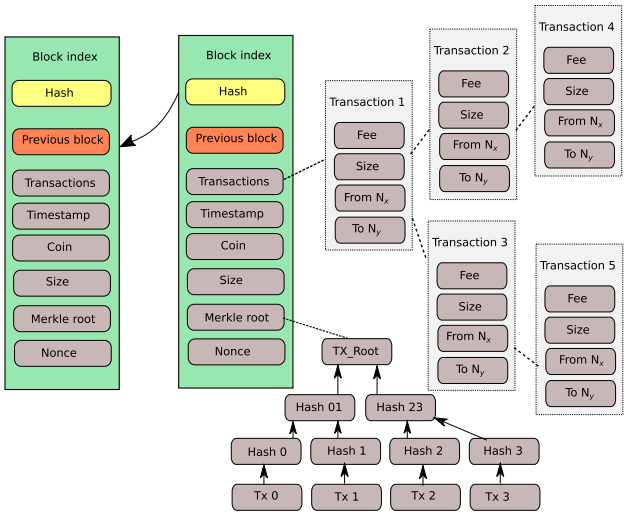


FIGURE 3. The blockchain data structure.

The work by Li *et al.* [80] can provide content integrity verification for named data networking, which can be adapted for communication among agriculture IoT nodes in green IoT-based agriculture. Specifically, the authors proposed a lightweight integrity verification architecture, named LIVE, for ensuring secure content access. The LIVE architecture uses the following three security levels: (1) Non-Cacheable; (2) 1-Cacheable; (3) All-Cacheable. To produce tokens for signature generation, the LIVE architecture uses a hash tree based signature algorithm (Merkle Hash Tree algorithm).

C. AUTHENTICATION SOLUTIONS

1) RFID AUTHENTICATION

Radio Frequency Identification (RFID) is a technology used for capturing and automatically identifying information in electronic tags. With the adaptation of RFID technology into green IoT-based agriculture, the crops will better be controlled and herd better monitored. Therefore, an unauthorized party can manage the RFID-tag, which the smart agriculture system will be compromised. Gope *et al.* [73] proposed an anonymous lightweight RFID authentication solution for IoT application. Specifically, the network model considered by the study is based on four entities, including, two servers (i.e., an authenticated cloud and a backend database), a reader, and an RFID-tag. Based on unlinkable pseudo-identity, emergency key, and hash function, the proposed solution can resist against the following five attacks: replay attack, forgery attack, cloning attack, DoS attack, and location tracking attack. In addition, this solution can achieve five security properties, namely, mutual authentication, tag anonymity, availability, and scalability, but false data injection attack, as well as DDoS attack, are not considered.

2) DELEGATED AUTHENTICATION

Since agriculture IoT data can be transported via untrusted public devices, the security solutions need to provide the delegated authentication. The work by Zhang *et al.* [77] proposed a semi-outsourcing privacy-preserving scheme, named SOPP, for the IoT data collection. The SOPP scheme considers three components, including, data center, public (untrusted) clouds, and IoT devices. To decreases the throughput and achieves a longer battery duration, the SOPP scheme applied elliptic curve cryptography as a one-way (non-interactive) authentication between untrusted public clouds and IoT devices. To block invalid access, the authentication is delegated to public clouds. The data center uses data decryption to provides data integrity.

D. ACCESS CONTROL SOLUTIONS

To supporting privacy-preserving in green IoT-based agriculture, an efficient access control scheme can be adapted. The work by Fan *et al.* [76] designed an access control protocol for fog-enabled IoT. The study considered cloud-fog computing that contains five entities, including, a cloud service provider, a group of fog nodes, a group of data owners, a certificate authority, and a group of IoT devices. For providing revocation and data confidentiality with verifiability, ciphertext-policy attribute-based encryption is adapted when an IoT device with an identifier submits a data access request.

The the blockchain technology [39] can be used for providing an access control in green IoT-based agriculture. Ouaddah *et al.* [81] proposed an access control framework, named FairAccess, for IoT application. The FairAccess framework uses the blockchain technology to get, grant, delegate, and revoke access. Zhang *et al.* [74] consider an IoT system with a large number of storage devices, servers, user devices, IoT gateways. Specifically, the study proposed an access control framework based on the Ethereum smart contract platform. This platform contains five main elements, including, smart contract, account/address, blockchain, transaction and message, and mining. To manage the policies and implement access control, the proposed framework provides functions or application binary interfaces (e.g., add new access control policy, updates the policy, returns the access result and penalty...etc.). The evaluation performance on two Raspberry Pi 3 Model B shows that the proposed framework may not be able to reflect the overhead in real-world IoT system.

E. DATA CONFIDENTIALITY SOLUTIONS

Data security in green IoT-based agriculture also includes confidentiality, which can be achieved by cipher-text based access control technique. Yao *et al.* [67] proposed a lightweight attribute-based encryption scheme for IoT application, which can be adapted for green IoT-based agriculture. To provide data confidentiality with integrity, the proposed scheme uses an elliptic curve integrated encryption scheme (ECDH). Specifically, the ECDH scheme is used for generating a sharing secret from two groups, including, the MAC key and encryption key. The performance evaluation in term of overhead (the total size of the private key, public key, and cipher-text) shows that the proposed scheme is much shorter than other related cryptographic methods that use decisional bilinear Diffie-Hellman exponent. In addition, the proposed scheme is robust against chosen plaintext and attribute-set attack.

V. PRIVACY-PRESERVING OVER BLOCKCHAIN

The blockchain technology can be effectively applied in almost all domains of IoT, including, green IoT-based agriculture [39], [82]–[85]. The application of blockchain technology for IoT is applied to provide privacy-preserving. To be specific, the blockchain is used for encrypted data sharing. Therefore, the blockchain can be used in green IoT-based agriculture as a distributed digital ledger containing all messages. This distributed ledger is replicated and stored in different IoT nodes at agriculture sensors layer, as presented in Fig. 6. Table 4 summarizes research for privacy-oriented blockchain-based solutions for IoT applications and how they will be adapted for green IoT-based agriculture. According to the characteristic of each privacy-oriented blockchain-based solution, we classify the blockchain-based solutions for green IoT-based agriculture into six categories, including, 1) Blockchain-based machine learning solution; 2) Blockchain-based distributed key management solution; 3) Blockchain-based access control solution; 4) Blockchain-based reputation and trust solution; 5) Blockchain-based authentication and identification solution, and 6) Blockchain-based secure SDN solution, as presented in Fig. 5.

A. BLOCKCHAIN-BASED SOLUTIONS

1) BLOCKCHAIN-BASED PKI SOLUTION

Jiang *et al.* [79] proposed a thin-client Authentication scheme, named PTAS, for IoT application. The PTAS scheme is applied in blockchain-based public key infrastructure (PKI). The PKI infrastructure is used to secure communication between IoT devices, which a certificate authority distribute certificates (a public key (PK) and identity (ID)) to IoT devices. To solve the problem of the single point of failure, the PTAS scheme is adapted in blockchain-based PKI. Specifically, the PTAS scheme uses the method of private information retrieval, which the identity of the user can be hidden in k indistinguishable identities. In addition, the PTAS scheme is robust against three attacks, namely, Sybil attack, eclipse attack, and 51% attack.

2) BLOCKCHAIN-BASED MACHINE LEARNING SOLUTION

The work by Shen *et al.* [91] proposed a privacy-preserving scheme, named secureSVM, for IoT application. The secureSVM scheme considers the data privacy of training support vector machine classifier (SVM) using blockchain-based encrypted IoT data. To protect the privacy of IoT data, the secureSVM scheme employs a public-key cryptosystem,

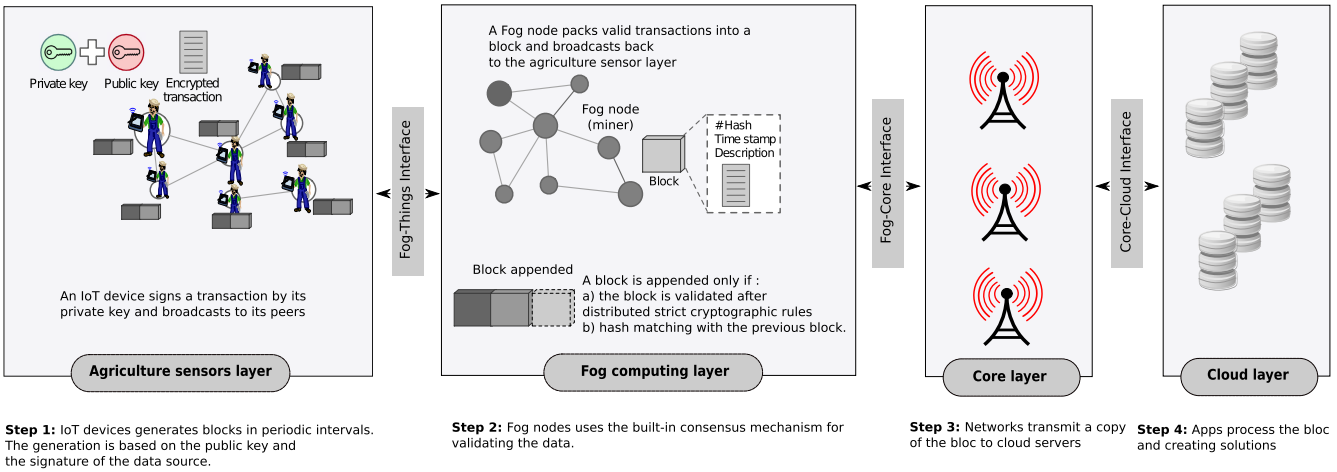


FIGURE 4. An illustration of blockchain working methodology for green IoT-based agriculture architecture.

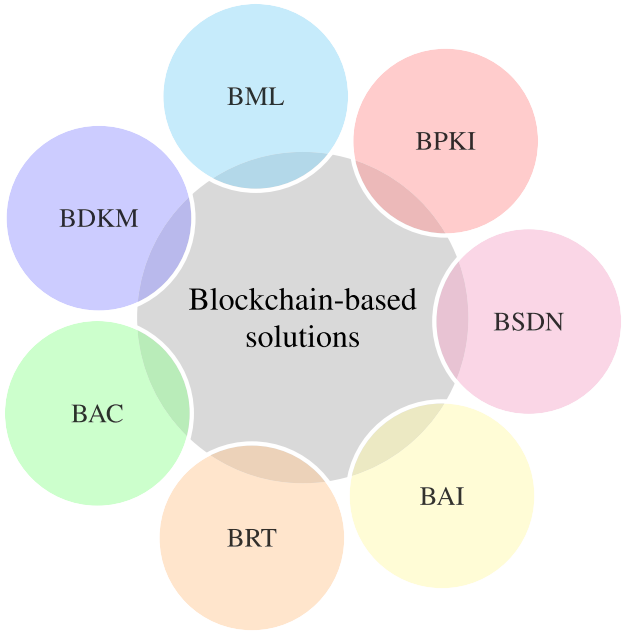


FIGURE 5. Blockchain-based solutions for green IoT-based agriculture. BPKI: Blockchain-based PKI solution; BML: Blockchain-based machine learning solution; BDKM: Blockchain-based distributed key management solution; BAC: Blockchain-based access control solution; BRT: Blockchain-based reputation and trust solution; BAI: Blockchain-based authentication and identification solution; BSDN: Blockchain-based secure SDN solution.

Paillier, which is an additive homomorphic cryptosystem. The secureSVM scheme is robust against two threat models, including, known ciphertext model and known background model. The secureSVM scheme can be adapted for green IoT-based agriculture. The blockchain-based IoT platform can be installed at the agriculture sensors layer and IoT data analysts at fog computing layer. The adaptation is summarized by the following steps:

- Step 1: Agriculture sensor nodes use sensing and transmitting valuable data through wireless;
- Step 2: Each access point collect data from the agriculture sensor nodes;
- Step 3: Each access point encrypts data using partially homomorphic encryption;
- Step 4: Each access point records the encrypted data on the blockchain;
- Step 5: Each access point uses the built-in consensus mechanism for validating the data;
- Step 6: Fog nodes communicate with an access point to obtain parameters of the training SVM classifier.

3) BLOCKCHAIN-BASED DISTRIBUTED KEY MANAGEMENT SOLUTION

The blockchain is used in key management architecture for eliminating the drawback of introducing a third party. Ma *et al.* [92] introduced a blockchain-based distributed key management architecture, named BDKMA, for IoT application. To achieve hierarchical access control, the BDKMA architecture uses security access managers for operating the blockchain. Specifically, the BDKMA architecture is based on the idea of authorization assignment mode and group access pattern. The BDKMA architecture can be applied to the network model composed of a device layer, a fog layer, and a cloud layer. The adaptation of BDKMA architecture in green IoT-based agriculture is summarized by the following steps:

- Step 1: Each agriculture sensor nodes selects its private key and generates the public key, encryption key, and secret access key;
- Step 2: Each agriculture sensor nodes packages encrypted secret access key and then signs and broadcasts the transaction to access point;
- Step 3: Each access point at agriculture sensors layer collects the transactions of the agriculture sensor nodes;
- Step 4: Each access point uses the built-in consensus mechanism for validating the data;

TABLE 4. Summary of privacy-oriented blockchain-based solutions for IoT applications and how they will be adapted for green IoT-based agriculture.

Solution	Year	Network model	Privacy-preserving model	Consensus algorithm	Countermeasures	How can be adapted for green IoT-based agriculture
Sharma et al. [86]	2017	The network model includes, IoT forwarding devices, Shelter modules, OrchApp, and Controller	- Privacy-preserving access control	- N/A	Shelter and OrchApp modules	- Integrate Shelter and OrchApp modules into the cloud computing layer - Integrate the distributed blockchain network into the fog computing layer - Interconnect the distributed blockchain network with the controllers
Dorri et al. [34]	2017	The network model composed of transactions, local blockchain, home miner, and local storage	- Privacy-preserving access control	- Smart home miner	- Generalized Diffie-Hellman - Lightweight hashing	- Place a local private blockchain inside a greenhouse - Integrate a miner in each greenhouse for processing incoming and outgoing transactions
Novo [87]	2018	The network model composed six different components: management hubs, blockchain network, smart contract, agent node, managers, and wireless sensor networks	- Privacy-preserving access control	- Proof-of-Work	- Access control rules	- The access management system is created at fog computing layer for creation of the blockchain network
Zhou et al. [88]	2018	The network model composed of n servers, the leader's device, and a leader	- Privacy protection of blockchain data	- Practical Byzantine fault tolerance	- Elliptic curve digital signature algorithm - Secure Hash Algorithm-256	- Blockchain-based IoT platform can be installed at the agriculture sensors layer - Fog computing node send transactions to the blockchain network
Hammi et al. [89]	2018	The network model composed of IoT devices and one device designed as master of the bubble	- Reputation and trust	- Proof of Work - Proof of Stake	- Elliptic curve digital signature algorithm - Hash algorithm	- Create secure virtual zones (bubbles) inside the agriculture sensors layer, where devices can communicate securely - Each device at agriculture sensors layer must communicate only with devices of its zone
Caro et al. [90]	2018	The network model is composed of six different components, including, provider, distributor, retailer, processor, producer, and consumer	- Traceability	- Proof of Work	- Hyperledger Sawtooth - Ethereum	- The AgriBlockIoT proposed that the blockchain as a layer which can be implemented in the traditional software platforms
Shen et al. [91]	2019	A data-driven IoT ecosystem, including blockchain-based IoT platform, IoT data providers, IoT data analyst, and IoT devices.	- Privacy-preserving machine learning training	- Proof-of-Work	- Paillier cryptosystem - 32-byte hash value	- Blockchain-based IoT platform can be installed at agriculture sensors layer - IoT data analysts can be installed at fog computing layer
Ma et al. [92]	2019	The network model composed of a device layer, a fog layer, and a cloud layer	- Privacy-preserving access control	- Proof-of-Work	- Symmetric cryptographic - Asymmetric cryptographic - Hash function	- Blockchain-based IoT platform can be installed at the agriculture sensors layer to achieve hierarchical access control
Dedeoglu et al. [93]	2019	The network model composed of three key layers, namely the application layer, the blockchain layer, and the data layer	- Reputation and trust	- Reputation-based adaptive block validation	- Hash algorithm	- Integrate a lightweight block generation mechanism inside the greenhouse
Ding et al. [94]	2019	The network model composed of two entities, attribute authorities and IoT devices	- Privacy-preserving access control	- Practical Byzantine fault tolerance	- Elliptic curve cryptosystem - Identity-based cryptography - Identity-based authentication and key agreement protocol - Hash algorithm	- The attribute-based access control is created at agriculture sensors layer for creation of the blockchain network
Si et al. [95]	2019	The network model is based on three layers, including, the application layer, the transport layer, and the sensing layer	- Privacy protection of blockchain data	- Practical Byzantine fault tolerance	- Double-chain model - Tamper-proof of data - Blind signature algorithm - Hash algorithm	- agriculture sensors layer adapts a double-chain model - The data blockchain part is calculated at fog computing layer
Derhab et al. [96]	2019	The system model is composed of the following four components: Virtual Switch, SDN controller, IP network, and Private cloud	- Privacy protection of blockchain data	- N/A	- K-Nearest Neighbors - Random subspace learning	- Integrate an IDS system into the access point at agriculture sensors layer - Integrate the Virtual Switch into the fog computing layer - Integrate the SDN controller into the cloud computing layer

- Step 5: An agriculture sensor node obtain access permission from access point using an access query transaction;
- Step 6: An agriculture sensor node periodically update the access keys and sends a key update transaction to the access point;

4) BLOCKCHAIN-BASED ACCESS CONTROL SOLUTION

To provide scalable access management in IoT application, Novo [87] proposed a distributed access control architecture using blockchain technology. The access control policies are enforced by the blockchain platform. The adaptation of proposed architecture in green IoT-based agriculture can bring the following six advantages to access control: transparency, scalability, lightweight, concurrency, accessibility, and mobility. The adaptation of proposed architecture is summarized in the following steps:

- Step 1: Fog node deploys the smart contract into the blockchain network at fog computing layer;
- Step 2: To be registered as a manager, each access point at agriculture sensors layer request the address of the smart contract;
- Step 3: To transfer the management control of an agriculture sensor device, an access point at agriculture sensors layer requests the agriculture sensor device's address and the blockchain address of the smart contract;

- Step 4: An access point at agriculture sensors layer enforces the policy creating a transaction towards the smart contract;
- Step 5: An access point at agriculture sensors layer adds an existing policy.

Ding *et al.* [94] proposed a attribute-based access control scheme for IoT application, which can be adapted for greenhouse. According to the identity or ability of each IoT devices, attribute authorities describe a set of attributes to each IoT devices. The blockchain is used to record the distribution of these attributes. The adaptation of this attribute-based access control scheme for blockchain-based greenhouse is summarized in the following steps:

- Step 1: Greenhouse miner generates a pair of public and secret key for each IoT devices;
- Step 2: Greenhouse miner sends both keys in a secure channel based on identity-based cryptography;
- Step 3: Each IoT devices uses an address along with its ID and then generate a corresponding address based on the hash algorithm;
- Step 4: IoT device inside greenhouse generates new block and broadcasts to the other consortium nodes using the practical Byzantine fault tolerance;
- Step 5: When IoT device wants to send to another device, they use identity-based authentication and key agreement (AKA) protocol.

Dorri *et al.* [34] introduced a smart home tier based on the blockchain technology, which can be adapted for greenhouse. The network model of the blockchain-based greenhouse is composed of the following components: transactions, local blockchain, greenhouse miner, and local storage. The adaptation of blockchain-based greenhouse is summarized in the following steps:

- Step 1: Greenhouse miner generates a key with an IoT device;
- Step 2: Greenhouse miner shares the key and stores it in the genesis transaction;
- Step 3: Greenhouse miner defines the policy header and adds it to the first block;
- Step 4: Each IoT device inside greenhouse communicate with another internal device using the permission from the miner;
- Step 5: Each IoT device inside greenhouse can store data on the cloud storage using the permission from the miner;
- Step 6: When IoT device wants to send to another external device, a Virtual Private Network (VPN) connection is used to routes the packets to the shared miner.

5) BLOCKCHAIN-BASED REPUTATION AND TRUST SOLUTION

Dedeoglu *et al.* [93] proposed a reputation and trust mechanism for blockchain-based IoT applications, which can be adapted for greenhouse. The proposed model verifying transactions based on three key layers, namely the application layer, the blockchain layer, and the data layer. The adaptation of blockchain-based greenhouse for trust architecture is summarized in the following steps:

- Step 1: IoT device inside greenhouse generates blocks in periodic intervals. The generation is based on the public key and the signature of the data source;
- Step 2: IoT device sends the blocks to greenhouse miner at agriculture sensors layer;
- Step 3: Greenhouse miner validates the blocks based on the number of validator node and the reputation of the block generating node.

To realize reliable storage and sharing of IoT information in green IoT-based agriculture, the work by Si *et al.* [95] is a security mechanism that can be adapted for smart agriculture. The proposed mechanism is based on blockchain technology, which is applied in three layers, including, the application layer, the transport layer, and the sensing layer. The application layer is mainly used by the cloud service. The data blockchain part is installed in the fog computing layer. In addition, the proposed mechanism uses a double-chain model with tamper-proof of data in the data blockchain.

Zhou *et al.* [88] proposed a threshold secure multi-party computing protocol, TSMPC, for blockchain-based threshold IoT system. The TSMPC protocol extends Shamir's (t, n)-secret sharing (SSS) [97]. Specifically, the TSMPC protocol is applied between a leader and n server, which can be adapted for green IoT-based agriculture. The network model is composed of n servers, the leader's device, and a leader. The performance evaluation on the Ethereum blockchain shows that a block can record transactions of at most 62,360 bytes. Therefore, the adaptation of a threshold secure multi-party computing protocol for green IoT-based agriculture is summarized in the following steps:

- Step 1: A fog computing node generates an initialize transaction with a verification key and sends it to the blockchain network;
- Step 2: IoT sensor node at agriculture sensors layer verify the transaction's verification key;
- Step 3: An access point at agriculture sensors layer verifies core shares, which can obtain a reward from the fog computing node.

6) BLOCKCHAIN-BASED AUTHENTICATION AND IDENTIFICATION SOLUTION

To ensure authentication and robust identification of IoT devices in IoT application, Hammi *et al.* [89] proposed an original decentralized system, called *bubbles of trust*, which can be applied for green IoT-based agriculture. Based on the blockchain technology, the *bubbles of trust* system create secure virtual zones (bubbles), which can protect the availability and data integrity. The *bubbles of trust* system is resistant against four attacks, namely, Sybil attack, spoofing attack, DoS/DDoS attack, and replay attack. Therefore, the adaptation of *bubbles of trust* system for green IoT-based agriculture consists of creating secure virtual zones

inside the agriculture sensors layer, where devices can communicate securely. Specifically, each device at agriculture sensors layer must communicate only with devices of its zone. The communications between devices are considered as transactions and must be validated by this blockchain network.

7) BLOCKCHAIN-BASED SECURE SDN SOLUTION

To facilitate software and hardware updates for green IoT-based agriculture, software-defined networking (SDN) is used, which allows easy control and management in a central location. To detect any false injection data, a blockchain-based secure SDN architecture is adapted. Derhab *et al.* [96] proposed two security components, namely, 1) Blockchain-based integrity checking system (BICS) 2) Intrusion detection system (IDS). These two systems are combined for SDN-architecture, which can be adapted for green IoT-based agriculture. The adaptation is summarized in the following steps:

- Step 1: Integrate the SDN controller into the cloud computing layer;
- Step 2: Integrate a Virtual Switch (vSwitch) into the fog computing layer
- Step 3: Integrate an IDS system into the access point at agriculture sensors layer. To detect cyber attacks, the IDS system combines two machine learning classifiers, namely, K-Nearest Neighbors and random subspace learning;
- Step 4: The SDN controller creates blocks and shares it via the blockchain;
- Step 5: The Firewall check the rules from vSwitch and blockchain.

To provides scalability within the current IoT application, the SDN and blockchains technology are combined by the work Sharma *et al.* [86]. Specifically, the work proposed a secure SDN architecture, named DistBlockNet, which is based on the blockchain technology. The DistBlockNet architecture interconnects a distributed blockchain network with the controllers. Each local network includes Shelter modules, OrchApp, and Controller. To maintains the updated flow rules table information, the distributed blockchain network uses the request/response and controller/verification nodes. The performance evaluation shows that DistBlockNet architecture is robust against DDoS/DoS attacks and cache poising/ARP spoofing. The adaptation of DistBlockNet architecture in green IoT-based agriculture is summarized by the following steps:

- Step 1: Integrate Shelter and OrchApp modules into the cloud computing layer;
- Step 2: Integrate the distributed blockchain network into the fog computing layer;
- Step 3: Interconnect the distributed blockchain network with the controllers at fog computing layer;
- Step 4: IoT sensor node at agriculture sensors layer sends data to the controllers.

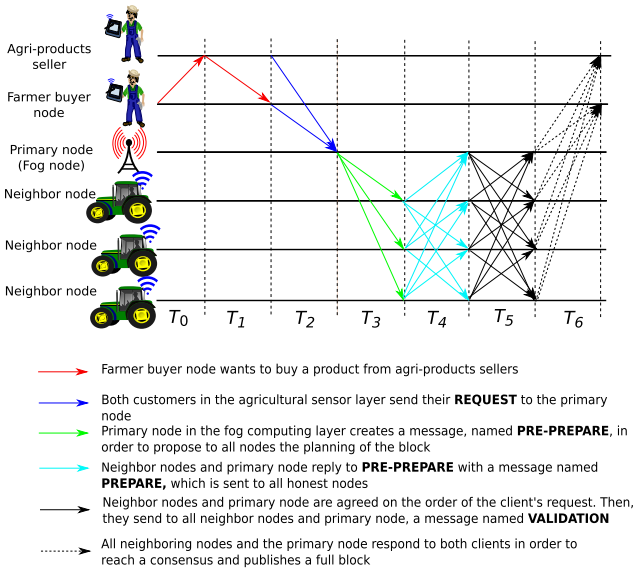


FIGURE 6. The consensus process based on the practical Byzantine fault tolerance (PBFT) algorithm for blockchain-based agri-products distribution.

B. CONSENSUS ALGORITHMS FOR BLOCKCHAIN-BASED SOLUTIONS

A consensus algorithm can be defined as the mechanism by which a Blockchain network achieves consensus. The public blockchains (i.e., decentralized) are built as distributed systems and, since they do not depend on a central authority, the distributed nodes must agree on the validity of transactions using a consensus algorithm. Table 5 summarizes consensus algorithms for Blockchain-based solutions and how they will be adapted for green IoT-based agriculture.

1) PROOF-OF-WORK (PoW)

The PoW is a consensus algorithm introduced by Bitcoin and widely used by other cryptocurrencies. This consensus is called "Mining", which the nodes in the IoT network are called "Miners" [98]. Specifically, the PoW algorithm is presented as a response to a mathematical problem, which requires considerable work, but is usually easily checked once the answer is obtained. A miner node continuously tests a variety of unique values (known as nonce) until an appropriate value is produced [123]. The minor node that solves the puzzle extracts the succeeding block, then adds it to the blockchain network and confirms the transactions, and receives the compensation for the block. The PoW can be adapted by a Blockchain-based solution for green IoT-based agriculture, which each access point at agriculture sensors layer is selected as miners in order to calculate the hash values for validating blocks. This adaptation ensures that access points are encouraged to maintain the blockchain network, as they are compensated for their efforts. The disadvantage of the PoW algorithm for green IoT-based agriculture is that computational resources require a lot of energy to validate the blocks.

TABLE 5. Summary of consensus algorithms for blockchain-based solutions and how they will be adapted for green IoT-based agriculture.

Consensus algorithm	Blockchain-based solutions	Type	Performance (+)	Limitation (-)	How can be adapted for green IoT-based agriculture
Proof-of-Work (PoW)	- Bitcoin [98]	Competition consensus	+ Resistance against DDoS attacks + Resistance against spam attacks	- The computational resources use a lot of energy to valid blocks - - Vulnerable to double-spend attack	- Each access point at agriculture sensors layer are selected as miners, which they calculate the hash values to valid blocks
Proof-of-Stake (PoS)	- Peercoin [99] - Nxt [100]	Competition consensus	+ Avoiding energy expenditure + More costly to attack	- Vulnerable to nothing-at-stake problem.	- Select all IoT nodes in agriculture sensors layer as the validators
Delegated Proof-of-Stake (DPoS)	- BitShares [101] - Steemit [102]	Cooperative consensus	+ Reducing the number of interactions between the nodes + Allows more transactions and faster validation	- Vulnerable to centralization since the number of delegate is limited	- Each access point at agriculture sensors layer is selected as a delegate
Delayed Proof-of-Work (DPoW)	- Komodo [103]	Cooperative consensus	+ Secure and resistant to attacks 51% + Adapted for blockchains that use PoW or PoS	- Vulnerable to notary node attack, eclipse attack, and double-spending attack	- Select all fog nodes in fog computing layer as notary nodes - Select all IoT nodes in agriculture sensors layer as normal nodes
Proof-of-capacity (PoC)	- Burstcoin [104]	Cooperative consensus	+ No dedicated hardware + No constant hard disk drive upgrades are required.	- Vulnerable to malware attacks	- Each fog nodes at fog computing layer are selected as miners
Proof of Stake Velocity (PoSV)	- Reddcoin [105]	Competition consensus	+ Reducing the wastefulness of mining + Requires low computing power or energy	- Vulnerable against attack 51%	- To increase the chances of finding a valid block, an IoT device should have a bigger holding of Reddcoins
Proof-of-Authority (PoA)	- POA.Network [106] - VeChain [107]	Cooperative consensus	+ Provide scalability + Avoiding energy expenditure	- Can used only in private and permissioned blockchains	- Select all fog nodes in fog computing layer as validators
Proof-of-History (PoH)	- Solana [108]	Cooperative consensus	+ Reducing data overhead + Without sharding	- Can used only in private and permissioned blockchains	- Each IoT device at agriculture sensors layer create a historical record
Proof-of-Activity (PoAC)	- Decred [109]	Competition consensus	+ Less energy consumption + Improved network topology	- Vulnerable to double-spend attack	- Each fog node (miner) at fog computing layer uses his hashing power to generate an empty block header - All IoT devices at agriculture sensors layer derive N pseudorandom stakeholders using the hash of the block header
Proof-of-Weight (PoWe)	- Algorand [110]	Competition consensus	+ Prevent Sybil attacks + Achieve scalability	- Reduce the incentive since it's very difficult to be rewarded	- Assigns a weight to each farmer according to the tokens they hold
Proof-of-Burn (PoB)	- Slimcoin [111]	Competition consensus	+ Mining without powerful hardware + More node can become involved in mining	- Only nodes that are willing to burn more money, they have a chance to be miners	- Each fog node at fog computing layer sends coins to a burn address
Proof of Elapsed Time (PoET)	- Hyperledger Sawtooth [112]	Competition consensus	+ Reduced participation costs	- Not appropriate for use in public blockchain networks	- Each IoT device at agriculture sensors layer generates a random wait time and sleeps for a fixed period of time
Proof-of-Importance (PoI)	- NEM [113]	Cooperative consensus	+ Requires no special hardware + Avoiding energy expenditure	- Vulnerable to nothing-at-importance problem	- Each IoT devices at agriculture sensors layer are assigned an importance score
Stellar Consensus protocol (SCP)	- Stellar Consensus [114]	Cooperative consensus	+ Low latency + Flexible trust + Asymptotic security + Decentralized control	- Reduce the incentive since there are no block rewards	- Apply a voting system in agriculture sensors layer to choose quorum and quorum slice among IoT devices and then use quorum intersection to guarantee agreement
Proof-of-Reputation (PoR)	- GoChain [115]	Cooperative consensus	+ Adapted for private and permissioned networks + Avoiding energy expenditure	- Can used only in private and permissioned blockchains	- Select an IoT node as an authoritative node if he has a reputation important enough
Delegated Byzantine Fault Tolerance (dBFT)	- Neo [116]	Competition consensus	+ Less energy consumption + Mining without powerful hardware	- Bookkeepers operate under real identities	- Apply a voting system in agriculture sensors layer to choose bookkeepers and speaker among IoT devices
Practical Byzantine fault tolerance (PBFT)	- Ripple [117] - DeepCoin [118] - Hyperledger Fabric [119] - DeliveryCoin [120] - Stellar [121] - Dispatch [122]	Cooperative consensus	+ Low variance of the reward + Less energy consumption	- The number of messages increases exponentially	- The fog nodes are used to receive requests from IoT devices - The fog nodes create PRE-PREPARE messages to propose to the other replicas the scheduling of the bloc

2) PROOF-OF-STAKE (PoS)

The PoS is a distributed consensus algorithm (used by Peercoin [99] and Nxt [100]) that requires the user to prove that they have a specific quantity of currency to validate any additional blocks in the blockchain network and to be awarded the reward. Compared to the PoW algorithm, the PoS is not computationally costly for validators, but it is vulnerable to nothing-at-stake problem. The PoS can be adapted by a Blockchain-based solution for green IoT-based agriculture, which all IoT nodes in agriculture sensors layer are selected as the validators.

3) DELEGATED PROOF-OF-STAKE (DPoS)

The DPoS is a consensus algorithm (used by BitShares [101] and Steemit [102]) that restricts the number of nodes in a blockchain network to a small number of entities chosen

by token owners. These delegates are responsible for the following three paid tasks: 1) implementing changes to the blockchain network, 2) recording transactions, and 3) ensuring the integrity of the registry. The DPoS algorithm can be adapted by a Blockchain-based solution for green IoT-based agriculture, which each access point at agriculture sensors layer is selected as a delegate. This adaptation ensures that access points provide an efficient, fast, decentralized consensus algorithm.

4) DELAYED PROOF-OF-WORK (DPoW)

The DPoW is a consensus algorithm designed by the Komodo project [103], which is a modified version of the Proof of Work consensus algorithm. The DPoW algorithm is based on the idea of notary nodes, which are used to record data to the blockchain network (e.g., Bitcoin). The DPoW can be adapted by a Blockchain-based solution for green IoT-based agriculture, which all fog nodes in fog computing layer are selected as notary nodes and all IoT nodes in agriculture sensors layer are selected as as normal nodes. This adaptation ensures that it is impossible to reorganize notarized blocks, which makes blockchains more secure and resistant to attacks 51%.

5) PROOF-OF-ACTIVITY (PoAC)

The PoAC algorithm (used by Decred [109]) is an extension of the Bitcoin protocol, which is based on combining Proof of Work component with a Proof of Stake type of system. The PoAC can be adapted by a Blockchain-based solution for green IoT-based agriculture as follows [124]. 1) Each fog node (miner) at fog computing layer uses his hashing power to generate an empty block header. 2) The fog node broadcasts her block header to IoT devices at agriculture sensors layer. 3) All IoT devices at agriculture sensors layer derive N pseudorandom stakeholders using the hash of the block header. 4) Every stakeholder at agriculture sensors layer checks whether the empty block header that the fog node broadcasted is valid.

6) PROOF-OF-AUTHORITY (PoA)

The PoA is a reputation-based consensus algorithm (used by POA.Network [106] and VeChain [107]) for private blockchain networks. The PoA consensus algorithm is based on the value of identity, which means that the validators use their own reputation to validate the blocks. The PoA can be adapted by a Blockchain-based solution for green IoT-based agriculture, which all fog nodes in fog computing layer are selected as validators. This adaptation ensures a limited number of block validators, which provides a highly scalable system.

7) PROOF-OF-IMPORTANCE (PoI)

The PoI is a consensus algorithm proposed by NEM [113]. The PoI can be adapted by a Blockchain-based solution for green IoT-based agriculture, which each IoT devices at agriculture sensors layer are assigned an importance score. The IoT devices with high scores of importance have a higher chance of harvesting a block. The transaction graph topology can be used as an input into the importance of an IoT device.

8) PROOF-OF-WEIGHT (PoWE)

The PoWe is proposed by Gilad *et al.* [110], which is based on the Algorand consensus model. The Algorand uses a Byzantine agreement protocol to reach consensus on the blockchain network. The users are selected randomly using verifiable random functions. Algorand users use a protocol to communicate, which assigns a weight to each user according to the tokens they hold. The users' weights are used to chooses committee members randomly among all users. The PoWe can be adapted by a Blockchain-based solution for green IoT-based agriculture, which an Algorand protocol assigns a weight to each farmer according to the tokens they hold. This adaptation ensures resistance to Sybil attacks and achieves scalability but reducing the incentive since it's very difficult to be rewarded.

9) PROOF-OF-BURN (PoB)

The PoB algorithm (used by Slimcoin [111]) is similar to a proof of work algorithm but with reduced energy consumption rates. The PoB network block validation process does not require the use of powerful computing resources and does not depend on powerful extraction equipment. Instead, Coins are deliberately burned and this is a way to ''invest'' resources in the blockchain, so that candidate miners are not required to invest physical resources. By burning Coins, users are able to demonstrate their engagement with the network, which can obtain the right to mine and validate transactions [125]. The PoB can be adapted by a Blockchain-based solution for green IoT-based agriculture, which each fog node at fog computing layer sends coins to a burn address.

10) PROOF-OF-CAPACITY (PoC)

The PoC is very similar to the PoW algorithm, which the storage is used instead of computation. The PoC (used by Burstcoin [104]) allows the mining nodes to use the free space on their hard disk. The PoC can be adapted by a Blockchain-based solution for green IoT-based agriculture, where each fog nodes at fog computing layer are selected as miners since they have high storage compared to nodes at agriculture sensors layer. To validating the blocs and winning the mining reward, the fog nodes involve a two-step process, including, plotting and mining.

11) PROOF OF ELAPSED TIME (POET)

The POET is a consensus algorithm frequently applied on the permissioned blockchain networks to decide on mining authorizations. The POET is based on the idea of ''Elapsed Time'', where each node involved in the system is expected to wait for a randomly selected period of time, and the first node to complete the designated waiting time wins the new block. The POET can be adapted by a Blockchain-based solution for green IoT-based agriculture, which each IoT device at agriculture sensors layer generates a random wait time and

sleeps for a fixed period of time. For more details about the PoET algorithm, we refer the reader to the Hyperledger Sawtooth project [112].

12) PROOF-OF-REPUTATION (PoR)

The PoR algorithm (used by GoChain [115]) is similar to PoA algorithm, which it is based on the reputations of the IoT nodes. An IoT node in the green IoT-based agriculture must have a reputation important enough to be voted as an authoritative node. Once an authoritative node is voted, he can sign and validate blocks in the blockchain network.

13) PRACTICAL BYZANTINE FAULT TOLERANCE (PBFT)

The PBFT (Practical Byzantine Fault Tolerance) algorithm is the first to be able to tolerate ''Byzantine'' faults, which is proposed by Miguel Castro and Barbara Liskov in 1999 [126]. This algorithm provides reliability and robustness properties in a synchronous environment and requires $N = 3f+1$ replicas to tolerate simultaneous Byzantine faults. The PBFT algorithm can be effectively applied in almost all domains of IoT, including, Internet of Energy [118], Internet of Drones [120], Internet of Vehicles [127], ...etc. Therefore, the PBFT algorithm can be adapted by a Blockchain-based solution for green IoT-based agriculture, as presented in Fig. 6. Specifically, when a farmer buyer node wants to buy a product from agri-products sellers, they send its request to the fog node. This fog node creates a PRE-PREPARE message to propose to the other replicas the scheduling of the bloc. The correct replicas respond to the PRE-PREPARE with a PREPARE message, which is sent to all replicas (i.e., neighbor nodes). Once the neighbor nodes have received $2f$ PREPARE and the associated PRE-PREPARE, then they agree on the order of the farmer buyer node's request. At the end, the neighbor nodes send a VALIDATION message to all replicas. Once a replica has received $2f + 1$ VALIDATION, then it executes the request and responds to both farmer buyer node and agri-products seller. If the client does not receive a response after a specified time period, he forwards the request to all replicas. When a replica receives a request, it starts view-change. Note that there are more variations of PBFT algorithm such as Aardvark [128], Zyzzyva [129], HQ [130], Q/U [131], and Abstract [132].

14) DELEGATED BYZANTINE FAULT TOLERANCE (dBFT)

The dBFT algorithm is a consensus method (used by Neo [116]) where all users elect nodes, called bookkeepers, who are responsible for adding new blocks to the blockchain. This elected node group can be updated regularly. The vote is weighted by the amount of cryptocurrency owned. Each bookkeeper is randomly selected to propose a block. This node is called a speaker. The bookkeepers become speakers in turn by random drawing. The speaker checks the signatures and the validity of transactions and then collects them in a block. The speaker proposes his block to all the other bookkeepers. Afterward, the bookkeepers verify the block and then each one vote in favor or against the block. The consensus is reached when at least 66% of bookkeepers vote in favor of the block and it is then added to the blockchain. The dBFT algorithm can be adapted for green IoT-based agriculture by applying a voting system in agriculture sensors layer to choose delegates and speaker among IoT devices.

15) STELLAR CONSENSUS PROTOCOL (SCP)

The SCP protocol (used by Stellar Consensus [114]) is based on federated Byzantine agreement (FBA). The nodes exchange a series of votes to confirm and accept a value. For this purpose, the SCP protocol determines a minimum quorum. The ''quorum'' is a set of nodes that are sufficient to reach an agreement. Each node chooses one or more quorum slices and includes in each slice the nodes in which it has confidence. Each quorum slice will then produce interactions with each other. To reach an agreement, the SCP protocol uses the idea of quorum intersection. A federated Byzantine agreement system enjoys quorum intersection if any two of its quorums share a node. The SCP protocol can be adapted for green IoT-based agriculture by applying a voting system in agriculture sensors layer to choose quorum and quorum slice among IoT devices and then use quorum intersection to guarantee agreement.

16) OTHER CONSENSUS ALGORITHMS

There are other consensus algorithms that can be adapted by a Blockchain-based solution for green IoT-based agriculture. We cite the following nine consensus algorithms: Byteball consensus [133], Mokka consensus [134], SPECTRE consensus [135], Block-Lattice consensus [136], Hashgraph consensus [137], Tangle consensus [138], Directed Acyclic Graphs (used by Iota [139]), Proof of Believability (used by IOST [140]), and RAFT consensus [141].

VI. CHALLENGES

To complete our overview, we outline research challenges that could improve the security and privacy solutions for IoT-based agriculture, summarized in the following recommendations:

A. MACHINE LEARNING TECHNIQUES FOR INTRUSION DETECTION SYSTEMS

Intrusion detection systems (IDSs) are implemented along with other security systems such as authentication and access control techniques using encryption mechanisms to protect systems against cyber attacks. Using data mining and machine learning techniques (e.g., Deep learning, Random forests, Support Vector Machine, Naive Bayes, ...etc), IDSs can differentiate between normal and malicious actions. The implementation of IDSs for IoT-based agriculture as a software application will able to identify security incidents. Therefore, the question we ask here is : how to choose the right machine learning technique among different types (i.e., reinforcement learning, unsupervised learning, or supervised learning)? We believe that a comparative study of machine

learning techniques for cyber security intrusion detection is needed for IoT-based agriculture.

B. DATASET FOR INTRUSION DETECTION IN IoT-BASED AGRICULTURE SCENARIOS

The datasets for cyber security are so important in intrusion detection, which are used for testing the performance of IDSs. Actually, most and recent IDSs are tested with KDD 1999 [142], NSL-KDD [143], CICIDS2017 [144], Bot-IoT [145], and CSE-CIC-IDS2018 [146]. These datasets are not simulated for IoT-based agriculture scenarios. A possible research direction in this topic could be related to developing a new dataset to build a network intrusion detector under IoT-based agriculture environment.

C. SCALABILITY ANALYSIS OF BLOCKCHAIN-BASED SOLUTIONS

To solve security and privacy problems (e.g., access control, reputation, trust, ...etc), we have seen that a blockchain-based solution brings advantages for IoT application. The application of a blockchain-based solution for IoT-based agriculture requires a study on the characteristics of the implementation. Therefore, there are many characteristics should be taken under consideration when a blockchain-based solution is proposed for IoT-based agriculture, such as scalability issues when the number of participating nodes at agriculture sensors layer is increased. Thus, one of the challenges that should receive more attention in the future is to provide a scalability analysis of blockchain-based solutions for IoT-based agriculture.

D. HOW TO PICK THE BEST CONSENSUS ALGORITHM

The performance of a blockchain-based solution for IoT-based agriculture is related to the effectiveness of the consensus algorithm. Therefore, since IoT devices at agriculture sensors layer are not always able to satisfy the high computational and energy requirements when addressing the validation of blocks and the storage of blockchain, consensus-efficient issues arise as follows:

- If the PoW algorithm is used, how to integrate a miner in each greenhouse for processing incoming and outgoing transactions?
- If the stellar consensus algorithm is used, how to design a voting system in agriculture sensors layer to choose quorum and quorum slice among IoT devices and then use quorum intersection to guarantee agreement?
- If the dBFT algorithm is used, how to design a voting system in agriculture sensors layer to choose bookkeepers and speaker among IoT devices?

E. DESIGN OF PRACTICAL AND COMPATIBLE CRYPTOGRAPHIC PROTOCOLS

In some cases of green IoT-based agriculture, it is not necessary to use blockchain to solve security and privacy problems (e.g., identity anonymity), which there are many other better solutions such as practical and compatible cryptographic solution. Therefore, a new cryptographic solution is proposed recently by Yang *et al.* [147] for the automatic dependent surveillance-broadcast, which they use the format-preserving encryption (FPE) and lightweight broadcast authentication protocol (TESLA) to achieve the identity anonymity. However, resource and power-constrained IoT devices at agriculture sensors layer are not always capable of meeting the substantial computational and power consumption in the processing of new cryptographic solution. Therefore, the design of practical and compatible cryptographic protocols is one of the significant research challenges in green IoT-based agriculture.

F. RESILIENCY AGAINST SPECIFIC ATTACKS IN THE CONTEXT OF LOW-RESOURCE IoT DEVICES

The threat models discussed in the environment of IoT-based agriculture and the key security problem is different in distinct smart agriculture applications. Sometimes, the specific problem does not exist in an IoT application, and it is meaningless to take combined attacks into consideration. The methods to solve attacks can be integrated together to solve problems in an application. To propose a scheme against a kind of attack in a smart agriculture application, the attack should be specific and defined at the beginning. The most important question that may arise is how to develop a new security strategy that can resist combined attacks while considering the practicability of deploying the solution, particularly in the context of low-resource IoT devices at agriculture sensors layer.

G. COUNTER MEASURES AGAINST 5G NETWORK SLICING THREATS

5G networks will be facilitators of IoT based agriculture applications, especially in the sensors layer (See Figure 1). 5G adopt network slicing as a means of partitioning the physical and network resources to optimally group the different traffic, isolate from other tenants and configure the network resources. The logical partitioning of network slicing divides and separates a single common physical network into various virtual, complete E2E networks and offers complete isolation for these virtual networks from each other in terms of access, transport, device and core network. The main advantage of Network Slicing is that now MNOs can configure and apply tailor-made customization of their network resources to accommodate different users and different traffic classes, and hence differentiated services.

Security of Network Slicing plays a significant role for the control and the coordination among different slices and for function of the related mechanisms that are responsible for the inter-network slices communication and the coordination between user and control plane. A security leakage that is related to the inter-slice communication functionality can lead to disruption of the inter-slice communication. Moreover, authentication for the identification of the privileged users in order to prevent impersonation attacks against slices

seems to be critical for the proper control of the network resources. Furthermore, the provision of differentiated services is also related to the provision of different security level of services among the slices. However, this must not affect the security level of another slice. In addition, DoS attacks focus on the possible exhaustion of network resources to lead in unavailability of network provisioned services [148]. These attacks must be dealt with a multi layered security framework that includes traditional methods, e.g. IDS and field specific solutions, e.g. slice isolation.

H. DEPLOYING IoT IN AGRICULTURE

As we mentioned in Section II, IoT in agriculture can be envisioned in different layers and from different perspectives. In this subsection, we try to summarize and emphasize the different conditions that exist in an agricultural environment that make the deployment of IoT challenging.

When talking about the WSNs, the specific characteristics of the environment, in which the nodes will be deployed, should be taken into account. Crops, or other obstacles in farmlands whose positions may change over time, cause considerable interference in the communication between nodes. These moving obstacles affect the connection quality of links, changing the channel conditions over time, affecting the deployment, packet routing algorithms, failure diagnosis methods, and other aspects of WSNs. Environmental factors such as temperature, rainfall, humidity, high solar radiation along with changing shading by plant leaves, as well as noise produced by building structures, such as greenhouses, further increase Spatio-temporal climatic variation, greatly affecting the communication among nodes that are deployed in such harsh environment. This changing environment imposes requirements and calls for novel duty-cycle control, sampling and scheduling, data reconstructions, as well as data storage and query, intelligent control, and other solutions [38], [149].

Although in theory or in simulated environments all these challenges have been already studied and analyzed when it comes to the actual deployment of IoT in the agricultural sector this task is very demanding and challenging. The modules that are used in order to sense and report any situation need to be accurate enough, properly shielded against environmental factors which can either lead to false reporting or destruction of the sensors permanently [150]. In addition, the replacement of power source to distributed sensor nodes that are spread in wide areas can be a very difficult task, if not impossible and must be taken into consideration during the design of such systems.

In terms of communication among nodes, since many different technologies can be combined, from GSM to WPAN and P2P, interoperability is the main challenge when designing or deploying such systems, especially in agriculture where high temperature and high humidity affect it in a negative way. Also when different communication methods are used in the same area (e.g. Bluetooth, ZigBee, and WiFi) interference is a parameter that needs to be also considered [151].

Since the sensors devices are deployed in an open field, which cannot be monitored by people all the time, the system can easily be attacked physically. In addition, sensors devices are not densely deployed in agricultural applications and they are more complex in terms of hardware components. Finally the area where sensor devices are located is not monitored so well compared to the one deployed inside a city and it is easy to add malicious nodes (e.g., Malicious 4G stations) that can overhear the information that is exchanged or perform several attacks like DDoS or MITM.

VII. CONCLUSION

In this paper, we surveyed the state-of-the-art of existing security and privacy solutions for green IoT-based agriculture. We provided an overview of a four-tier green IoT-based agriculture architecture. Through extensive research and analysis that was conducted, we were able to classify the threat models against green IoT-based agriculture into five categories, including, attacks against privacy, authentication, confidentiality, availability, and integrity properties. In addition, we analyzed the privacy-oriented blockchain-based solutions as well as consensus algorithms for green IoT-based agriculture. There still exist several challenging research areas, such as machine learning techniques, datasets for intrusion detection, scalability analysis of blockchain-based solutions, how to pick the best consensus algorithm, and the design of practical and compatible cryptographic protocols, which should be further investigated in the near future.

REFERENCES

[1] N. Ahmed, D. De, and I. Hussain, "Internet of Things (IoT) for smart precision agriculture and farming in rural areas," *IEEE Internet Things J.*, vol. 5, no. 6, pp. 4890–4899, Dec. 2018.

[2] T. Song, R. Li, B. Mei, J. Yu, X. Xing, and X. Cheng, "A privacy preserving communication protocol for IoT applications in smart homes," *IEEE Internet Things J.*, vol. 4, no. 6, pp. 1844–1852, Dec. 2017.

[3] A. Ometov, S. V. Bezzateev, J. Kannisto, J. Harju, S. Andreev, and Y. Koucheryavy, "Facilitating the delegation of use for private devices in the era of the Internet of wearable things," *IEEE Internet Things J.*, vol. 4, no. 4, pp. 843–854, Aug. 2017.

[4] M. Mohammadi, A. Al-Fuqaha, M. Guizani, and J.-S. Oh, "Semisupervised deep reinforcement learning in support of IoT and smart city services," *IEEE Internet Things J.*, vol. 5, no. 2, pp. 624–635, Apr. 2018.

[5] H. Al-Hamadi and I. R. Chen, "Trust-based decision making for health IoT systems," *IEEE Internet Things J.*, vol. 4, no. 5, pp. 1408–1419, Oct. 2017.

[6] N. Lu, N. Cheng, N. Zhang, X. Shen, and J. W. Mark, "Connected vehicles: Solutions and challenges," *IEEE Internet Things J.*, vol. 1, no. 4, pp. 289–299, Aug. 2014.

[7] Y.-J. Chen and L.-C. Wang, "Privacy protection for Internet of drones: A network coding approach," *IEEE Internet Things J.*, vol. 6, no. 2, pp. 1719–1730, Apr. 2019.

[8] 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.

[9] O. Elijah, T. A. Rahman, I. Orikumhi, C. Y. Leow, and M. H. D. N. Hindia, "An overview of Internet of Things (IoT) and data analytics in agriculture: Benefits and challenges," *IEEE Internet Things J.*, vol. 5, no. 5, pp. 3758–3773, Oct. 2018.

[10] *Global Smart Agriculture Marke*. Accessed: Jul. 25, 2019. [Online]. Available: https://www.zionmarketresearch.com/report/smart-agriculture-market

[11] L. J. Klein, H. F. Hamann, N. Hinds, S. Guha, L. Sanchez, B. Sams, and N. Dokoozlian, "Closed loop controlled precision irrigation sensor network," *IEEE Internet Things J.*, vol. 5, no. 6, pp. 4580–4588, Dec. 2018.
[12] A. L. Diedrichs, F. Bromberg, D. Dujovne, K. Brun-Laguna, and T. Watteyne, "Prediction of frost events using machine learning and IoT sensing devices," *IEEE Internet Things J.*, vol. 5, no. 6, pp. 4589–4597, Dec. 2018.
[13] W.-L. Chen, Y.-B. Lin, Y.-W. Lin, R. Chen, J.-K. Liao, F.-L. Ng, Y.-Y. Chan, Y.-C. Liu, C.-C. Wang, C.-H. Chiu, and T.-H. Yen, "AgriTalk: IoT for precision soil farming of turmeric cultivation," *IEEE Internet Things J.*, vol. 6, no. 3, pp. 5209–5223, Jun. 2019.
[14] A. Mukherjee, S. Misra, N. S. Raghuwanshi, and S. Mitra, "Blind entity identification for agricultural IoT deployments," *IEEE Internet Things J.*, vol. 6, no. 2, pp. 3156–3163, Apr. 2019.
[15] M. A. Zamora-Izquierdo, J. Santa, J. A. Martínez, V. Martínez, and A. F. Skarmeta, "Smart farming IoT platform based on edge and cloud computing," *Biosyst. Eng.*, vol. 177, pp. 4–17, Jan. 2019.
[16] P. Abouzar, D. G. Michelson, and M. Hamdi, "RSSI-based distributed self-localization for wireless sensor networks used in precision agriculture," *IEEE Trans. Wireless Commun.*, vol. 15, no. 10, pp. 6638–6650, Oct. 2016.
[17] *Iot in Agriculture: 5 Technology Use Cases for Smart Farming (and 4 Challenges to Consider)*. Accessed: Jul. 25, 2019. [Online]. Available: https://easternpeak.com/blog/iot-in-agriculture-5-technology-use-cases-for-smart-farming-and-4-challenges-to-consider/
[18] S.-C. Cha, T.-Y. Hsu, Y. Xiang, and K.-H. Yeh, "Privacy enhancing technologies in the Internet of Things: Perspectives and challenges," *IEEE Internet Things J.*, vol. 6, no. 2, pp. 2159–2187, Apr. 2019.
[19] M. A. Ferrag, L. A. Maglaras, H. Janicke, J. Jiang, and L. Shu, "Authentication protocols for Internet of Things: A comprehensive survey," *Secur. Commun. Netw.*, vol. 2017, pp. 1–41, Nov. 2017.
[20] C. Brewster, I. Roussaki, N. Kalatzis, K. Doolin, and K. Ellis, "IoT in agriculture: Designing a Europe-wide large-scale pilot," *IEEE Commun. Mag.*, vol. 55, no. 9, pp. 26–33, Sep. 2017.
[21] P. P. Ray, "Internet of things for smart agriculture: Technologies, practices and future direction," *AIS*, vol. 9, no. 4, pp. 395–420, Jun. 2017.
[22] A. Khanna and S. Kaur, "Evolution of Internet of Things (IoT) and its significant impact in the field of precision agriculture," *Comput. Electron. Agricult.*, vol. 157, pp. 218–231, Feb. 2019.
[23] J. Ruan, Y. Wang, F. T. S. Chan, X. Hu, M. Zhao, F. Zhu, B. Shi, Y. Shi, and F. Lin, "A life cycle framework of green IoT-based agriculture and its finance, operation, and management issues," *IEEE Commun. Mag.*, vol. 57, no. 3, pp. 90–96, Mar. 2019.
[24] K. T. Nguyen, M. Laurent, and N. Oualha, "Survey on secure communication protocols for the Internet of Things," *Ad Hoc Netw.*, vol. 32, pp. 17–31, Sep. 2015.
[25] J. Granjal, E. Monteiro, and J. S. Silva, "Security for the Internet of Things: A survey of existing protocols and open research issues," *IEEE Commun. Surveys Tuts.*, vol. 17, no. 3, pp. 1294–1312, 3rd Quart., 2015.
[26] F. A. Alaba, M. Othman, I. A. T. Hashem, and F. Alotaibi, "Internet of Things security: A survey," *J. Netw. Comput. Appl.*, vol. 88, pp. 10–28, Jun. 2017.
[27] J. Lin, W. Yu, N. Zhang, X. Yang, H. Zhang, and W. Zhao, "A survey on Internet of Things: Architecture, enabling technologies, security and privacy, and applications," *IEEE Internet Things J.*, vol. 4, no. 5, pp. 1125–1142, Oct. 2017.
[28] Y. Yang, L. Wu, G. Yin, L. Li, and H. Zhao, "A survey on security and privacy issues in Internet-of-Things," *IEEE Internet Things J.*, vol. 4, no. 5, pp. 1250–1258, Oct. 2017.
[29] M. A. Khan and K. Salah, "IoT security: Review, blockchain solutions, and open challenges," *Future Gener. Comput. Syst.*, vol. 82, pp. 395–411, May 2018.
[30] M. Ammar, G. Russello, and B. Crispo, "Internet of Things: A survey on the security of IoT frameworks," *J. Inf. Secur. Appl.*, vol. 38, pp. 8–27, Feb. 2018.
[31] A. Altaf, H. Abbas, F. Iqbal, and A. Derhab, "Trust models of Internet of smart things: A survey, open issues, and future directions," *J. Netw. Comput. Appl.*, vol. 137, pp. 93–111, Jul. 2019.
[32] A.-R. Sadeghi, C. Wachsmann, and M. Waidner, "Security and privacy challenges in industrial Internet of Things," in *Proc. 52nd ACM/EDAC/IEEE Design Autom. Conf. (DAC)*, Jun. 2015, pp. 1–6.
[33] 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.
[34] A. Dorri, S. S. Kanhere, R. Jurdak, and P. Gauravaram, "Blockchain for IoT security and privacy: The case study of a smart home," in *Proc. IEEE Int. Conf. Pervas. Comput. Commun. Workshops (PerCom Workshops)*, Mar. 2017, pp. 618–623.
[35] D. E. Kouicem, A. Bouabdallah, and H. Lakhlef, "Internet of Things security: A top-down survey," *Comput. Netw.*, vol. 141, pp. 199–221, Aug. 2018.
[36] A. Panarello, N. Tapas, G. Merlino, F. Longo, and A. Puliafito, "Blockchain and IoT integration: A systematic survey," *Sensors*, vol. 18, no. 8, p. 2575, Aug. 2018.
[37] F. Dalipi and S. Y. Yayilgan, "Security and privacy considerations for IoT application on smart grids: Survey and research challenges," in *Proc. IEEE 4th Int. Conf. Future Internet Things Cloud Workshops (FiCloudW)*, Aug. 2016, pp. 63–68.
[38] A. Tzounis, N. Katsoulas, T. Bartzanas, and C. Kittas, "Internet of Things in agriculture, recent advances and future challenges," *Biosyst. Eng.*, vol. 164, pp. 31–48, Dec. 2017.
[39] M. A. Ferrag, M. Derdour, M. Mukherjee, A. Derhab, L. Maglaras, and H. Janicke, "Blockchain technologies for the Internet of Things: Research issues and challenges," *IEEE Internet Things J.*, vol. 6, no. 2, pp. 2188–2204, Apr. 2019.
[40] M. Srbinovska, C. Gavrovski, V. Dimcev, A. Krkoleva, and V. Borozan, "Environmental parameters monitoring in precision agriculture using wireless sensor networks," *J. Cleaner Prod.*, vol. 88, pp. 297–307, Feb. 2015.
[41] K.-T. Chen, H.-H. Zhang, T.-T. Wu, J. Hu, C.-Y. Zhai, and D. Wang, "Design of monitoring system for multilayer soil temperature and moisture based on WSN," in *Proc. Int. Conf. Wireless Commun. Sensor Netw.*, Dec. 2014, pp. 425–430.
[42] M. Mafuta, M. Zennaro, A. Bagula, G. Ault, H. Gombachika, and T. Chadza, "Successful deployment of a wireless sensor network for precision agriculture in Malawi," *Int. J. Distrib. Sensor Netw.*, vol. 9, no. 5, May 2013, Art. no. 150703.
[43] O. Postolache, M. Pereira, and P. Girão, "Sensor network for environment monitoring: Water quality case study," in *Proc. 4th Symp. Environ. Instrum. Meas.*, Lecce, Italy, 2013, pp. 30–34.
[44] D. D. Wu, D. L. Olson, and J. R. Birge, "Risk management in cleaner production," *J. Cleaner Prod.*, vol. 53, pp. 1–6, Aug. 2013.
[45] J. Huuskonen and T. Oksanen, "Soil sampling with drones and augmented reality in precision agriculture," *Comput. Electron. Agricult.*, vol. 154, pp. 25–35, Nov. 2018.
[46] S. Ehsan, K. Bradford, M. Brugger, B. Hamdaoui, Y. Kovchegov, D. Johnson, and M. Louhaichi, "Design and analysis of delay-tolerant sensor networks for monitoring and tracking free-roaming animals," *IEEE Trans. Wireless Commun.*, vol. 11, no. 3, pp. 1220–1227, Mar. 2012.
[47] D. Liu, Y. Gong, G. Wang, X. Chen, X. Zhang, and G. Wu, "Research advances in mechanization of pesticide spraying technology for facility agriculture," *Asian Agricult. Res.*, vol. 10, pp. 81–86, Jul. 2018.
[48] V. V. H. Ram, H. Vishal, S. Dhanalakshmi, and P. M. Vidya, "Regulation of water in agriculture field using Internet Of Things," in *Proc. IEEE Technol. Innov. ICT Agricult. Rural Develop. (TIAR)*, Jul. 2015, pp. 112–115.
[49] M.-S. Liao, S.-F. Chen, C.-Y. Chou, H.-Y. Chen, S.-H. Yeh, Y.-C. Chang, and J.-A. Jiang, "On precisely relating the growth of Phalaenopsis leaves to greenhouse environmental factors by using an IoT-based monitoring system," *Comput. Electron. Agricult.*, vol. 136, pp. 125–139, Apr. 2017.
[50] A. Castañeda, D. Doan, D. Newhouse, M. C. Nguyen, H. Uematsu, and J. P. Azevedo, "A new profile of the global poor," *World Develop.*, vol. 101, pp. 250–267, Jan. 2018.
[51] M. F. Bellemare and J. R. Bloem, "Does contract farming improve welfare? A review," *World Develop.*, vol. 112, pp. 259–271, Dec. 2018.
[52] J. M. Talavera, L. E. Tobón, J. A. Gómez, M. A. Culman, J. M. Aranda, D. T. Parra, L. A. Quiroz, A. Hoyos, and L. E. Garreta, "Review of IoT applications in agro-industrial and environmental fields," *Comput. Electron. Agricult.*, vol. 142, pp. 283–297, Nov. 2017.
[53] L. Minbo, Z. Zhu, and C. Guangyu, "Information service system of agriculture IoT," *Automatika*, vol. 54, no. 4, pp. 415–426, Jan. 2013.
[54] Y. Liu, W. Han, Y. Zhang, L. Li, J. Wang, and L. Zheng, "An Internet-of-Things solution for food safety and quality control: A pilot project in China," *J. Ind. Inf. Integr.*, vol. 3, pp. 1–7, Sep. 2016.

[55] J. Wang and H. Yue, "Food safety pre-warning system based on data mining for a sustainable food supply chain," *Food Control*, vol. 73, pp. 223–229, Mar. 2017.

[56] F. Capello, M. Toja, and N. Trapani, "A real-time monitoring service based on industrial Internet of Things to manage agri-food logistics," in *Proc. 6th Int. Conf. Inf. Syst., Logistics Supply Chain*, Bordeaux, France, pp. 10–21, 2016. Accessed: 2016. [Online]. Available: http://ils2016conference.com/wpcontent/uploads/2015/03/ILS2016_FB01_1.pdf

[57] M. Mukherjee, R. Matam, L. Shu, L. Maglaras, M. A. Ferrag, N. Choudhury, and V. Kumar, "Security and privacy in fog computing: Challenges," *IEEE Access*, vol. 5, pp. 19293–19304, 2017.

[58] M. Mukherjee, L. Shu, and D. Wang, "Survey of fog computing: Fundamental, network applications, and research challenges," *IEEE Commun. Surveys Tuts.*, vol. 20, no. 3, pp. 1826–1857, 3rd Quart., 2018.

[59] V. B. C. Souza, W. Ramirez, X. Masip-Bruin, E. Marin-Tordera, G. Ren, and G. Tashakor, "Handling service allocation in combined fog-cloud scenarios," in *Proc. IEEE Int. Conf. Commun. (ICC)*, May 2016, pp. 1–5.

[60] Y. Xu, V. Mahendran, and S. Radhakrishnan, "SDN docker: Enabling application auto-docking/undocking in edge switch," in *Proc. IEEE Conf. Comput. Commun. Workshops (INFOCOM WKSHPS)*, Apr. 2016, pp. 864–869.

[61] R. Graziani and B. Vachon, *Connecting Networks Companion Guide*. San Jose, CA, USA: Cisco Press, 2014.

[62] M. Roopaei, P. Rad, and K.-K.-R. Choo, "Cloud of things in smart agriculture: intelligent irrigation monitoring by thermal imaging," *IEEE Cloud Comput.*, vol. 4, no. 1, pp. 10–15, Jan. 2017.

[63] M. A. Ferrag, L. Maglaras, and A. Derhab, "Authentication and authorization for mobile IoT devices using biofeatures: Recent advances and future trends," *Secur. Commun. Netw.*, vol. 2019, pp. 1–20, May 2019.

[64] L. Guo, C. Zhang, J. Sun, and Y. Fang, "A privacy-preserving attribute-based authentication system for mobile health networks," *IEEE Trans. Mobile Comput.*, vol. 13, no. 9, pp. 1927–1941, Sep. 2014.

[65] S. Salamatian, W. Huleihel, A. Beirami, A. Cohen, and M. Medard, "Why botnets work: Distributed brute-force attacks need no synchronization," *IEEE Trans. Inf. Forensics Security*, vol. 14, no. 9, pp. 2288–2299, Sep. 2019.

[66] C. Lai, H. Li, X. Liang, R. Lu, K. Zhang, and X. Shen, "CPAL: A conditional privacy-preserving authentication with access linkability for roaming service," *IEEE Internet Things J.*, vol. 1, no. 1, pp. 46–57, Feb. 2014.

[67] X. Yao, Z. Chen, and Y. Tian, "A lightweight attribute-based encryption scheme for the Internet of Things," *Future Gener. Comput. Syst.*, vol. 49, pp. 104–112, Aug. 2015.

[68] Z. Yan, W. Ding, V. Niemi, and A. V. Vasilakos, "Two schemes of privacy-preserving trust evaluation," *Future Gener. Comput. Syst.*, vol. 62, pp. 175–189, Sep. 2016.

[69] G. Sun, V. Chang, M. Ramachandran, Z. Sun, G. Li, H. Yu, and D. Liao, "Efficient location privacy algorithm for Internet of Things (IoT) services and applications," *J. Netw. Comput. Appl.*, vol. 89, pp. 3–13, Jul. 2017.

[70] R. Lu, K. Heung, A. H. Lashkari, and A. A. Ghorbani, "A lightweight privacy-preserving data aggregation scheme for fog computing-enhanced IoT," *IEEE Access*, vol. 5, pp. 3302–3312, 2017.

[71] Q. Wang, D. Chen, N. Zhang, Z. Qin, and Z. Qin, "LACS: A lightweight label-based access control scheme in IoT-based 5G caching context," *IEEE Access*, vol. 5, pp. 4018–4027, 2017.

[72] K. Gai, K.-K.-R. Choo, M. Qiu, and L. Zhu, "Privacy-preserving content-oriented wireless communication in Internet-of-Things," *IEEE Internet Things J.*, vol. 5, no. 4, pp. 3059–3067, Aug. 2018.

[73] P. Gope, R. Amin, S. K. Hafizul Islam, N. Kumar, and V. K. Bhalla, "Lightweight and privacy-preserving RFID authentication scheme for distributed IoT infrastructure with secure localization services for smart city environment," *Future Gener. Comput. Syst.*, vol. 83, pp. 629–637, Jun. 2018.

[74] Y. Zhang, S. Kasahara, Y. Shen, X. Jiang, and J. Wan, "Smart contract-based access control for the Internet of Things," *IEEE Internet Things J.*, vol. 6, no. 2, pp. 1594–1605, Apr. 2019.

[75] Z. Guan, Y. Zhang, L. Wu, J. Wu, J. Li, Y. Ma, and J. Hu, "APPA: An anonymous and privacy preserving data aggregation scheme for fog-enhanced IoT," *J. Netw. Comput. Appl.*, vol. 125, pp. 82–92, Jan. 2019.

[76] K. Fan, H. Xu, L. Gao, H. Li, and Y. Yang, "Efficient and privacy preserving access control scheme for fog-enabled IoT," *Future Gener. Comput. Syst.*, vol. 99, pp. 134–142, Oct. 2019.

[77] X. Zhang, C. Liu, S. Poslad, and K. K. Chai, "A provable semi-outsourcing privacy preserving scheme for data transmission from IoT devices," *IEEE Access*, vol. 7, pp. 87169–87177, 2019.

[78] S. Li, M. Li, H. Xu, and X. Zhou, "Searchable encryption scheme for personalized privacy in IoT-based big data," *Sensors*, vol. 19, no. 5, p. 1059, Mar. 2019.

[79] W. Jiang, H. Li, G. Xu, M. Wen, G. Dong, and X. Lin, "PTAS: Privacy-preserving thin-client authentication scheme in blockchain-based PKI," *Future Gener. Comput. Syst.*, vol. 96, pp. 185–195, Jul. 2019.

[80] Q. Li, X. Zhang, Q. Zheng, R. Sandhu, and X. Fu, "LIVE: Lightweight integrity verification and content access control for named data networking," *IEEE Trans. Inf. Forensics Security*, vol. 10, no. 2, pp. 308–320, Feb. 2015.

[81] A. Ouaddah, A. Abou Elkalam, and A. Ait Ouahman, "FairAccess: A new Blockchain-based access control framework for the Internet of Things," *Secur. Commun. Netw.*, vol. 9, no. 18, pp. 5943–5964, Dec. 2016.

[82] S. Mondal, K. P. Wijewardena, S. Karuppuswami, N. Kriti, D. Kumar, and P. Chahal, "Blockchain inspired RFID-based information architecture for food supply chain," *IEEE Internet Things J.*, vol. 6, no. 3, pp. 5803–5813, Jun. 2019.

[83] M. Alaslani, F. Nawab, and B. Shihada, "Blockchain in IoT systems: End-to-end delay evaluation," *IEEE Internet Things J.*, vol. 6, no. 5, pp. 8332–8344, Oct. 2019.

[84] M. Wu, K. Wang, X. Cai, S. Guo, M. Guo, and C. Rong, "A comprehensive survey of blockchain: From theory to IoT applications and beyond," *IEEE Internet Things J.*, vol. 6, no. 5, pp. 8114–8154, Oct. 2019.

[85] Y. Sun, L. Zhang, G. Feng, B. Yang, B. Cao, and M. A. Imran, "Blockchain-enabled wireless Internet of Things: Performance analysis and optimal communication node deployment," *IEEE Internet Things J.*, vol. 6, no. 3, pp. 5791–5802, Jun. 2019.

[86] P. K. Sharma, S. Singh, Y.-S. Jeong, and J. H. Park, "DistBlockNet: A distributed blockchains-based secure SDN architecture for IoT networks," *IEEE Commun. Mag.*, vol. 55, no. 9, pp. 78–85, Sep. 2017.

[87] O. Novo, "Blockchain meets IoT: An architecture for scalable access management in IoT," *IEEE Internet Things J.*, vol. 5, no. 2, pp. 1184–1195, Apr. 2018.

[88] L. Zhou, L. Wang, Y. Sun, and P. Lv, "BeeKeeper: A blockchain-based IoT system with secure storage and homomorphic computation," *IEEE Access*, vol. 6, pp. 43472–43488, 2018.

[89] M. T. Hammi, B. Hammi, P. Bellot, and A. Serhrouchni, "Bubbles of trust: A decentralized blockchain-based authentication system for IoT," *Comput. Secur.*, vol. 78, pp. 126–142, Sep. 2018.

[90] M. P. Caro, M. S. Ali, M. Vecchio, and R. Giaffreda, "Blockchain-based traceability in Agri-Food supply chain management: A practical implementation," in *Proc. IoT Vertical Topical Summit Agricult.-Tuscany (IOT Tuscany)*, May 2018, pp. 1–4.

[91] M. Shen, X. Tang, L. Zhu, X. Du, and M. Guizani, "Privacy-preserving support vector machine training over blockchain-based encrypted IoT data in smart cities," *IEEE Internet Things J.*, vol. 6, no. 5, pp. 7702–7712, Oct. 2019.

[92] M. Ma, G. Shi, and F. Li, "Privacy-oriented blockchain-based distributed key management architecture for hierarchical access control in the IoT scenario," *IEEE Access*, vol. 7, pp. 34045–34059, 2019.

[93] V. Dedeoglu, R. Jurdak, G. D. Putra, A. Dorri, and S. S. Kanhere, "A trust architecture for blockchain in IoT," 2019, *arXiv:1906.11461*. [Online]. Available: http://arxiv.org/abs/1906.11461

[94] S. Ding, J. Cao, C. Li, K. Fan, and H. Li, "A novel attribute-based access control scheme using blockchain for IoT," *IEEE Access*, vol. 7, pp. 38431–38441, 2019.

[95] H. Si, C. Sun, Y. Li, H. Qiao, and L. Shi, "IoT information sharing security mechanism based on blockchain technology," *Future Gener. Comput. Syst.*, vol. 101, pp. 1028–1040, Dec. 2019.

[96] A. Derhab, M. Guerroumi, A. Gumaei, L. Maglaras, M. A. Ferrag, M. Mukherjee, and F. A. Khan, "Blockchain and random subspace learning-based IDS for SDN-enabled industrial IoT security," *Sensors*, vol. 19, no. 14, p. 3119, Jul. 2019.

[97] A. Shamir, "How to share a secret," *Commun. ACM*, vol. 22, no. 11, pp. 612–613, 1979.

[98] S. Nakamoto. (2008). *Bitcoin: A Peer-to-Peer Electronic Cash System*. [Online]. Available: https://bitcoin.org/bitcoin.pdf

[99] *Peercoin*. Accessed: Jul. 25, 2019. [Online]. Available: https://peercoin.net/

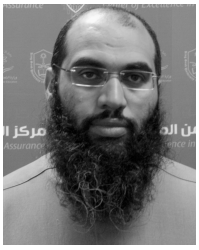
[100] *NXT*. Accessed: Jul. 25, 2019. [Online]. Available: https://nxtplatform.org/

[101] *Bitshares*. Accessed: Jul. 25, 2019. [Online]. Available: https://bitshares.org/
[102] *Steemit*. Accessed: Jul. 25, 2019. [Online]. Available: https://steemit.com/trending/blockchain
[103] *Komodo*. Accessed: Jul. 25, 2019. [Online]. Available: https://komodoplatform.com/
[104] *Burstcoin*. Accessed: Jul. 25, 2019. [Online]. Available: https://www.burst-coin.org/
[105] L. Ren. (2014). *Proof of Stake Velocity: Building the Social Currency of the Digital Age*. [Online]. Available: https://bravenewcoin.com/insights/proof-of-stake-velocity–building-the-social-currency-of-the-digital-age
[106] *Poa.network*. Accessed: Jul. 25, 2019. [Online]. Available: https://poa.network/
[107] *Vechain*. Accessed: Jul. 25, 2019. [Online]. Available: https://www.vechain.org/
[108] *Solana*. Accessed: Jul. 25, 2019. [Online]. Available: https://solana.io/
[109] *Decred*. Accessed: Jul. 25, 2019. [Online]. Available: https://www.decred.org/
[110] Y. Gilad, R. Hemo, S. Micali, G. Vlachos, and N. Zeldovich, "Algorand: Scaling Byzantine agreements for cryptocurrencies," in *Proc. 26th Symp. Oper. Syst. Princ.*, 2017, pp. 51–68.
[111] *Slimcoin*. Accessed: Jul. 25, 2019. [Online]. Available: http://slimco.in/
[112] *Hyperledger Sawtooth*. Accessed: Jul. 25, 2019. [Online]. Available: https://sawtooth.hyperledger.org/docs/core/releases/1.0/architecture/poet.html
[113] *Nem*. Accessed: Jul. 25, 2019. [Online]. Available: https://nem.io/
[114] D. Mazieres, "The stellar consensus protocol: A federated model for internet-level consensus," in *Proc. Stellar Develop. Found.*, 2015, p. 32.
[115] *Gochain*. Accessed: Jul. 25, 2019. [Online]. Available: https://gochain.io/
[116] *Neo*. Accessed: Jul. 25, 2019. [Online]. Available: https://neo.org
[117] *Ripple*. Accessed: Jul. 25, 2019. [Online]. Available: https://www.ripple.com/
[118] M. A. Ferrag and L. Maglaras, "DeepCoin: A novel deep learning and blockchain-based energy exchange framework for smart grids," *IEEE Trans. Eng. Manage.*, to be published.
[119] *Hyperledger Fabric*. Accessed: Jul. 25, 2019. [Online]. Available: https://www.hyperledger.org/projects/fabric
[120] M. A. Ferrag and L. Maglaras, "DeliveryCoin: An IDS and blockchain-based delivery framework for drone-delivered services," *Computers*, vol. 8, no. 3, p. 58, Aug. 2019.
[121] *Stellar*. Accessed: Jul. 25, 2019. [Online]. Available: https://www.stellar.org
[122] *Dispatch*. Accessed: Jul. 25, 2019. [Online]. Available: https://www.dispatchlabs.io/
[123] G. Zyskind, O. Nathan, and A. Pentland, "Decentralizing privacy: Using blockchain to protect personal data," in *Proc. IEEE Secur. Privacy Workshops*, May 2015, pp. 180–184.
[124] I. Bentov, C. Lee, A. Mizrahi, and M. Rosenfeld, "Proof of activity: Extending bitcoin's proof of work via proof of stake [extended abstract]," *SIGMETRICS Perform. Eval. Rev.*, vol. 42, no. 3, pp. 34–37, Dec. 2014.
[125] *Slimcoin : A Peer-to-Peer Crypto-Currency With Proof-of-Burn*. Accessed: Jul. 25, 2019. [Online]. Available: https://github.com/slimcoin-project/slimcoin-project.github.io/raw/master/whitepaperSLM.pdf
[126] M. Castro and B. Liskov, "Practical Byzantine fault tolerance," in *Proc. OSDI*, 1999, pp. 173–186.
[127] K. Kaur, S. Garg, G. Kaddoum, F. Gagnon, and S. Hassan Ahmed, "Blockchain-based lightweight authentication mechanism for vehicular fog infrastructure," 2019, *arXiv:1904.01168*. [Online]. Available: http://arxiv.org/abs/1904.01168
[128] A. Clement, E. L. Wong, L. Alvisi, M. Dahlin, and M. Marchetti, "Making Byzantine fault tolerant systems tolerate byzantine faults," in *Proc. NSDI*, vol. 9, 2009, pp. 153–168.
[129] R. Kotla, L. Alvisi, M. Dahlin, A. Clement, and E. Wong, "Zyzzyva: Speculative Byzantine fault tolerance," *ACM Trans. Comput. Syst. (TOCS)*, vol. 27, no. 4, p. 7, 2009.
[130] J. Cowling, D. Myers, B. Liskov, R. Rodrigues, and L. Shrira, "HQ replication: A hybrid quorum protocol for Byzantine fault tolerance," in *Proc. 7th Symp. Oper. Syst. Design Implement.* Berkeley, CA, USA: USENIX Association, 2006, pp. 177–190.
[131] M. Abd-El-Malek, G. R. Ganger, G. R. Goodson, M. K. Reiter, and J. J. Wylie, "Fault-scalable Byzantine fault-tolerant services," *SIGOPS Oper. Syst. Rev.*, vol. 39, no. 5, p. 59, Oct. 2005.
[132] R. Guerraoui, N. Knežević, V. Quéma, and M. Vukolić, "The next 700 BFT protocols," in *Proc. 5th Eur. Conf. Comput. Syst.*, 2010, pp. 363–376.
[133] *Byteball Consensus*. Accessed: Jul. 25, 2019. [Online]. Available: https://obyte.org/
[134] *Mokka Consensus*. Accessed: Jul. 25, 2019. [Online]. Available: https://ega-forever.github.io/mokka/
[135] *Spectre Consensus*. Accessed: Jul. 25, 2019. [Online]. Available: https://eprint.iacr.org/2016/1159.pdf
[136] C. LeMahieu. (2018). *Nano: A Feeless Distributed Cryptocurrency Network*. [Online]. Available: https://nano. org/en/whitepaper
[137] *Hashgraph Consensus*. Accessed: Jul. 25, 2019. [Online]. Available: https://www.hedera.com/whitepaper
[138] *Tangle Consensus*. Accessed: Jul. 25, 2019. [Online]. Available: http://tanglereport.com/wp-content/uploads/2018/01/IOTA_Whitepaper.pdf
[139] *Iota*. Accessed: Jul. 25, 2019. [Online]. Available: https://www.iota.org/
[140] *Iost*. Accessed: Jul. 25, 2019. [Online]. Available: https://iost.io/
[141] *Raft Consensus*. Accessed: Jul. 25, 2019. [Online]. Available: https://raft.github.io/raft.pdf
[142] *KDD cup 1999*. Accessed: Aug. 30, 2019. [Online]. Available: http://kdd.ics.uci.edu/databases/kddcup99/kddcup99.html
[143] *NSL KDD*. Accessed: Aug. 30, 2019. [Online]. Available: https://www.unb.ca/cic/datasets/nsl.html
[144] *Cicds2017 Dataset*. Accessed: Aug. 30, 2019. [Online]. Available: https://www.unb.ca/cic/datasets/ids-2017.html
[145] *Bot-IoT Dataset*. Accessed: Aug. 30, 2019. [Online]. Available: https://www.unsw.adfa.edu.au/unsw-canberra-cyber/cybersecurity/ADFA-NB15-Datasets/bot_iot.php
[146] *CSE-CIC-IDS 2018 Dataset*. Accessed: Aug. 30, 2019. [Online]. Available: https://www.unb.ca/cic/datasets/ids-2018.html
[147] H. Yang, Q. Zhou, M. Yao, R. Lu, H. Li, and X. Zhang, "A practical and compatible cryptographic solution to ADS-B security," *IEEE Internet Things J.*, vol. 6, no. 2, pp. 3322–3334, Apr. 2019.
[148] R. Khan, P. Kumar, D. N. K. Jayakody, and M. Liyanage, "A survey on security and privacy of 5G technologies: Potential solutions, recent advancements and future directions," *IEEE Commun. Surveys Tuts.*, to be published.
[149] L. Mottola and G. P. Picco, "Programming wireless sensor networks: Fundamental concepts and state of the art," *ACM Comput. Surv.*, vol. 43, no. 3, p. 19, 2011.
[150] K. Langendoen, A. Baggio, and O. Visser, "Murphy loves potatoes: Experiences from a pilot sensor network deployment in precision agriculture," in *Proc. 20th IEEE Int. Parallel Distrib. Process. Symp.*, Apr. 2006, p. 8.
[151] K. Bannister, G. Giorgetti, and S. Gupta, "Wireless sensor networking for hot applications: Effects of temperature on signal strength, data collection and localization," in *Proc. 5th Workshop Embedded Netw. Sensors (HotEmNets)*, 2008, pp. 1–5.

MOHAMED AMINE FERRAG received the bachelor's, master's, and Ph.D. degrees from Badji Mokhtar University, Algeria, in June 2008, June 2010, and June 2014, respectively, all in computer science. Since October 2014, he has been an Assistant Professor with the Department of Computer Science, University of Guelma, Algeria. Since July 2019, he has been a Visiting Senior Researcher with the NAU-Lincoln Joint Research Center of Intelligent Engineering, Nanjing Agricultural University, China. He has been conducting several research projects with international collaborations on these topics. He participated in many international conferences worldwide and has been granted short-term research visitor internships to many renowned universities including, De Montfort University, U.K., and Istanbul Technical University, Turkey. His research interests include wireless network security, network coding security, and applied cryptography. He is currently serving on various editorial positions such as an Editorial Board Member in Journals (Indexed SCI & Scopus) such as, *IET Networks*, the *International Journal of Internet Technology and Secured Transactions* (Inderscience Publishers), *EAI Endorsed Transactions on Security and Safety* (EAI), the *International Journal of Web Services Research* (IJWSR) (IGI Global), and the *International Journal on Semantic Web and Information Systems* (IJSWIS) (IGI Global).

LEI SHU (Senior Member, IEEE) received the B.S. degree in computer science from South Central University for Nationalities, China, in 2002, the M.S. degree in computer engineering from Kyung Hee University, South Korea, in 2005, and the Ph.D. degree from the Digital Enterprise Research Institute, National University of Ireland, Galway, Ireland, in 2010. Until 2012, he was a Specially Assigned Researcher with the Department of Multimedia Engineering, Graduate School of Information Science and Technology, Osaka University, Japan. He is currently a Distinguished Professor with Nanjing Agricultural University, China, and a Lincoln Professor with the University of Lincoln, U.K. He is also the Director of the NAU-Lincoln Joint Research Center of Intelligent Engineering. He has published more than 400 articles in related conferences, journals, and books in the areas of sensor networks and Internet of Things. His current H-index is 54 and i10-index is 197 in Google Scholar Citation. His current research interests include wireless sensor networks and the Internet of Things. He has also served as a TPC member for more than 150 conferences, such as ICDCS, DCOSS, MASS, ICC, GLOBECOM, ICCCN, WCNC, and ISCC. He was a recipient of the 2014 Top Level Talents in Sailing Plan of Guangdong Province, China, the 2015 Outstanding Young Professor of Guangdong Province, and the GLOBECOM 2010, ICC 2013, ComManTel 2014, WICON 2016, SigTelCom 2017 Best Paper Awards, the 2017 and 2018 IEEE Systems Journal Best Paper Awards, the 2017 *Journal of Network and Computer Applications* Best Research Paper Award, and the Outstanding Associate Editor Award of 2017, and the 2018 IEEE Access. He has also served more than 50 various Co-Chair for international conferences/workshops, such as IWCMC, ICC, ISCC, ICNC, Chinacom, especially the Symposium Co-Chair for IWCMC 2012, ICC 2012, the General Co-Chair for Chinacom 2014, Qshine 2015, Collaboratecom 2017, DependSys 2018, and SCI 2019, the TPC Chair for InisCom 2015, NCCA 2015, WICON 2016, NCCA 2016, Chinacom 2017, InisCom 2017, WMNC 2017, and NCCA 2018.

XING YANG received the M.S. degree in control engineering from the Nanjing University of Information Science and Technology, China, in 2018. He is currently pursuing the Ph.D. degree with the College of Engineering, Nanjing Agricultural University, China. His current research interests include fault diagnosis in wireless sensor networks, the agricultural Internet of Things, and machine learning algorithms.



ABDELOUAHID DERHAB received the engineering, master's, and Ph.D. degrees in computer science from the University of Sciences and Technology Houari Boummediene (USTHB), Algiers, in 2001, 2003, and 2007, respectively. From 2002 to 2012, he was a full-time Researcher with the CERIST Research Center, Algeria. He is currently an Assistant Professor with the Center of Excellence in Information Assurance (COEIA), King Saud University. His interest research areas are network security, intrusion detection systems, malware analysis, mobile security, and mobile networks.

LEANDROS MAGLARAS (Senior Member, IEEE) received the B.Sc. degree from the Aristotle University of Thessaloniki, Greece, in 1998, the M.Sc. degree in industrial production and management from the University of Thessaly, in 2004, and the M.Sc. and Ph.D. degrees in electrical & computer engineering from the University of Volos, in 2008 and 2014, respectively. He is currently the Head of the National Cyber Security Authority of Greece and a Visiting Lecturer with the School of Computer Science and Informatics, De Montfort University, U.K. He has authored more than 80 articles in scientific magazines and conferences. His research interests include wireless sensor networks and vehicular ad hoc networks. He serves on the Editorial Board of several international peer-reviewed journals such as IEEE Access, the *Journal on Security & Communication Networks* (Wiley), *EAI Transactions on e-Learning*, *EAI Transactions on Industrial Networks*, and the *Journal of Intelligent Systems*.