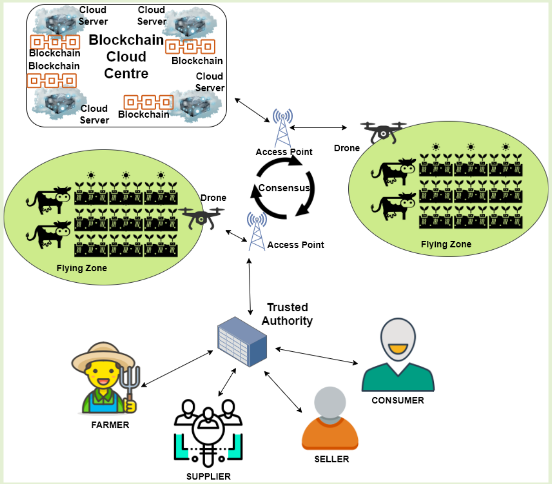
Smart Secure Sensing for IoT-Based Agriculture: Blockchain Perspective

Anusha Vangala, Ashok Kumar Das, *Senior Member, IEEE*, Neeraj Kumar, *Senior Member, IEEE*, and Mamoun Alazab, *Senior Member, IEEE*

***Abstract*—Agriculture is a vital area for the sustenance of mankind engulfing manufacturing, security, traceability, and sustainable resource management. With the resources receding expeditiously, it is of utmost significance to innovate techniques that help in the subsistence of agriculture. The growth of Internet of Things (IoT) and Blockchain technology as two rapidly emerging fields can ameliorate the state of food chain today. This paper provides a rigorous literature review to inspect the state-of-the-art development of the schemes that provide information security using blockchain technology. After identifying the core requirements in smart agriculture, a generalized blockchain-based security architecture has been proposed. A detailed cost analysis has been conducted on the studied schemes. A meticulous comparative analysis uncovered the drawbacks in existing research. Furthermore, detailed analysis of the literature has also revealed the security goals towards which the research has been directed and helped to identify new avenues for future research using artificial intelligence.**



***Index Terms*—Smart agriculture, Internet of Things (IoT), blockchain technology, authentication, security.**

I. Introduction

According to the survey report in [1] by the Department of Economic and Social Affairs, United Nations, the world population could reach 11 billions by the year 2100, with more than 50% concentrated in 9 countries due to a net outflow of more than 1 million in the decade 2010-2020 from the other countries to these nine countries. Even though the population growth rate has decreased below 1.1% per year in 2015-2020, human life expectancy has increased since 1990 by more than 8 years, with an average of 72.8 years per person.

The Food and Agriculture Organization of the United Nations published a detailed report [2] on the amount of food that is wasted due to various factors during pre-harvest, harvest and post-harvest stages, and the depth of its impact on the economy, environment, health and survival of human race. It uses Food Loss Index (FLI) as an indicative parameter for the percentage of food that is taken off the supply chain. The studies indicate that about 14% of the produced foods is lost by post-harvest stage globally. The wastage may be in terms of quantitative loss of food leading to reduced amount of food available for consumption. This is countered using concepts of providing security to food. The other more prevalent form of food wastage is qualitative food wastage which reduces the attributes in a food that makes it unconsumable such as the nutritional value of the food, non-compliance with food standards and their economic impact.

Duque-Acevedo *et al.* [3] provided a very deep and through analytical study of the food wastage statistics from 1931 to 2018 and the impact of global economic policies on food

Manuscript received June 17, 2020; revised July 16, 2020; accepted July 23, 2020. Date of publication July 27, 2020; date of current version August 13, 2021. This work was supported in part by the Mathematical Research Impact Centric Support (MATRICS) Project funded by the Science and Engineering Research Board (SERB), India, under Grant MTR/2019/000699 and in part by the Ripple Centre of Excellence Scheme, CoE in Blockchain (Sanction No. IIIT/R&D Office/Internal Projects/001/2019), IIIT Hyderabad, India. The associate editor coordinating the review of this article and approving it for publication was Dr. Hari P. Gupta. *(Corresponding authors: Neeraj Kumar; Mamoun Alazab.)*

Anusha Vangala and Ashok Kumar Das are with the Center for Security, Theory and Algorithmic Research, International Institute of Information Technology Hyderabad, Hyderabad 500 032, India (e-mail: anusha.vangala@research.iiit.ac.in; iitkgp.akdas@gmail.com).

Neeraj Kumar is with the Department of Computer Science and Engineering, Thapar Institute of Engineering and Technology, Patiala 147 004, India, also with the Department of Computer Science and Information Engineering, Asia University, Taiwan, also with King Abdul Aziz University, Jeddah, Saudi Arabia, and also with Charles Darwin University, Australia (e-mail: neeraj.kumar@thapar.edu).

Mamoun Alazab is with the College of Engineering, IT and Environment, Charles Darwin University, Casuarina, NT 0810, Australia (e-mail: alazab.m@ieee.org).

Digital Object Identifier 10.1109/JSEN.2020.3012294

wastage. They also studied the effect of new global framework on sustainable development on local policies of different countries. The Food Wastage Footprint–Full Cost Accounting Report [4] by the Food and Agriculture Organization of the United Nations provides a very thorough and detailed study of several statistical methodologies and models that can accurately calculate the cost of wastage of food on various economic and social factors required to sustain the world. It also studies the different factors, natural and otherwise, that affects food wastage directly or indirectly. These statistics suggest the exigency for planning an efficient solution for food production and distribution throughout the world.

A. Need for IoT in Agriculture

An *IoT connected device* has the ability to sense the surrounding environment to take necessary readings and send the data through the internet to a server, that can store the data for future use or to another device, like a smart phone, where a user can view the data. This allows continuous monitoring of a system under review. Such a monitored environment allows the user to take decisions on the actions to be performed [5].

A *smart sensing environment* consists of a connected network of devices which can constantly send and receive each other's data. In addition, it also has the capability to take decisions on behalf of a user and perform an action on the environment in order to improve its condition. This change imposed on the environment calls for further monitoring of the surroundings, and thus, continuously moves towards an evolving environment. In a smart sensing system, the user may be sent the monitored data, actions taken and effect of actions on the environment. The user may further have the choice to impose an action different from the one determined by the collectively functioning devices with a decision support system. A smart sensing system is required in an agricultural field to assimilate the state of field, its affect on growth of the field and to ascertain the actions required on the field for better outcome of a good produce.

Precision Agriculture (PA), also known as "Site Specific Crop Management ($SSCM$)", is a technique for automated management of agricultural crops, fields and animals using a "smart sensing system" which can accommodate an environment that is adapted to the current needs of the system using the disseminated technology. It involves the following: a) collecting objective spatial and time-sensitive data using remote and proximal sensors, b) application of filtering methods to extract appropriate data, c) incorporation of the Artificial Intelligence (AI)-specific algorithms for decision making, and d) use of actuation systems to execute the required actions. Such managerial strategies can help to mitigate the issues revolving around food production, distribution and sustainability [6], [7].

B. Application Areas of IoT-Based Agriculture

Tzounis *et al.* [8] and Talavera *et al.* [9] describe the following agricultural areas which require the venture of technology.

1) Agriculture Monitoring: To provide an adequate environment for growing crops with the maximum produce, it is crucial to monitor the parameters that affect the growth of plants at every stage of their growth. A number of sensors in both wired and wireless form, such as ground sensors, climate sensors, weather stations and radiation sensors produce data flows, which are stored and used for monitoring, knowledge mining, reasoning, and control. Moreover, any agriculture monitoring involves the following components:

- *Air Monitoring*: It involves the collection of parameters, such as temperature, humidity, and pollutants that could alter or damage the crops.
- *Soil Monitoring*: It monitors the soil moisture, pH, electric conductivity (EC), and nutrients and chemicals like nitrite present in the soil. The pH in soil is a very important parameter that reflects if the soil is healthy enough for good crop. The amount of nutrients appropriate for the crop may either help the crop flourish or damage it.
- *Water Monitoring*: It is crucial to monitor the water quality with the pH, temperature, chemicals and nutrients, measurement of conductivity, turbidity and also the water level and rainfall in order to provide the right kind of growth-supportive environment.
- *Livestock Monitoring*: Sensors that are placed on animals allow to check if any damage is impending on the crop due to animal livestock. In many cases, animal work and products are used to maintain the soil nutrients to promote effective growth of crops. Reynolds *et al.* [10] provided the statistical justification on the need of animals for sustenance of agricultural.
- *Irrigation Control*: An automated irrigation system requires the data on ground water levels and rainfall to minimize water wastage. It also requires to monitor the weather to avoid irrigating the land immediately before or after rainfall.
- *Plant Monitoring*: It encompasses studying the plant life closely for any signs of damage due to diseases or bugs on a periodic basis so that an appropriate action may be taken to circumvent the problem before-hand if possible, or take recovery measures.
- *Fertilizer and Pesticides Control*: Regular use of fertilizers and pesticides is among the top exigencies of agriculture. The specific type of fertilizer, the amount required, and the period of time between each spray are decided based on the values of parameters sensed by the various sensors.
- *Illumination Control*: Proper sunlight is essential for promoting proper photosynthesis in plants. An ambient light can be controlled through the use of light sensors and actuators.

2) Controlled Agriculture/Smart Greenhouses: Greenhouses provide an artificial environment with proper control over all the required necessities specifically needed for the healthy growth of a crop. The process can be eased for the user by integrating IoT with the use of sensors to supervise the greenhouse.

3) Food Supply Chain Tracking: According to the "Food and Agriculture Organization of the United Nations" [2], the food supply chain consists of the following: 1) pre-harvest agricultural production when the produce is on the farm, 2) post-harvest operations when the produce undergoes basics procedures like cleaning and sorting, 3) secure storage of food, 4) safe transportation of food, 5) food processing when it is made consumable, 6) sale of food, and 7) household and business consumption. In all these stages, it is required to monitor and reduce the quality and quantity wastage.

4) Precision Farming/Smart Farming: Based on the analysis of Gebbers and Adamchuk [11] and Hedley [12], precision agriculture can be comprehended as consisting of a collection of technologies including automated machinery, sensor networks, and data analytics to study and change the dynamic variation in the uncertain parameters of agricultural systems.

C. Research Contributions

We summarize the main contributions of this work as follows:

- We discuss the security requirements as well as security threats that are extremely necessary to design the security protocols in an IoT-based agriculture environment. Furthermore, we discuss the threat (attack) model that defines an adversary's capabilities and it is needed to consider in the IoT-based agriculture environment in order to design the security protocols.
- We then discuss various functionality requirements that are essential for designing the security protocols in the IoT-based agriculture environment.
- We also discuss various blockchain technologies with their consensus algorithms needed for mining the created blocks by the miner nodes in a Peer-to-Peer (P2P) network. We also discuss various attacks that can be mounted in consensus processes.
- Next, we discuss a generalized blockchain-based architecture for smart agriculture environment. We then review and analyze the existing competing security schemes developed in varied application areas of IoT-based smart sensing applications.
- We present a detailed comparative study of the existing competing schemes proposed in IoT-based smart sensing applications.
- Finally, we discuss a few emerging directions including some open challenges in the IoT-based agriculture environment.

D. Paper Outline

Fig. 1 presents the organization of the paper. The paper starts with Section I-A that emphasizes the necessity of embedding IoT technology in research and ends with Section I-B by giving the specific areas in agriculture where IoT can be applied. Sections II and III identify the issues of security in agriculture and the associated requirements that the designed security schemes should satisfy. Section IV explains a general working of blockchain technology with Section IV-A and Section IV-B giving the general features and challenges faced in a blockchain based system. It also studies some of the most used consensus algorithms. Section V develops a generalized architecture for creating an authentication scheme based on blockchain for a smart agriculture system and also studies in detail the architecture and cryptographic schemes developed in smart agriculture that use the blockchain concept innovatively. In Section VI, we peform the experiments for computing execution time needed for various cryptographic primitives using the widely-accepted "Multiprecision Integer and Rational Arithmetic Cryptographic Library (MIRACL)" [13]. In Section VII, we present analytical comparisons and cost comparisons of the existing competing schemes. Section VIII identifies some possible directions and open issues that can be pursued for research in future. Finally, Section IX concludes the paper.

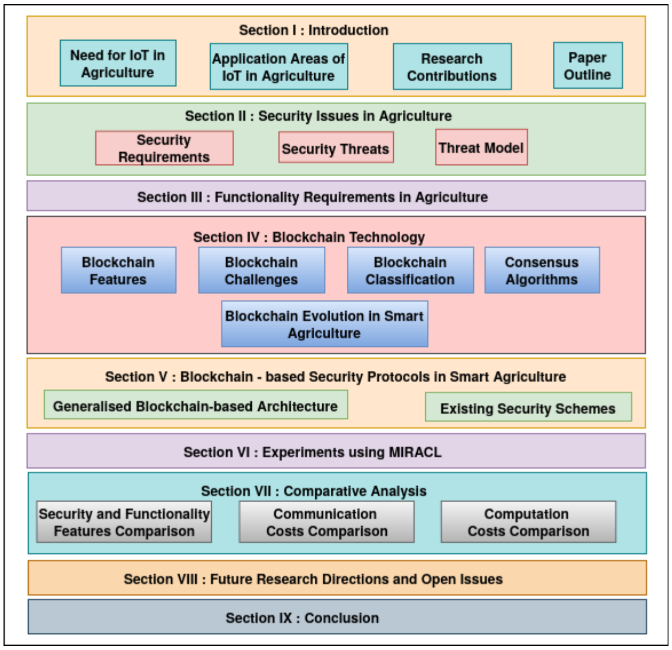

Section I : Introduction
Need for IoT in Agriculture
Application Areas of IoT in Agriculture
Research Contributions
Paper Outline
Section II : Security Issues in Agriculture
Security Requirements
Security Threats
Threat Model
Section III : Functionality Requirements in Agriculture
Section IV : Blockchain Technology
Blockchain Features
Blockchain Challenges
Blockchain Classification
Consensus Algorithms
Blockchain Evolution in Smart Agriculture
Section V : Blockchain - based Security Protocols in Smart Agriculture
Generalised Blockchain-based Architecture
Existing Security Schemes
Section VI : Experiments using MIRACL
Section VII : Comparative Analysis
Security and Functionality Features Comparison
Communication Costs Comparison
Computation Costs Comparison
Section VIII : Future Research Directions and Open Issues
Section IX : Conclusion

Fig. 1. Roadmap of the paper.

II. Security Issues in Agriculture Environment

In this section, we mainly discuss several security requirements as well as security threats (attacks) that are associated with an IoT-based smart agriculture environment.

A. Security Requirements

Any security scheme that caters to provide a solution for smart agriculture should focus on one or more of the following security requirements:

- *Authentication*: This attribute encompasses a technique to ensure that an entity is genuine during its identification, before providing any access to the system.
- *Integrity*: It is to ensure that information that is received by the receiver is the same as that sent by the sender, without even minor change.
- *Confidentiality*: It is to ensure that information that is sensitive to the system is never disclosed to any party, who does not have the authority to its access.
- *Availability*: An entity that has the authorization to access a service, should never be denied the access even under the circumstances of the Denial-of-Service (DoS) attacks.

- *Non-repudiation*: It allows no entity to repudiate the services or actions that were taken up by that entity. This property in turn ensures traceability of a service to an entity.
- *Authorization*: This feature ensures that only an entity that is given the rights to provide any particular network service, does so.
- *Freshness*: This property ensures that a message received is not generated before a threshold time period, which disallows any message to be replayed by an adversary.
- *Forward secrecy*: After a node is detached from the network, either voluntarily or otherwise, it should not be allowed access to any communication that continues within the network.
- *Backward secrecy*: A node that has been recently added to the network should not be privy to a communication that had taken place before its addition to the group.

B. Security Threats

An IoT-enabled smart agriculture can be vulnerable to many possible attacks and some of them are listed below as discussed in [14].

- *Replay attack*: In a replay attack, after a transmission from an entity, an adversary $\mathcal{A}$, may reuse the content from the previous transmission and attempt to deceive an authorized entity.
- *Man-in-the-middle attack*: During transmission between two entities, $\mathcal{A}$ can read the transmitted messages and may then attempt to modify or delete the contents of the messages delivered to the receiver.
- *Stolen-verifier attack*: If an access point (gateway node) stores a list or a table of passwords corresponding to the identities, $\mathcal{A}$ may attempt to steal the list from the access point, thereby gaining access to all passwords.
- *Stolen/Lost smart card attack*: Once $\mathcal{A}$ has obtained lost/stolen smart card, the techniques such as power analysis attacks [15] and timings attacks [16] can be used to extract the credentials stored in the memory of a smart card or a mobile device. The extracted credentials can be then used to further derive the secret data used in the calculation of the credentials.
- *Password guessing attack*: This attack involves attempts to speculate the correct password using the intercepted messages and illegal access to credentials stored in the smart card or the mobile device.
- *Password change attack*: In this attack, after obtaining access to a stolen smart card or a mobile device, attempts can be made by $\mathcal{A}$ to change the passwords of the existing registered users in order to be able to gain unauthorized access.
- *Denial-of-Service (DoS) attack*: This is a specific type of attack in which services are denied to an authorized user on account of overuse of the system's resources by other factors such as a failure in hardware or software bugs or over-allocation of bandwidth to certain users [17].
- *Privileged-insider attack*: In this kind of attack, an existing user within the system attempts to misuse his/her privileges in order to acquire unauthorized rights to access/modify/delete vital information. To avoid this, the system should have to check if the access provided is legal for the given type of user.
- *Impersonation attack*: If an adversary $\mathcal{A}$ claims to be the sender by sending fake generated messages, he/she is said to impersonate the receiver. In such an attack, it is not possible for the receiver to distinguish that the received message is from the adversary and not from the sender.
- *Resilience against sensing (smart) device capture attack*: An adversary $\mathcal{A}$ may physically seize the sensing device and extract sensitive information from the captured device to establish communication with other non-compromised sensing devices. To comprehend the amount of damage caused by device capture attack, estimations can be made by calculating the probability of compromised communication a) between two non-compromised devices and, b) between a non-compromised device and a user, given that n_c devices are already compromised in a network. The former is considered in the schemes for access control, device authentication and key management. The later one is considered in a user authentication or a user access control scheme. For any scheme to be resilient to this attack, the effort is to minimize these probabilities. In an ideal case, the probability should be close to zero.
- *Resilience against new sensing devices deployment attacks*: An IoT environment is also susceptible to a number of attacks, such as illegal deployment of new sensing devices, replication of existing sensing devices, Sybil, and wormhole attacks.
  - In a wormhole attack [18], an adversary tricks two distant nodes into communicating via a wormhole tunnel, using an in-band or out-of-band channel, that can circumvent through the network traffic. Thus, deluding the nodes into the impression that they are near to each other. Such a tunnel gives the adversary control over the network traffic. A wormhole attack can lead other possible attacks on packets such as modification, sniffing and dropping.
  - In a *Sybil attack*, the adversary generates multiple pseudonym identities which are misunderstood for multiple entities [19], [20]. This can lead to multiple requests being accepted from the same entity under different identities. The "51% attack on a blockchain" is an example of a Sybil attack [21]. The identities used by the adversary may already exist in the network, or may be newly generated.
  - In a *sensing device replication attack* [22], instead of creating fake identities, a compromised node itself is replicated by an adversary deliberately. This allows the adversary to first capture a device, extract sensitive information from it, and replicate the information in other nodes, and deploy the replicated nodes in the network to involve them in communication with other non-compromised devices.

C. Threat Model

In this paper, we follow the widely-accepted "Dolev-Yao (DY) threat model" [23] along with the current *de facto*

"Canetti and Krawczyk's model (CK-adversary model)" [24]. According to the DY model, an adversary $\mathcal{A}$ can not only eavesdrop on the communicated messages among the entities, but also can inject the malicious information, modify or delete the message contents in between the communication. On the other side, being the CK-adversary $\mathcal{A}$, has all the abilities as in the DY model, and also can compromise secret credentials, secret keys and even session states if those information are available in insecure memory of the participants through the session hijacking attack. The end-point communicating entities (e.g., IoT smart devices) are not treated as trustworthy entities in the network. Since an agriculture field can not be monitored 24 × 7, there is a possibility of direct physical capture of the smart devices from the field itself. Therefore, by compromising physically some smart devices, $\mathcal{A}$ can extract all the credentials available in those devices' memory by applying the sophisticated "power analysis attacks" as explained in [25]. The extracted credentials can be further utilized for mounting other attacks, such as impersonation attacks.

III. Functionality Requirements in Agriculture Environment

In this section, we list down some basic functionality requirements in an IoT-based agriculture environment.

1) Dynamic New Smart Device Addition: In an IoT-based agriculture environment, it is extremely essential that a security scheme should support dynamic node addition facility after initial deployment of the nodes including the smart devices in the network. As an IoT smart device in the agriculture environment may be physically captured by an adversary or its battery power may be exhausted, a new device needs to be deployed into the existing network.

2) High Scalability: Support of high scalability is a basic functionality requirement in a modern day IoT-enabled agriculture environment. High scalability should assure that even if the number of IoT smart devices are going to increase, the overall network performance should not be affected by this factor.

3) Mutual Authentication: Among all the security services, mutual authentication and key management are considered as two important techniques to assure secure communication in an IoT-enabled agriculture environment. Resource limitations of the IoT smart devices and their vulnerability to physical capture make the design of a mutual authentication between two IoT smart devices and also between a remote end-user and an IoT smart device inside the IoT-based agriculture environment become a challenging task.

4) Availability: The device communication and control in an IoT-based agriculture environment is performed in real time to keep a real-world impact. For instance, a user (e.g., a farmer) might require to remotely control an agriculture field by monitoring crops condition and require to access data any time.

5) Efficiency: In an IoT-based agriculture environment, various smart devices are resource limited, including the limited battery lifetime. In addition, the IoT smart devices might have also other constraints, such as storage. Furthermore, the IoT devices might need frequent communication among them for secure communication. As a result, it is desirable that a designed security protocol should encompass minimum possible computation and communication overhead, as well as storage overhead to store the secret credentials including the session keys for secure communication with other nodes.

IV. Blockchain Technology and Its Evolution in Smart Agriculture

In a network of systems that share vital information and use it for further processing, usually a central authority is assigned the task of maintaining the correctness and validity of the information. When such a centralized system is prone to failure, it can lead to a massive loss of vital data needed in critical applications. To overcome such disastrous problems, it is convenient to move the authoritative tasks to a decentralized system.

Blockchain technology is a decentralized system which allows multiple systems to maintain a local copy of a public ledger, called a blockchain, by executing a commitment protocol to add a new block into the blockchain with a process, called as *mining*, and a *consensus protocol* to ensure consistency among various local copies [26]. Such a system avoids single point failure by allowing multiple authority points with multiple nodes such that if one node fails, all the nodes connected to it will be redirected to another node as long as there is no disconnection of the network. This can be further improvised as a distributed system with no central nodes, where all the nodes cooperatively maintain the vital data [27]. A blockchain is a data structure with a number of data blocks linked linearly in a chronological order to form a chain and protected using cryptographic techniques. A block consists of a header with the hash of the previous block, the root of the the merkle hash tree, and time in seconds when the block was added [28]. It is worth noticing that the contents of a block may vary from one application to another application [29], [30].

A. Blockchain Features

In the following, we list the core features of blockchain as follows [31]:

- *Decentralization*: In a decentralized system, there are several trusted agencies which cooperate collectively to maintain the data in a blockchain [32].
- *Persistence*: The data in a blockchain is tamper-resistant as any given data is validated by multiple nodes and replicated in the local copies of all the nodes. Any change in one of the copies can be clearly identified when the copies of the ledger differ in their content. Blockchains are also made tamper-proof by disallowing deletion of blocks.
- *Anonymity*: The blockchain technology allows each node to have multiple pseudonyms/addresses to ensure privacy preservation on the transactions [33].
- *Auditability*: To verify any transaction, a user may access any node in the network and trace the transactions. This feature is possible due to the validation of the transactions before recording them during the mining process. Allowing such a verification by a user ensures traceability, and

hence, non-repudiation of the transactions by the nodes is also achieved [34].

B. Blockchain Challenges

Zheng *et al.* [31] studies the working of the blockchain system with emphasis on the types of blockchains, their applications in various domains and directions for research in blockchains. The challenges faced in any blockchain system are as follows [31]:

- *Scalability*: As blocks can only be added to a blockchain and never deleted, the amount of storage space is a primary issue. Several solutions have been studied including limiting the number of transactions processed per unit time, the trade-off between large and small block sizes, lightweight clients, and partitioned blocks [35]–[38].
- *Privacy Leakage*: The content of transactions are publicly available, and hence, the blockchain cannot ensure transactional privacy [39], [40]. Also, various techniques are developed to link the users with their pseudonyms as discussed in [41]–[44].
- *Selfish Mining*: Blockchains are susceptible to collusion from nodes if 51% of the nodes are dishonest. This is also known as 51% attack. Such nodes could add blocks to the chain that reverse an existing transaction that had been previously validated [45], [46].

C. Blockchain Classification

A blockchain system is a distributed P2P network with three possible roles for a node: a) lightweight nodes, b) full nodes, and c) consensus nodes. A lightweight node stores only the block header. A full node stores a complete replica of the blockchain and is allowed to verify the blocks. On the other side, a consensus node can participate in mining and consensus process [47]. The type of blockchain appropriate for an application is classified by how the participation of the nodes is allowed in the mining process, consensus process, accessing the network and the level of decentralization [31]. There are three types of blockchains, which are listed below:

- *Public/Permissionless/Open-Access Blockchain*: A public blockchain allows any node to participate in the reading and adding of transactions, with fees. There is no permission required for a node to participate in the consensus validation of blocks. As any node is allowed, it is not possible for every node to know the identity of every other node in the network. A random topology of the network may be used that results in the process of propagating validated transactions being usually carried out with the help of hierarchical flooding. The nodes perform peer discovery through a query-response cycle on a fixed set of Domain Name System (DNS) servers and publishing their peer lists. To restrict malicious nodes from publishing false peer lists, a reputation system based on penalty score is maintained [47]. A public blockchain is completely decentralized in nature. The blockchain is completely immutable as new blocks of transactions may be stored in varied nodes of the distributed system. It is transparent as the amount of influence that a node can have is directly proportional to the amount of resources they can employ [48]. In such case, the transaction throughput is very low.
- *Private/Permissioned/Closed-Access Blockchain*: A private blockchain is a blockchain system consisting of pre-determined nodes allowed to access the network to read and add transactions [49]. Only the nodes which are granted permission are allowed to participate in the consensus process. Peer discovery is either lightweight or non-existent as every node in the network is aware of the identity of the other participating node. Propagation of transaction data is very efficient due to limited participants. The blockchain may be tampered with if majority of the nodes agree [50]. The final consensus can be fully controlled by one organization and the validated blockchain may also be reversed by appending new blocks. It is owned by a single organization and has high transaction throughput.
- *Hybrid/Consortium/Shared-Permissioned Blockchain*: A consortium blockchain employs a partially decentralized system which is a hybrid of public and private blockchains in order to support scalability over closed blockchains [51]. Only a permitted set of participant nodes may be allowed to perform core activities such as mining, consensus and propagation, without any fees. The visibility of the blockchain may be either restricted to the approved consensus nodes or to those nodes that have been authorized for certain access rights, if permissioned, or may be public. The blockchain may be owned by multiple organizations and has high transaction throughput. The blockchain may be tampered with if majority of the nodes agree.

A transaction in a blockchain is a digital exchange of assets. This exchange can be executed according to the transactional models [52], [53]:

- *Unspent Transaction Outputs (UTXO) model*: In this model, every user maintains instances of digital assets received, but not yet sent as rows of asset type and its quantities. A transaction is the sum of separate quantities of different assets being spent. Transactions are recorded by deleting a set of rows (UTXOs) from the sender and adding a set of rows (UTXOs) from the receiver in the database. This model provides privacy, scalability and security, but it complicates parallel execution of transactions as ordering is required to ensure correctness of database [54].
- *Account-based online transactional model*: It consists of executable bytecode programs, called *smart contracts* that are replicated locally in every node inside the blockchain which activates appropriate logical computations on all honest nodes simultaneously to maintain consistency. A smart contract is triggered by addressing a transaction to it. This model developed by Szabo [55] is simple and space-efficient.

D. Consensus Algorithms

A comprehensive and detailed study of the existing consensus algorithms has been done by Wang *et al.* [47], Aggarwal *et al.* [56], Nyugen and Kim [57] and Zhang *et al.* [52]. Some of the most used consensus algorithms are summarized below.

- *Ripple*: Ripple is a client-server based consensus algorithm developed by Schwartz *et al.* [58] that executes in rounds. Every server has a list of servers called the "Unique Node List (UNL)" from which it can accept transaction proposals. Before each round, the server collects its received transactions into a candidate set and publishes it. It receives the candidate sets from the servers in its UNL and validates them by voting "Yes" or "No". If a transaction receives less than a threshold amount of votes, it is discarded before next round. In the final round, only the transactions which received more than 80% "Yes" votes are included in the ledger before closing it.
- *Practical Byzantine Fault Tolerance (PBFT)*: An unreliable distributed system consists of both faulty and non-faulty systems. The non-faulty systems must agree on a task by sending messages regardless of the unpredictable behaviour of the faulty systems of sending conflicting messages. Lamport *et al.* [59] identified this problem as the "Byzantine Generals Problem" concluding that unanimity can be reached in such an untrusted distributed environment if the number of non-faulty systems is more than three times the number of faulty systems, and not more than half of the network connectivity is faulty. A number of algorithmic solutions are provided in such cases. Castro and Liskov [60] proposed a protocol where one of the nodes is elected as the primary node and the rest are secondary nodes. A consensus is achieved when $f + 1$ nodes agree that the block is valid, with f faulty nodes in an asynchronous environment.
- *Proof of Work (PoW)*: This consensus scheme requires the *miners* to solve a puzzle and the block created by the first node that solves this puzzle will be added to the blockchain. The miners compute a hash value for the dynamically altering value of the block header such that it cannot exceed a certain threshold [61]. To arrive at this value, the nodes have to try multiple values for nonce in brute force. The first node to arrive at such a value is the *winner* and its block is accepted to be replicated in the local copies of blockchains of all other nodes. As more nodes join the role of miners, the processing time, cost and energy expended increase; thereby reducing the efficiency of this algorithm [29].
- *Proof of Stake (PoS)*: This algorithm introduces penalties in addition to rewards during consensus. A miner deposits a part of his currency as stake to participate in consensus. If the miner is successful in validating a block, the stake is increased; otherwise, the stake is lost. Only the miners who are rich in currency and are willing to place bets on the block can participate. The identities of the miners who have deposited stakes are known and a miner who stakes the highest is chosen once its ownership is proved using digital signatures. A rich miner is less likely to commit fraud as they may lose their stake. PoS is advantageous in consuming less energy, less cost and processing fast as compared to those for PoW [62].
- *Proof of Activity (PoA)*: Bentov *et al.* [63] proposed the PoA consensus algorithm where the miners begin with the PoW consensus expending their computational resources until a new block to be added is found. Next, it shifts to execute PoS algorithm to add the miner's rewards to the winner block containing the block header.
- *Delegated Proof of Stake (DPoS)*: In DPoS, the nodes in the network execute a voting process to elect a few third party witnesses which perform the consensus on behalf of the network. If any of the witnesses misbehaves, they are immediately replaced. The voting influence of a node is directly proportional to the amount of currency it holds. DPoS is a robust protocol that works even if majority of the witness nodes fail [64].
- *Proof of Burn (PoB)*: Stewart [65] developed the PoB consensus where the miners burn their currency at stake by sending the coins to eater addresses and make them unusable to show their commitment to mining. A node which burns more coins has more power. It can be verified easily, but the burnt coins cannot be revoked.
- *Proof of Elapsed Time (PoET)*: In this consensus protocol, the miners are made to wait for a random amount of time. The miner whose wait time is completed first becomes the one whose block will be added to the chain. PoET was developed by Intel on a special instruction set, called "Software Guard Extensions (SGX)" that ensures trusted code to run correctly in controlled environment [66]. The amount of time to wait is generated using SGX.
- *Proof of Luck (PoL)*: Milutinovic *et al.* [67] proposed a simplistic consensus algorithm, called as Proof of Luck (PoL), where the miners generate random numbers, and the block created by the miner with the highest generated random number is added to the blockchain. It is worth noticing that PoL requires all the nodes to be time synchronized to generate random numbers simultaneously.
- *Proof of Space (PoSp)*: Dziembowski *et al.* [68] proposed a consensus algorithm in which the miners would expend some unit of disk space instead of computational effort. The miners in PoSp generate numerous plots on the hard disk. The miner with the largest number of plots wins.

In addition, Wang *et al.* [47], and Tschorsch and Scheuermann *et al.* [69] describe an abstraction process for development of Proof of Concepts (PoX) consensus algorithm and study the PoX-related schemes in detail. Table I gives a summary of the discussed consensus mechanisms. Finally, we provide a summary of possible attacks on the consensus algorithms in blockchains based on Zhang and Lee's analysis [70], which is shown in Table II.

E. Blockchain Evolution in Smart Agriculture

Usage of blockchain in the smart agriculture can have a considerable positive effect on the economy. A study on the impact of the usage of blockchains in the grains sector in Australia [78] shows an increase in the Gross Domestic Product (GDP) by approximately 2.5%. Christidis and Devetsikiotis [53] have shown how the decentralized nature of blockchains can lead to the heterogeneity of Internet of Things,

TABLE I
BLOCKCHAIN CONSENSUS MECHANISMS AND THEIR APPLICATIONS

Consensus mechanism	Concept	Resource	Applications
Ripple	Voting in multiple rounds	No resource	XRP ledger [71]
PBFT	Voting	No resource	Tendermint [72]
PoW	Hashing	Computations	Bitcoin [29] Ethereum [73]
PoS	Digital signatures	Currency	PeerCoin [62] SnowWhite [74] Ouroboros [75]
DPoS	Voting	Currency	BitShared Ark EOS
PoB	Address suspension	Currency	SlimCoin [76]
PoL	Random number generation	Intel SGX	Luckychain
PoA	Hashing digital signatures	Computations currency	Decred
PoET	Random number generation	Intel SGX	Sawtooth Lake
PoSp	Maximum plots on disk	Storage space	Storj [77]

TABLE II
ATTACKS ON CONSENSUS MECHANISMS

Attack	Affected consensus protocols	Description
Double spending	Most protocols	Repeated usage of token
Selfish mining	PoW	Gain profits by generating blocks privately in a mining pool
Nothing at stake	PoS	Blocks added to all branches in a fork
Bribe attack	PoS	Honest nodes are given incentive to add blocks on private fork
Stake bleeding attack	PoS	Broadcast transactions copied from main chain onto private fork to earn extra fees and increase stake
Fake stake attack	PoS	Increase the smaller valued stakes to higher valued stakes

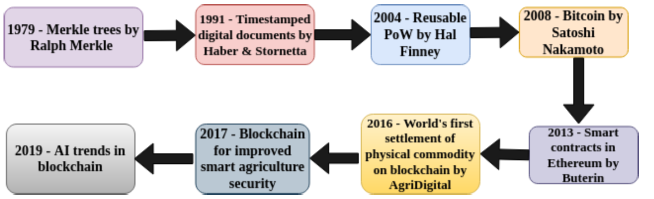

1979 - Merkle trees by Ralph Merkle
1991 - Timestamped digital documents by Haber & Stornetta
2004 - Reusable PoW by Hal Finney
2008 - Bitcoin by Satoshi Nakamoto
2013 - Smart contracts in Ethereum by Buterin
2016 - World's first settlement of physical commodity on blockchain by AgriDigital
2017 - Blockchain for improved smart agriculture security
2019 - AI trends in blockchain

Fig. 2. Evolution timeline of blockchain in smart agriculture.

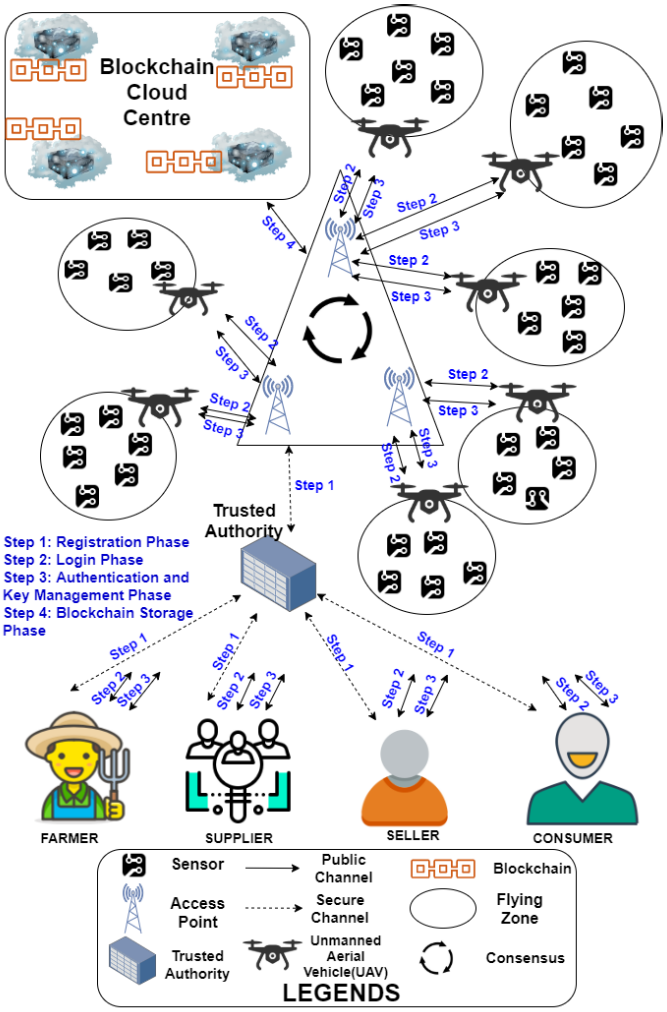


Fig. 3. Cloud-assisted blockchain-based general architecture for IoT-enabled smart sensing agriculture.

making it widely applicable to numerous domains. A study by the "Food and Agriculture Organization of the United Nations" in conjunction with the "International Telecommunication Union (Bangkok)" in 2019 [79] shows the growing influence of blockchains in various areas of agricultural sectors along with the risks and possibilities it poses. Fig. 2 shows the evolution of blockchain into smart agriculture.

V. BLOCKCHAIN-BASED SECURITY PROTOCOLS IN SMART AGRICULTURE

This section explores existing competing security schemes developed in varied application areas of IoT-based smart sensing applications.

A. Generalized Blockchain-Based Architecture

A generalized blockchain-based architecture for smart agriculture has been proposed in Fig. 3.

An agricultural field may be divided into disjoint zones, called flying zones. Few unmanned aerial vehicles (UAVs), also referred to as drones, may be assigned to a flying zone [80]. The drones collect data from the smart sensor devices placed in its assigned flying zone and forward to its associated access point. The access points forward the collected data from its associated drones to the user requesting the data. To ensure security in the system, all entities go through a registration phase with a Trusted Authority (TA), before authenticating them for login access to the data. The TA will also assign the sensors (smart devices), drones and access points in the system. During registration, each of the smart devices, drones and access points are assigned credentials including secret keys. After the deployment of the registered entities, a drone needs to authenticate with its access point and also with its other neighbor drones in the flying zone. Similarly, smart devices deployed in the agriculture field need to make secure communication with their neighbor smart devices. To serve these activities, a mutual authentication and key agreement scheme is extremely essential [81]. There are four types of users: a) farmer, b) supplier, c) seller and d) consumer. Sometimes, an external user (for example, a farmer) can be given access to the real-time data from the deployed smart devices directly. However, to give such an access, a user authentication is needed where a user will establish session keys with its accessed smart devices provided that they mutually authenticate each other.

The information collected by the access points from the drones and also by an external user from the accessed smart devices form various transactions. These transactions are then used to form the blocks. Since the information is private and confidential, we consider the private blockchain in the smart agriculture scenario. Note that the transactions are encrypted by the public key of the owner (in this case, an access point) which are then stored in the blocks. The blocks are then mined using some efficient consensus algorithm. For example, we may utilize the Ripple or PBFT consensus algorithm. After successful validation of the blocks by the nodes in the P2P network consisting of the trusted access points, the blocks are then added in the blockchain maintained by the blockchain cloud center.

B. Overview of Existing Security Schemes

In this section, we review some of the competing existing security protocols including blockchain based solutions and authentication protocols proposed in the literature related to IoT-enabled agriculture and other related environments. In recent years, the authentication becomes one of the potential security services in various networking environments to secure the networks [82]–[94].

Almadhoun *et al.* [95] proposed a system with IoT devices which are assigned to a fog node. The fog nodes have the capability to perform computations required during authentication process on behalf of IoT devices, thus reducing their burden of processing. A smart contract contains the association of the fog nodes to its linked IoT devices [96]. The administration is responsible for managing the permissions of which user is allowed to access which device and perform what operations. The cloud consists of huge storage and computation servers that store the enormous data collected by the IoT devices. The end users require permission to access their IoT devices. All the entities except the IoT devices have unique Ethereum address and interact with the smart contract directly or through an application. Their scheme supports confidentiality, integrity and non-repudiation, and it is also resilient against Denial of Service (DoS) attacks [97].

Cui *et al.* [98] proposed a hierarchical architecture in a multi wireless sensor network (WSN) environment with a hybrid blockchain model. It consists of a public blockchain with the base stations and end users as the miners to authenticate and register the cluster heads with the help of smart contracts. A local blockchain with the cluster heads as the miners is used to register and authenticate the ordinary nodes using smart contracts. The Ethernet address associated with each node is hashed to obtain its identity, which is further marked as OrdinaryID (OID), ClusterID (CID) and StationID (SID) to designate their roles vividly. During initialization, the base station generates the public-private key pairs and the IDCard for each node. The cluster head sends registration request to the public blockchain, which stores its details and allows access to the local blockchain. When the ordinary node sends a request of registration to the cluster head, it verifies the timestamp and triggers the smart contract on the local blockchain to verify its details [99]. Once verified, the node details are stored on the local blockchain and allows access to the cluster network. When the node sends a request to communicate with another ordinary node through the cluster head, it finds the base station of the related WSN that triggers the smart contract on the public blockchain to check if both the requesting and requested nodes exist, have valid IDs and are alive. If both the nodes are in the same cluster, a secure channel is established. Otherwise, the corresponding cluster head nodes exchange the authentication credentials with the transaction voucher obtained from the local blockchain. If the nodes belong to different WSNs, the corresponding cluster head nodes exchange the authentication credentials with the transaction voucher obtained from the public blockchain. Then a secure communication channel is established between the two nodes for further communication. When an end user wants to communicate with a node, the user sends a request to the base station which triggers a smart contract to authenticate the user's identity. If it is successful, the credentials are sent to the user and the node to establish a secure connection. Their scheme is resistant against Sybil attack, DoS attack, Man-in-the-Middle (MiTM) attack as well as replay attack. Furthermore, it supports scalability, decentralization, and cross-domain authentication.

The Public Key Infrastructure (PKI) is used to obtain the public key of an entity. The PKI is usually realized as an organized tree with a root. This leads to a centralized structure where the data of all the other entities is vulnerably dependent on the root. To overcome this issue, a decentralized blockchain based PKI has been proposed that considers thin clients to perform the same functions as a full node user. In a blockchain based-PKI, an entity creates two key pairs: a) online private-public key pair and b) offline private-public key pair, and adds the details onto the blockchain along with the signatures, after being verified by the miners. To obtain a key corresponding to an identity, the most recent block associated with that identity is retrieved which has either the key or an update that the key that has been revoked [100].

Jiang *et al.* [101], [102] in their works have come up with the following innovative schemes for authentication. In their first scheme, called "Privacy-preserving Thin-client Scheme (PTS)" [101], Alice, being the initiator, first sends her identity and public key to Bob, the responder. Bob authenticates Alice by sending her identity along with $k - 1$ random identities to the full node users. Each of the full node users traverse their blockchain to retrieve the public keys corresponding to the identities received and sends them to Bob. If the public key of Alice's identity received from all the full node users is the same, Alice's public key is verified as true. Then, Bob sends his identity and a nonce encrypted with Alice's public key to Alice. Alice decrypts Bob's identity and nonce with her secret key, retrieves Bob's public key from her blockchain, and verifies Bob's pubic key with the full node users. Then Alice sends her nonce, Bob's nonce and her identity encrypted with Bob's public key. Bob after decrypting the message with his secret key, verifies the correctness of Bob's nonce, encrypts Alice's nonce with Alice's public key and sends it back to Alice. Once Alice verifies the received nonce as true, Alice and Bob are mutually authenticated. To reduce cost, they proposed another scheme, called "Efficient Privacy-preserving Thin-client Scheme (EPTS)". It was shown that EPTS can significantly reduce computational cost of the full node users and communication cost when k is particularly large.

Jiang *et al.* [102] also proposed a "Privacy-preserving Thin-client Authentication Scheme (PTAS)" which employs the idea of private information retrieval (PIR). To enhance the security of PTAS, they also proposed an $(m-1)$-private-PTAS which removes the restriction that the number of full node users, say m, should be a power of 2 and that the full node users do not collude. In fact, this enhanced scheme ensures that even if $m-1$ nodes collude together, the thin-client's privacy is still preserved. The number of full node searches in PTS is $m.k$, whereas in PTAS it is independent of the number of full node users m and in $(m-1)$-private PTAS the total searches is $m.k/2$.

Yao *et al.* [103] proposed a scheme for authentication in a Vehicular Ad Hoc Networks (VANETs) with Fog computing [104]. It allows computation to be conducted in units closer to the vehicular units based on blockchains. Their system framework consists of an Audit Department (AD), On-Board Unit (OBU), Road Side Unit (RSU), Service Manager (SM), Witness Peer (WP) and a consortium blockchain. The vehicle OBU sends its public key and identity to the AD, which returns part of the public and private key and is used by OBU to construct the complete public and private key, thus successfully performs the registration of the OBU. The same process is used to register SM with AD. When an OBU requests access to RSU, it creates a ciphertext from the IDs of all the SMs and the Lagrange difference polynomial, and sends to RSU. This ciphertext is further forwarded from RSU to the SM which extracts the OBUs identity and signature and verifies it [105]. Once verified successfully, it searches and updates its local database and forwards the authentication details to the Witness Peer (WP). The WPs store the details into their memory and create a block after a time period after executing the PBFT consensus algorithm. The scheme ensures confidentiality through encryption at every phase, integrity by denying access on detection of tampering, anonymity by random choice of pseudonyms, traceability and anonymity by revoking the public key of the identity of the misbehaving entity, and also non-interactivity.

Kaur *et al.* [106] also proposed a different scheme for authentication in a vehicular fog network. In their approach, an OBU of a vehicle sends an encrypted concatenation of OBU's identity and timestamp to the AD [107]. The AD verifies the timestamp and checks the availability of the identity on the blockchain. It stores an authenticator, say $auth$ as the bitwise XOR of two parts: the first is the hash of the concatenation of secret key and identity of OBU and the second part is the hash of the concatenation of the secret key of AD and identity of OBU. It then computes and sends the secret and public keys for OBU, along with the second part of authenticator $auth$, which is saved by OBU. When the OBU requests access to the SM, it constructs and sends to SM: the first, authenticator $auth$ and the second, authenticator value $Auth_{OBU}$ generated using $auth$, timestamp, OBU identity, and the public variant of the OBU secret key. Once $Auth_{OBU}$ is verified to be valid, SM also constructs another authenticator $Auth_{SM_j}$ that is verified by OBU. A common session key is then computed using the key derivation function on the authenticator $auth$, timestamps of OBU and SM, and OBU identity. These authentication results are added to the blockchain similar to the consensus process as suggested in [103], [108].

Islam and Shin [109] proposed a healthcare system which uses an UAV to read data from a Body Sensors Hive (BSH) that collects health data (HD) from sensors placed on users [110], [111]. The UAV verifies the authenticity of the received data and then forwards it the server. The server is responsible for adding data as a block into the blockchain after consensus with the Ground Control Station (GCS) and private cloud. For this to work, the details of the user are initially registered on the blockchain using a smart contract. A smart contract is also used to assign a UAV with a set of users using the UAV's public key. Each entity in the system has a private key based on its "media access control address (MAC address)", timestamp and a random seed, and a corresponding public key is also generated. A trust token is generated for BSH and UAV during registration that is used during communication with the server. To synchronize the UAV with its BSHs, UAV encrypts and sends a shared key with the public keys of all the BSHs. The BSH decrypts the shared key and double encrypts its public key with first, the trust token and then, with the shared key. Their system is resistant against MiTM attack, replay attack, and also illegal data tampering and unauthorized data access attacks.

Chen *et al.* [112] discussed an innovative platform, known as AgriTalk, that uses precision farming for the soil cultivation of turmeric. Their system automates the fertilization, pest control and irrigation processes using an IoT environment with sensors, actuators and controllers. The factors to be monitored for turmeric cultivation are pH, nutrients, electric conductivity (EC), moisture levels, amount of nitrite, Nitrogen (N), Pottasium (K), Phosphorus (P) and light. The amount of NPK required for the available amount of EC is determined by quadratic equations, which are then fed into a first layer of a neural network model. This model uses three neurons as the hidden layer and outputs the productivity from the output layer. This is repeated until the bias converges and the output rhizosphere weight is related to the content of the curcumin in the soil using a linear equation. The actual harvested productivity is then compared to the predicted productivity to obtain the growth rate. Similarly, for pest and fertilizer control, a model was established to relate the environmental factors such as the humidity, temperature, and egg hatching period. The AgriTalk system consists of SnsrCtrl board with soil and insect sensors, a weather station connected to it by wires, AgriCtrl microcontroller board that controls all the connected IoT devices, and an AgriTalk server in the cloud [113]. To detect any abnormality in sensor functioning, the values of nearby sensors are compared and the power consumption is monitored. To correct a hardware failure, the device is replaced. To correct a software failure, device application is modified by calibration without the need to modify the firmware or sensors operational range. AgriTalk has a good performance for message delay using 4G [114]. They also noticed that the precision of the regression model can be further increased by including more factors like the wind speed and direction to predict the rate of eruption of diseases.

Wu and Tsai [115] proposed a system that provides information privacy, integrity, preservation and accuracy, with a rapid authentication scheme. It amalgamates the concepts of blockchain, dark web, bilinear pairings, "keyed-hash message authentication code or hash-based message authentication code (HMAC)", symmetric encryption, 4G mobile communication, and Global Positioning System (GPS) location sensing to deflect "Distributed Denial-of-Service (DDoS) attack". The dark web was applied to create a private blockchain and used it for identity authentication before a user is allowed to search. The packets received from the equipment are distributed over the blockchain. A user sends encrypted search data to the trusted authority (TA), which is then forwarded to the dark net servers whose locations are unknown to the user to ensure protection against cyber attacks on them. The blockchain stores messages received from the TA in a block. To ensure integrity of any message, it will calculate its HMAC and compare it with the HMAC of the stored message. The origin of the message is also verified using the bilinear pairing operations.

Zhou *et al.* [116] proposed an authentication scheme which used the Identity Based Encryption (IBE) as the PKI for distribution of keys with the integration of blockchain. In their scheme, a user sends an identity, a random seed and a signature to the Key Generation Center (KGC) to request for a private key. The KGC divides the nodes under its control into three groups: a) supervision nodes, b) production nodes, and c) protection nodes. The supervision nodes verify the user identity and sign with its master key. After consensus from the other nodes, a validated block is added to the blockchain and a partial private key is sent to the user. The protection nodes participate in the block verification consensus and key distribution consensus with the help of Proof of Vote (PoV) consensus algorithm that uses the supervision nodes' signature to generate partial private key and sends it to a production node. The production nodes also participate in block verification consensus and transmit the partial private key to the user. After a fixed number of blocks are added, a supervision node changes its role into protection node and a new supervision node is re-elected. The private and public keys pair is used by the users to mutually authenticate each other. The key escrow problem, where the KGC can produce the user's private key to decrypt messages meant for the user, is circumvented using blinding of the partial information in the channel in this scheme.

TABLE III
EXECUTION TIME (IN MILLISECONDS) OF CRYPTOGRAPHIC PRIMITIVES USING MIRACL

Primitive	Max. time (ms)	Min. time (ms)	Average time (ms)
T_{bp}	8.44	4.424	4.603
T_h	0.149	0.024	0.055
T_{exp}	0.248	0.046	0.072
T_{eca}	0.002	0.001	0.002
T_{ecm}	1.979	0.327	0.480
$T_{ecsiggen}$	2.128	0.351	0.535
$T_{ecsigver}$	4.110	0.679	1.017
T_{senc}	0.008	0.002	0.003
T_{sdec}	0.005	0.002	0.003
T_{mul}	0.007	0.001	0.002
T_{add}	0.003	0.001	0.001

VI. EXPERIMENTS USING MIRACL

In this section, we perform the experiments of various cryptographic primitives using the widely-accepted "Multiprecision Integer and Rational Arithmetic Cryptographic Library (MIRACL)" [13] for measuring the average time needed for the primitives. We then use these experimental results for comparative study on computational costs among various existing schemes in Section VII. It is worth noticing that MIRACL is a cryptographic library based on "C/C++ programming language" that contains the "open source SDK for Elliptic Curve Cryptography".

Let $GF(q)$ be a Galois (finite) field where q is a sufficiently large prime. We then consider a non-singular elliptic curve $E_q(u, v)$ of the type: "$y^2 = x^3+ux+v \pmod q$" where $u, v \in Z_q$ are two constants such that the condition $4\,u^3+27\,v^2 \neq 0 \pmod q$ is satisfied and $Z_q = \{0,\ 1,\ 2,\ \ldots, q-1\}$.

Various operations are symbolized by the notations T_{bp}, T_{exp}, T_{ecm}, T_{eca}, T_{senc}/T_{sdec}, T_h, T_{mul}, T_{add}, $T_{ecsiggen}$ and $T_{ecsigver}$ to signify the time required for a "bilinear pairing", a "modular exponentiation", an "elliptic curve point (scalar) multiplication", an "elliptic curve point addition", a "symmetric key encryption/decryption using the Advanced Encryption Standard (AES-128) [117]", a "one-way hash function using SHA-256 hashing algorithm [118]", a "modular multiplication over $GF(q)$", a "modular addition over $GF(q)$", an "elliptic curve digital signature generation using ECDSA algorithm [119]" and an "elliptic curve digital signature verification using ECDSA algorithm", respectively. Here, the elliptic curve point addition and multiplication are carried out on a non-singular elliptic curve $E_q(u, v)$.

The platform that we considered for MIRACL is as follows: Ubuntu 18.04.4 LTS, with memory: 7.7 GiB, processor: Intel® Core™ i7-8565U CPU @ 1.80GHz × 8, OS type: 64-bit and disk: 966.1 GB. The experiments were executed for each cryptographic primitive for 100 runs. The maximum, minimum and average run-time in milliseconds are then recorded for each cryptographic primitive from these 100 runs. The obtained experimental results are finally listed in Table III.

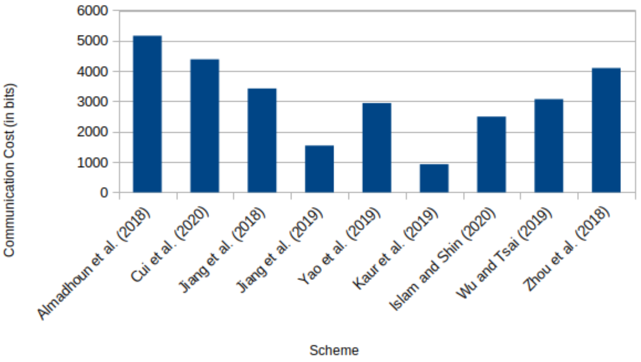


Fig. 4. Communication costs comparison.

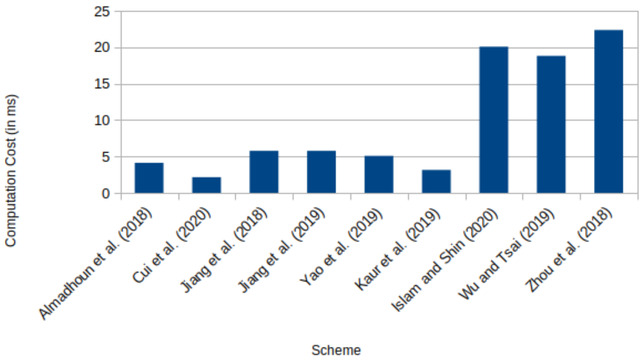


Fig. 5. Computation costs comparison.

TABLE IV
SECURITY AND FUNCTIONALITY ATTRIBUTES COMPARISON

Scheme	Security & functionality attributes	Application areas
Almadhoun *et al.* [95]	Confidentiality, Integrity, Non-repudiation	General
Cui *et al.* [98]	Scalability Mutual Authentication, Cross Domain Authentication, Decentralization	Multi-WSN
Jiang *et al.* [101]	Anonymity, Privacy Preserving, Thin Client	PKI-based authentication
Jiang *et al.* [102]	Anonymity, Privacy Preserving, Thin Client	PKI-based authentication
Yao *et al.* [103]	Confidentiality, Integrity, Anonymity, Non-interactivity, Traceability, Non-repudiation	VANETs
Kaur *et al.* [106]	Confidentiality, Integrity, Anonymity, Non-interactivity, Non-repudiation, Mutual Authentication, Key Exchange, Forward Secrecy	VANETs
Islam and Shin [109]	Authentication, Integrity, Authorized Access	Internet of Drones (IoD) in Healthcare
Chen *et al.* [112]	Sensor Calibration Good Message Delay Performance	Smart Agriculture
Wu and Tsai [115]	Identity Authentication, Key Exchange, Location Privacy, Integrity, Information Preservation, Information Accuracy	Smart Agriculture
Zhou *et al.* [116]	Decentralization, Integrity, Mutual Authentication, Key Exchange	PKI-based authentication

VII. Comparative Analysis

In this section, we perform a detailed comparative study on communication and computation costs, and also security and functionality features among the considered existing competing schemes, such as the schemes of Almadhoun *et al.* [95], Cui *et al.* [98], Jiang *et al.* [101], Jiang *et al.* [102], Yao *et al.* [103], Kaur *et al.* [106], Islam and Shin [109], Chen *et al.* [112], Wu and Tsai [115] and Zhou *et al.* [116].

A. Communication Costs Comparison

For communication cost analysis, the "identity", "random number (nonce)", "elliptic curve point of the form $P = (P_x, P_y)$ where P_x and P_y are x and y coordinates of P respectively", "hash output (if SHA-256 hash algorithm is applied)", and "timestamp" are 160, 160, $(160 + 160) = 320$, 256 and 32 bits, respectively. It is also assumed that the security level of an 160-bit elliptic curve cryptography (ECC) is same as that for an 1024-bit RSA public key cryptosystem. Under these assumptions, the comparative study on communication costs among the existing schemes is shown in Fig. 4. The communication costs needed for online computation for the schemes of Almadhoun *et al.* [95], Cui *et al.* [98], Jiang *et al.* [101], Jiang *et al.* [102], Yao *et al.* [103], Kaur *et al.* [106], Islam and Shin [109], Chen *et al.* [112], Wu and Tsai [115] and Zhou *et al.* [116] are 5160, 4384, 3424, 1542, 2944, 928, 2496, 3072 and 4096 bits, respectively. It is observed that the schemes of Kaur *et al.* [106] and Jiang *et al.* [102] need less communication costs as compared to other compared schemes.

B. Computation Costs Comparison

For computational costs comparison among the considered existing competing schemes, we consider the experimental results performed in Section VI where the average execution time for the cryptographic primitives are listed in Table III. The comparative study on computational costs among the existing schemes is shown in Fig. 5. The computation costs needed for exchange of the messages among the entities for the schemes of Almadhoun *et al.* [95], Cui *et al.* [98], Jiang *et al.* [101], Jiang *et al.* [102], Yao *et al.* [103], Kaur *et al.* [106], Islam and Shin [109], Chen *et al.* [112], Wu and Tsai [115] and Zhou *et al.* [116] are 4.13, 2.16, 5.78, 5.78, 5.08, 3.16, 20.08, 18.82 and 22.37 milliseconds, respectively. It is seen that the computation costs needed in the schemes of Islam and Shin, Wu and Tsai, and Zhou *et al.* are significantly more than other schemes.

C. Security and Functionality Features Comparison

Table IV provides a concise view of the cryptographic attributes supported by each of the existing competing schemes and the domains they are applicable to. In Table V, we have summarised the core concept of the schemes by specifying how the technology of blockchain can be leveraged alongside the cryptographic tools used in those schemes. We have also listed various potential attacks that the schemes are resistant against an adversary who is either passive or active in nature. Furthermore, Fig. 4 and 5 show the costs spent in the computations of various cryptographic operations used and in the communication of messages between various entities involved in the schemes. Finally, Table VI lists the advantages and

TABLE V
CONCEPT SUMMARY

Scheme	Blockchain usage	Cryptographic concept	Resisted attacks
Almadhoun *et al.* [95]	Fog nodes access blockchain and execute smart contracts	Hash Asymmetric Encryption	MiTM Replay DoS
Cui *et al.* [98]	Local blockchain to authenticate ordinary nodes, Public blockchain to authenticate cluster heads **Type**: Consortium	Hash Signatures	Sybil Attack MiTM Replay DoS
Jiang *et al.* [101]	PKI is stores as blockchain	Private Information Retrieval	Dishonest Node Collusion
Jiang *et al.* [102]	PKI is stores as blockchain	Private Information Retrieval	Dishonest Node Collusion
Yao *et al.* [103]	Store a registered vehicle's authentication details to be used for verification **Type**: Consortium	Elliptic Curve Cryptography	MiTM DDoS Impersonation Attack
Kaur *et al.* [106]	Store authenticator & retrieves to verify **Type**: Consortium	Elliptic Curve Cryptography	Replay Impersonation Attack
Islam and Shin [109]	Storage of Data after authentication **Type**: Consortium	Symmetric Encryption Signatures Bloom Filters	MiTM Replay Unauthorized Access Data Tampering Attacks
Wu and Tsai [115]	Distribute authentication packets over blockchain **Type**: Private	Symmetric Encryption HMAC Bilinear Pairings	MiTM Data Tampering DDoS Hardware Attacks Server Location Exposure Packet Loss Physical Device Capture Device Location Change Attacks
Zhou *et al.* [116]	Build KGC **Type**: Consortium	Identity Based Encryption	KGC Attack Key Escrow Problem Replay DDoS Session Hijacking

TABLE VI
ADVANTAGES AND DRAWBACKS COMPARISON

Scheme	Advantages	Drawbacks
Almadhoun *et al.* [95]	Low Computation Cost	1) Does not meet most IoT communication scenarios 2) High Communication Cost
Cui *et al.* [98]	Low Computation Cost	1) No support for Dynamic Node Addition 2) High Communication Cost
Jiang *et al.* [101]	1) Viable for thin clients (smartphone users) 2)Low Computation Cost	High Communication Cost
Jiang *et al.* [102]	1) Viable for thin clients (smartphone users) 2) Need not to download entire blockchain	1) Not resistant to 51% attack
Yao *et al.* [103]	Low Computation Cost	No support for mutual authentication between vehicles and service managers (SMs)
Kaur *et al.* [106]	1) Low Computation Cost 2) Low Communication Cost	ID_{OBU_i} is sent in clear text (no anonymity)
Islam and Shin [109]	1) High Connectivity 2)Low Power Transmission 3) Tested on different hardware	Expensive Computations
Chen *et al.* [112]	1) Curcumin Concentration increased by 5 times 2) 40-60% increased Chlorophyll 3) Software sensor calibration without any modification to the sensor	Less frequent sampling frequency leading to data inaccuracy
Wu and Tsai [115]	1) Lightweight Encryption 2) Multi-faceted security	Expensive Computations
Zhou *et al.* [116]	1) Inexpensive blinding technology for secure channel 2) Role replacement prevents any bias in system 3) Parallel request process enhances speed and scale of the system	1) Expensive Computations 2) High Communication Cost

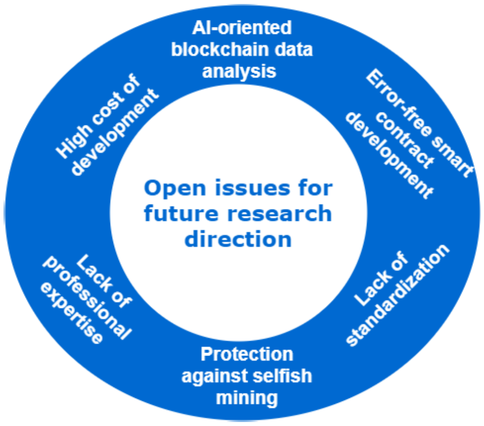

AI-oriented blockchain data analysis
Error-free smart contract development
Lack of standardization
Protection against selfish mining
Lack of professional expertise
High cost of development
Open issues for future research direction

Fig. 6. Open issues and challenges in blockchain-based smart sensing agriculture.

disadvantages of each studied scheme. It is worth to notice that there is a trade-off among the security and functionality features, core concepts applied, resilience against potential attacks, pros and cons, and also the involved communication and computation overheads in each scheme.

VIII. FUTURE RESEARCH DIRECTIONS, OPEN ISSUES AND CHALLENGES

In this section, we discuss a number of open issues and challenges that show the future directions to encourage active researchers to work in the domain of blockchain-based smart sensing agriculture environment as represented in Fig. 6.

1) AI-Based Prediction Systems: The development of security schemes can be enhanced using other fields, such as Artificial Intelligence (AI), Big data analytics and Machine Learning (ML) [120], [121]. AI/ML can be used to analyze the data of the IoT device sensors stored in the blockchain. Security schemes for smart agriculture with blockchain can be furthered towards including AI/ML based analysis by amalgamating the proposed architecture with the one given in Singh *et al.* [122]. Further research can be conducted to see how the AI/ML can be used not only in the data analysis, but also in the security schemes. Big data can used along with blockchain technology to handle the ever-increasing amount of data collected from the IoT smart devices. Thus, ML can be also used to develop learning modes which allow the system to upgrade its security system to be resistant against new attacks for which the the scheme was not designed initially.

2) Error-Free Development of Smart Contracts: Smart contracts have the capability of automating the processes inside the blockchain. Any error or bug in a smart contract can lead to erroneous data being recorded in the blockchain. Since a blockchain can be used as a backbone for a number of applications, such bugs in smart contracts end in disastrous implications.

3) Lack of Standardization: Currently, no standards exist for the operation of a blockchain. It can lead to major incompatibility among organizations with regards to governance and interoperability.

4) Lack of Professional Expertise: Due to the novelty of the blockchain concept, very few technologists have the skills required to sustain this field.

5) High Cost of Development: Adding a block to a blockchain is an expensive operation. It takes about USD 550 to add a work to the blockchain. It is imperative to find methods to reduce this cost significantly.

6) Protection Against Selfish Mining: In blockchain with small number of nodes, it is crucial to ensure that computational resources are not piled by a single miner node or a small group of miner nodes in excess. Such a situation can lead to successful tampering or reversing of the blockchain. There has been no instance of such an attack until now, but current systems are not equipped to deal with such circumstances in case they occur in near future.

IX. Conclusion

In this paper, a systematic survey has been conducted on the usage and applications of blockchain technology in smart agriculture in providing security goals. A thorough analysis has been made on the security attributes, application areas, advantages, drawbacks, and costs of computation and communication involved in the considered existing competing schemes. This study has led to identification for future directions for some open and challenging problems towards which the research should be propelled.

Acknowledgment

The authors thank the anonymous reviewers and associate editor for their valuable feedback on the paper, which helped us to improve its quality and presentation.

References

[1] (2019). *World Population Prospects 2019: Highlights* United Nations, Department of Economic and Social Affairs, Population Division. [Online]. Available: https://population.un.org/wpp/Publications/Files/WPP2019_Highlights.pdf

[2] (2019). *The State of Food and Agriculture*. Food and Agriculture Organization of the United Nations. [Online]. Available: http://www.fao.org/3/ca6030en/ca6030en.pdf

[3] M. Duque-Acevedo, L. J. Belmonte-Urena, F. J. Cortes-Garcia, and F. Camacho-Ferre, "Agricultural waste: Review of the evolution, approaches and perspectives on alternative uses," *Global Ecol. Conservation*, vol. 22, Jun. 2020, Art. no. e00902.

[4] (2014). *Food Wastage Footprint-Full Cost Accounting*. Food and Agriculture Organization of the United Nations. [Online]. Available: http://www.fao.org/3/a-i3991e.pdf

[5] J. Vora, S. Tanwar, S. Tyagi, N. Kumar, and J. J. P. C. Rodrigues, "Home-based exercise system for patients using IoT enabled smart speaker," in *Proc. IEEE 19th Int. Conf. e-Health Netw., Appl. Services (Healthcom)*, Dalian, China, Oct. 2017, pp. 1–6.

[6] V. Saiz-Rubio and F. Rovira-Más, "From smart farming towards agriculture 5.0: A review on crop data management," *Agronomy*, vol. 10, no. 2, p. 207, Feb. 2020.

[7] U. Shafi, R. Mumtaz, J. García-Nieto, S. A. Hassan, S. A. R. Zaidi, and N. Iqbal, "Precision agriculture techniques and practices: From considerations to applications," *Sensors*, vol. 19, no. 17, p. 3796, Sep. 2019.

[8] 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.

[9] J. M. Talavera *et al.*, "Review of IoT applications in agro-industrial and environmental fields," *Comput. Electron. Agricult.*, vol. 142, pp. 283–297, Nov. 2017.

[10] L. P. Reynolds, M. C. Wulster-Radcliffe, D. K. Aaron, and T. A. Davis, "Importance of animals in agricultural sustainability and food security," *J. Nutrition*, vol. 145, no. 7, pp. 1377–1379, Jul. 2015.

[11] R. Gebbers and V. I. Adamchuk, "Precision agriculture and food security," *Science*, vol. 327, no. 5967, pp. 828–831, Feb. 2010.

[12] C. Hedley, "The role of precision agriculture for improved nutrient management on farms," *J. Sci. Food Agricult.*, vol. 95, no. 1, pp. 12–19, Jan. 2015.

[13] (2020). *MIRACL Cryptographic SDK: Multiprecision Integer and Rational Arithmetic Cryptographic Library*. Accessed: Jul. 2020. [Online]. Available: https://github.com/miracl/MIRACL

[14] A. K. Das, S. Zeadally, and D. He, "Taxonomy and analysis of security protocols for Internet of Things," *Future Gener. Comput. Syst.*, vol. 89, pp. 110–125, Dec. 2018.

[15] P. C. Kocher, J. Jaffe, and B. Jun, "Differential power analysis," in *Proc. 19th Annu. Int. Cryptol. Conf. (CRYPTO)*, Santa Barbara, CA, USA, 1999, pp. 388–397.

[16] P. C. Kocher, "Timing attacks on implementations of Diffie-Hellman, RSA, DSS, and other systems," in *Proc. 16th Annu. Int. Cryptol. Conf.-Adv. Cryptol. (CRYPTO)*, Barbara, CA, USA, 1996, pp. 104–113.

[17] A. D. Wood and J. A. Stankovic, "Denial of service in sensor networks," *Computer*, vol. 35, no. 10, pp. 54–62, Oct. 2002.

[18] Y.-C. Hu, A. Perrig, and D. B. Johnson, "Packet leashes: A defense against wormhole attacks in wireless networks," in *Proc. 22nd Annu. Joint Conf. IEEE Comput. Commun. Societies (INFOCOM)*, vol. 3. San Francisco, California, USA, Mar./Apr. 2003, pp. 1976–1986.

[19] J. R. Douceur, "The Sybil Attack," in *Peer-to-Peer Systems*. Berlin, Germany: Springer, 2002, pp. 251–260.

[20] J. Newsome, E. Shi, D. Song, and A. Perrig, "The sybil attack in sensor networks: Analysis & defenses," in *Proc. 3rd Int. Symp. Inf. Process. Sensor Netw. (IPSN)*, Berkeley, CA, USA, 2004, pp. 259–268.

[21] A. Kumari, R. Gupta, S. Tanwar, and N. Kumar, "Blockchain and AI amalgamation for energy cloud management: Challenges, solutions, and future directions," *J. Parallel Distrib. Comput.*, vol. 143, pp. 148–166, Sep. 2020.

[22] B. Parno, A. Perrig, and V. Gligor, "Distributed detection of node replication attacks in sensor networks," in *Proc. IEEE Symp. Secur. Privacy (S&P'05)*, Oakland, CA, USA, May 2005, pp. 49–63.

[23] D. Dolev and A. Yao, "On the security of public key protocols," *IEEE Trans. Inf. Theory*, vol. 29, no. 2, pp. 198–208, Mar. 1983.

[24] R. Canetti and H. Krawczyk, "Universally composable notions of key exchange and secure channels," in *Proc. Int. Conf. Theory Appl. Cryptograph. Techn. (EUROCRYPT)*, Amsterdam, The Netherlands, 2002, pp. 337–351.

[25] T. S. Messerges, E. A. Dabbish, and R. H. Sloan, "Examining smart-card security under the threat of power analysis attacks," *IEEE Trans. Comput.*, vol. 51, no. 5, pp. 541–552, May 2002.

[26] R. Gupta, A. Kumari, and S. Tanwar, "A taxonomy of blockchain envisioned edge-as-a-connected autonomous vehicles," *Trans. Emerg. Telecommun. Technol.*, to be published.

[27] I. Mistry, S. Tanwar, S. Tyagi, and N. Kumar, "Blockchain for 5G-enabled IoT for industrial automation: A systematic review, solutions, and challenges," *Mech. Syst. Signal Process.*, vol. 135, Jan. 2020, Art. no. 106382.

[28] U. Bodkhe *et al.*, "Blockchain for industry 4.0: A comprehensive review," *IEEE Access*, vol. 8, pp. 79764–79800, 2020.

[29] S. Nakamoto, *Bitcoin Open Source Implementation of P2P Currency*, P2P Foundation, Amsterdam, The Netherlands, vol. 18, 2009.

[30] A. Narayanan, J. Bonneau, E. Felten, A. Miller, and S. Goldfeder, *Bitcoin Cryptocurrency Technologies: A Comprehensive Introduction*. Princeton, NJ, USA: Princeton Univ. Press, 2016.

[31] Z. Zheng, S. Xie, H.-N. Dai, X. Chen, and H. Wang, "Blockchain challenges and opportunities: A survey," *Int. J. Web Grid Services*, vol. 14, no. 4, pp. 352–375, 2018.

[32] A. Jindal, G. S. Aujla, and N. Kumar, "SURVIVOR: A blockchain based edge-as-a-service framework for secure energy trading in SDN-enabled vehicle-to-grid environment," *Comput. Netw.*, vol. 153, pp. 36–48, Apr. 2019.

[33] S. Tanwar, Q. Bhatia, P. Patel, A. Kumari, P. K. Singh, and W.-C. Hong, "Machine learning adoption in blockchain-based smart applications: The challenges, and a way forward," *IEEE Access*, vol. 8, pp. 474–488, 2020.

[34] P. K. Sharma, N. Kumar, and J. H. Park, "Blockchain-based distributed framework for automotive industry in a smart city," *IEEE Trans. Ind. Informat.*, vol. 15, no. 7, pp. 4197–4205, Jul. 2019.

[35] A. Chauhan, O. P. Malviya, M. Verma, and T. S. Mor, "Blockchain and scalability," in *Proc. IEEE Int. Conf. Softw. Qual., Rel. Secur. Companion (QRS-C)*, Lisbon, Portugal, Jul. 2018, pp. 122–128.

[36] G. Karame, “On the security and scalability of Bitcoin’s blockchain,” in *Proc. ACM SIGSAC Conf. Comput. Commun. Secur.*, Oct. 2016, pp. 1861–1862.

[37] G. Malavolta, P. Moreno-Sanchez, C. Schneidewind, A. Kate, and M. Maffei, “Anonymous multi-hop locks for blockchain scalability and interoperability,” in *Proc. Netw. Distrib. Syst. Secur. Symp.*, 2019, pp. 1–30.

[38] S. Kim, Y. Kwon, and S. Cho, “A survey of scalability solutions on blockchain,” in *Proc. Int. Conf. Inf. Commun. Technol. Converg. (ICTC)*, Oct. 2018, pp. 1204–1207.

[39] S. Meiklejohn *et al.*, “A fistful of bitcoins: Characterizing payments among men with no names,” in *Proc. Conf. Internet Meas. Conf.*, 2013, pp. 127–140.

[40] A. Kosba, A. Miller, E. Shi, Z. Wen, and C. Papamanthou, “Hawk: The blockchain model of cryptography and privacy-preserving smart contracts,” in *Proc. IEEE Symp. Secur. Privacy (SP)*, May 2016, pp. 839–858.

[41] A. Biryukov, D. Khovratovich, and I. Pustogarov, “Deanonymisation of clients in bitcoin P2P network,” in *Proc. ACM SIGSAC Conf. Comput. Commun. Secur. (CCS)*, 2014, pp. 15–29.

[42] P. Koshy, D. Koshy, and P. McDaniel, “An analysis of anonymity in bitcoin using P2P network traffic,” in *Proc. 18th Int. Conf. Financial Cryptogr. Data Secur.*, Christ Church, Barbados, 2014, pp. 469–485.

[43] I. D. Mastan and S. Paul, “A new approach to deanonymization of unreachable bitcoin nodes,” in *Proc. 17th Int. Conf. Cryptol. Netw. Secur.*, Naples, Italy, 2018, pp. 277–298.

[44] Q. ShenTu and J. Yu, “Research on anonymization and de-anonymization in the bitcoin system,” 2015, *arXiv:1510.07782*. [Online]. Available: https://arxiv.org/abs/1510.07782

[45] Q. Bai, X. Zhou, X. Wang, Y. Xu, X. Wang, and Q. Kong, “A deep dive into blockchain selfish mining,” in *Proc. ICC - IEEE Int. Conf. Commun. (ICC)*, May 2019, pp. 1–6.

[46] A. Sapirshtein, Y. Sompolinsky, and A. Zohar, “Optimal selfish mining strategies in bitcoin,” in *Proc. 20th Int. Conf. Financial Cryptogr. Data Secur.* Berlin, Germany: Springer 2017, pp. 515–532.

[47] W. Wang *et al.*, “A survey on consensus mechanisms and mining strategy management in blockchain networks,” *IEEE Access*, vol. 7, pp. 22328–22370, 2019.

[48] Q. Feng, D. He, S. Zeadally, M. K. Khan, and N. Kumar, “A survey on privacy protection in blockchain system,” *J. Netw. Comput. Appl.*, vol. 126, pp. 45–58, Jan. 2019.

[49] S. Tanwar, K. Parekh, and R. Evans, “Blockchain-based electronic healthcare record system for healthcare 4.0 applications,” *J. Inf. Secur. Appl.*, vol. 50, Feb. 2020, Art. no. 102407.

[50] U. Bodkhe, P. Bhattacharya, S. Tanwar, S. Tyagi, N. Kumar, and M. S. Obaidat, “BloHosT: Blockchain enabled smart tourism and hospitality management,” in *Proc. Int. Conf. Comput., Inf. Telecommun. Syst. (CITS)*, Aug. 2019, pp. 1–5.

[51] P. Bhattacharya, S. Tanwar, U. Bodke, S. Tyagi, and N. Kumar, “BinDaaS: Blockchain-based deep-learning as-a-Service in healthcare 4.0 applications,” *IEEE Trans. Netw. Sci. Eng.*, early access, Dec. 25, 2019, doi: 10.1109/TNSE.2019.2961932.

[52] R. Zhang, R. Xue, and L. Liu, “Security and privacy on blockchain,” *ACM Comput. Surv.*, vol. 52, no. 3, p. 51, 2019.

[53] K. Christidis and M. Devetsikiotis, “Blockchains and smart contracts for the Internet of Things,” *IEEE Access*, vol. 4, pp. 2292–2303, 2016.

[54] V. Buterin. *Thoughts on UTXOs*. Accessed: Jan. 9, 2020. [Online]. Available: https://medium.com/@ConsenSys/thoughts-on-utxo-by-vitalik-buterin-2bb782c67e53

[55] N. Szabo. *Smart Contracts*. Accessed: Mar. 15, 2020. [Online]. Available: http://szabo.best.vwh.net/smart.contracts.html

[56] S. Aggarwal, R. Chaudhary, G. S. Aujla, N. Kumar, K.-K.-R. Choo, and A. Y. Zomaya, “Blockchain for smart communities: Applications, challenges and opportunities,” *J. Netw. Comput. Appl.*, vol. 144, pp. 13–48, Oct. 2019.

[57] G.-T. Nguyen and K. Kim, “A survey about consensus algorithms used in blockchain,” *J. Inf. Process. Syst.*, vol. 14, no. 1, pp. 101–128, 2018.

[58] D. Schwartz *et al.*, “The ripple protocol consensus algorithm,” *Ripple Labs Inc White Paper*, vol. 5, no. 8, pp. 1–8, 2014.

[59] L. Lamport, R. Shostak, and M. Pease, “The byzantine generals problem,” *ACM Trans. Program. Lang. Syst. (TOPLAS)*, vol. 4, no. 3, pp. 382–401, Jul. 1982.

[60] M. Castro and B. Liskov, “Practical byzantine fault tolerance and proactive recovery,” *ACM Trans. Comput. Syst. (TOCS)*, vol. 20, no. 4, pp. 398–461, Nov. 2002.

[61] U. Bodkhe, D. Mehta, S. Tanwar, P. Bhattacharya, P. K. Singh, and W.-C. Hong, “A survey on decentralized consensus mechanisms for cyber physical systems,” *IEEE Access*, vol. 8, pp. 54371–54401, 2020.

[62] S. King and S. Nadal, “PPCoin: Peer-to-peer crypto-currency with proof-of-stake,” Tech. Rep., 2012.

[63] I. Bentov, C. Lee, A. Mizrahi, and M. Rosenfeld, “Proof of activity: Extending bitcoin’s proof of work via proof of stake [extended abstract],” *ACM SIGMETRICS Perform. Eval. Rev.*, vol. 42, no. 3, pp. 34–37, 2014.

[64] *DPOS Consensus Algorithm-The Missing White Paper*. Accessed: Mar. 15, 2020. [Online]. Available: https://steemit.com/dpos/@dantheman/dpos-consensus-algorithm-this-missing-white-paper

[65] I. Stewart. (2012). *Proof of Burn-Bitcoin Wiki*. [Online]. Available: https://en.bitcoin.it/wiki/Proof_of_burn

[66] (2014). *Intel Software Guard Extensions Programming Reference*. [Online]. Available: https://software.intel.com/sites/default/files/managed/48/88/329298-002.pdf

[67] M. Milutinovic, W. He, H. Wu, and M. Kanwal, “Proof of luck: An efficient blockchain consensus protocol,” in *Proc. 1st Workshop Syst. Softw. Trusted Execution (SysTEX)*, no. 2. Tento, Italy, 2016, pp. 1–6.

[68] S. Dziembowski, S. Faust, V. Kolmogorov, and K. Pietrzak, “Proofs of space,” in *Advances in Cryptology (CRYPTO)*. Santa Barbara, CA, USA: Springer, 2015, pp. 585–605.

[69] F. Tschorsch and B. Scheuermann, “Bitcoin and beyond: A technical survey on decentralized digital currencies,” *IEEE Commun. Surveys Tuts.*, vol. 18, no. 3, pp. 2084–2123, 3rd Quart., 2016.

[70] S. Zhang and J.-H. Lee, “A group signature and authentication scheme for blockchain-based mobile-edge computing,” *IEEE Internet Things J.*, vol. 7, no. 5, pp. 4557–4565, May 2020.

[71] (2014). *The XRP Ledger*. [Online]. Available: https://xrpl.org/consensus-principles-and-rules.html

[72] J. Kwon, “Tendermint: Consensus without mining,” Self-Published Paper (Draft v.0.6), vol. 1, no. 11, 2014. [Online]. Available: https://tendermint.com/static/docs/tendermint.pdf

[73] G. Wood, “Ethereum: A secure decentralised generalised transaction ledger,” *Ethereum Project Yellow Paper*, vol. 151, pp. 1–32, Apr. 2014.

[74] I. Bentov, R. Pass, and E. Shi, “Snow white: Provably secure proofs of stake,” IACR Cryptol. ePrint Arch., Tech. Rep. 919, 2016.

[75] A. Kiayias, A. Russell, B. David, and R. Oliynykov, “Ouroboros: A provably secure proof-of-stake blockchain protocol,” in *Proc. Annu. Int. Cryptol. Conf. (CRYPTO)*, Santa Barbara, CA, USA, 2017, pp. 357–388.

[76] (2014). *Slimcoin: A Peer-to-Peer Crypto-Currency with Proof-of-Burn-Mining without Powerful Hardware*. [Online]. Available: https://github.com/slimcoin-project/slimcoin-project.github.io/raw/master/whitepaperSLM.pdf

[77] S. L. Inc. *Storj: A Decentralized Cloud Storage Network Framework-WhitePaper*. Accessed: Apr. 29, 2020. [Online]. Available: https://storj.io/storj.pdf

[78] D. Gunasekera and E. Valenzuela, “Adoption of blockchain technology in the australian grains trade: An assessment of potential economic effects,” *Econ. Papers: A J. Appl. Econ. Policy*, vol. 39, no. 2, pp. 152–161, Jun. 2020.

[79] *e-Agriculture in Action: Blockchain for Agriculture-Opportunities and Challenges*, Food and Agriculture Organization of the United Nations and International Telecommunication Union, Bangkok, Thailand, 2019. [Online]. Available: http://www.fao.org/3/CA2906EN/ca2906en.pdf

[80] P. Mehta, R. Gupta, and S. Tanwar, “Blockchain envisioned UAV networks: Challenges, solutions, and comparisons,” *Comput. Commun.*, vol. 151, pp. 518–538, Feb. 2020.

[81] S. Banerjee *et al.*, “Design of an anonymity-preserving group formation based authentication protocol in global mobility networks,” *IEEE Access*, vol. 6, pp. 20673–20693, 2018.

[82] X. Li, T. Liu, M. S. Obaidat, F. Wu, P. Vijayakumar, and N. Kumar, “A lightweight privacy-preserving authentication protocol for VANETs,” *IEEE Syst. J.*, early access, May 25, 2020, doi: 10.1109/JSYST.2020.2991168.

[83] X. Li, J. Niu, S. Kumari, F. Wu, and K.-K.-R. Choo, “A robust biometrics based three-factor authentication scheme for global mobility networks in smart city,” *Future Gener. Comput. Syst.*, vol. 83, pp. 607–618, Jun. 2018.

[84] D. Mishra, A. K. Das, and S. Mukhopadhyay, “A secure and efficient ECC-based user anonymity-preserving session initiation authentication protocol using smart card,” *Peer–Peer Netw. Appl.*, vol. 9, no. 1, pp. 171–192, Jan. 2016.

[85] V. Odelu, A. K. Das, and A. Goswami, "SEAP: Secure and efficient authentication protocol for NFC applications using pseudonyms," *IEEE Trans. Consum. Electron.*, vol. 62, no. 1, pp. 30–38, Feb. 2016.

[86] M. Wazid, A. K. Das, S. Kumari, X. Li, and F. Wu, "Design of an efficient and provably secure anonymity preserving three-factor user authentication and key agreement scheme for TMIS," *Secur. Commun. Netw.*, vol. 9, no. 13, pp. 1983–2001, Sep. 2016.

[87] X. Li, S. Liu, F. Wu, S. Kumari, and J. J. P. C. Rodrigues, "Privacy preserving data aggregation scheme for mobile edge computing assisted IoT applications," *IEEE Internet Things J.*, vol. 6, no. 3, pp. 4755–4763, Jun. 2019.

[88] A. K. Das, M. Wazid, N. Kumar, A. V. Vasilakos, and J. J. P. C. Rodrigues, "Biometrics-based privacy-preserving user authentication scheme for cloud-based industrial Internet of Things deployment," *IEEE Internet Things J.*, vol. 5, no. 6, pp. 4900–4913, Dec. 2018.

[89] M. Wazid *et al.*, "Design of lightweight authentication and key agreement protocol for vehicular ad hoc networks," *IEEE Access*, vol. 5, pp. 14966–14980, 2017.

[90] M. Wazid, A. K. Das, N. Kumar, and J. J. P. C. Rodrigues, "Secure three-factor user authentication scheme for Renewable-Energy-Based smart grid environment," *IEEE Trans. Ind. Informat.*, vol. 13, no. 6, pp. 3144–3153, Dec. 2017.

[91] A. K. Das, S. Kumari, V. Odelu, X. Li, F. Wu, and X. Huang, "Provably secure user authentication and key agreement scheme for wireless sensor networks," *Secur. Commun. Netw.*, vol. 9, no. 16, pp. 3670–3687, Nov. 2016.

[92] A. K. Das, "A secure user anonymity-preserving three-factor remote user authentication scheme for the telecare medicine information systems," *J. Med. Syst.*, vol. 39, no. 3, p. 30, Mar. 2015.

[93] A. Dua, N. Kumar, A. K. Das, and W. Susilo, "Secure message communication protocol among vehicles in smart city," *IEEE Trans. Veh. Technol.*, vol. 67, no. 5, pp. 4359–4373, May 2018.

[94] S. Chatterjee, A. K. Das, and J. K. Sing, "A novel and efficient user access control scheme for wireless body area sensor networks," *J. King Saud Univ.-Comput. Inf. Sci.*, vol. 26, no. 2, pp. 181–201, Jul. 2014.

[95] R. Almadhoun, M. Kadadha, M. Alhemeiri, M. Alshehhi, and K. Salah, "A user authentication scheme of IoT devices using blockchain-enabled fog nodes," in *Proc. IEEE/ACS 15th Int. Conf. Comput. Syst. Appl. (AICCSA)*, Oct. 2018, pp. 1–8.

[96] A. Kumari, S. Tanwar, S. Tyagi, and N. Kumar, "Fog computing for healthcare 4.0 environment: Opportunities and challenges," *Comput. Electr. Eng.*, vol. 72, pp. 1–13, Nov. 2018.

[97] R. Singh, S. Tanwar, and T. P. Sharma, "Utilization of blockchain for mitigating the distributed denial of service attacks," *Secur. Privacy*, vol. 3, no. 3, May 2020.

[98] Z. Cui *et al.*, "A hybrid BlockChain-based identity authentication scheme for multi-WSN," *IEEE Trans. Services Comput.*, vol. 13, no. 2, pp. 241–251, Apr. 2020.

[99] R. Gupta, S. Tanwar, F. Al-Turjman, P. Italiya, A. Nauman, and S. W. Kim, "Smart contract privacy protection using AI in cyber-physical systems: Tools, techniques and challenges," *IEEE Access*, vol. 8, pp. 24746–24772, 2020.

[100] J. Vora *et al.*, "BHEEM: A blockchain-based framework for securing electronic health records," in *Proc. IEEE Globecom Workshops (GC Wkshps)*, Dec. 2018, pp. 1–6.

[101] W. Jiang, H. Li, G. Xu, M. Wen, G. Dong, and X. Lin, "A privacy-preserving thin-client scheme in blockchain-based PKI," in *Proc. IEEE Global Commun. Conf. (GLOBECOM)*, Dec. 2018, pp. 1–6.

[102] 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.

[103] Y. Yao, X. Chang, J. Misic, V. B. Misic, and L. Li, "BLA: Blockchain-assisted lightweight anonymous authentication for distributed vehicular fog services," *IEEE Internet Things J.*, vol. 6, no. 2, pp. 3775–3784, Apr. 2019.

[104] A. Kumari, S. Tanwar, S. Tyagi, N. Kumar, R. M. Parizi, and K.-K.-R. Choo, "Fog data analytics: A taxonomy and process model," *J. Netw. Comput. Appl.*, vol. 128, pp. 90–104, Feb. 2019.

[105] A. Kumari, S. Tanwar, S. Tyagi, N. Kumar, M. S. Obaidat, and J. J. P. C. Rodrigues, "Fog computing for smart grid systems in the 5G environment: Challenges and solutions," *IEEE Wireless Commun.*, vol. 26, no. 3, pp. 47–53, Jun. 2019.

[106] K. Kaur, S. Garg, G. Kaddoum, F. Gagnon, and S. H. Ahmed, "Blockchain-based lightweight authentication mechanism for vehicular fog infrastructure," in *Proc. IEEE Int. Conf. Commun. Workshops (ICC Workshops)*, May 2019, pp. 1–6.

[107] J. Bhatia, Y. Modi, S. Tanwar, and M. Bhavsar, "Software defined vehicular networks: A comprehensive review," *Int. J. Commun. Syst.*, vol. 32, no. 12, p. e4005, Aug. 2019.

[108] S. Tanwar, J. Vora, S. Tyagi, N. Kumar, and M. S. Obaidat, "A systematic review on security issues in vehicular ad hoc network," *Secur. Privacy*, vol. 1, no. 5, p. e39, Sep. 2018.

[109] A. Islam and S. Young Shin, "A blockchain-based secure healthcare scheme with the assistance of unmanned aerial vehicle in Internet of Things," *Comput. Electr. Eng.*, vol. 84, Jun. 2020, Art. no. 106627.

[110] R. Gupta, S. Tanwar, S. Tyagi, N. Kumar, M. S. Obaidat, and B. Sadoun, "HaBiTs: Blockchain-based telesurgery framework for healthcare 4.0," in *Proc. Int. Conf. Comput., Inf. Telecommun. Syst. (CITS)*, Beijing, China, Aug. 2019, pp. 1–5.

[111] J. Hathaliya, P. Sharma, S. Tanwar, and R. Gupta, "Blockchain-based remote patient monitoring in healthcare 4.0," in *Proc. IEEE 9th Int. Conf. Adv. Comput. (IACC)*, Dec. 2019, pp. 87–91.

[112] W.-L. Chen *et al.*, "AgriTalk: IoT for precision soil farming of turmeric cultivation," *IEEE Internet Things J.*, vol. 6, no. 3, pp. 5209–5223, Jun. 2019.

[113] S. Tanwar, S. Tyagi, and S. Kumar, "The role of Internet of Things and smart grid for the development of a smart city," in *Intelligent Communication and Computational Technologies*. Singapore: Springer, 2018, pp. 23–33.

[114] R. Gupta, S. Tanwar, S. Tyagi, and N. Kumar, "Tactile Internet and its applications in 5G era: A comprehensive review," *Int. J. Commun. Syst.*, vol. 32, no. 14, p. e3981, Sep. 2019.

[115] H.-T. Wu and C.-W. Tsai, "An intelligent agriculture network security system based on private blockchains," *J. Commun. Netw.*, vol. 21, no. 5, pp. 503–508, Oct. 2019.

[116] B. Zhou, H. Li, and L. Xu, "An authentication scheme using identity-based encryption & blockchain," in *Proc. IEEE Symp. Comput. Commun. (ISCC)*, Natal, Brazil, Jun. 2018, pp. 556–561.

[117] (Nov. 2001). *Advanced Encryption Standard*. FIPS PUB 197, Nat. Inst. Standards Technol. (NIST), U.S. Dept. Commerce. Accessed: Jun. 2020. [Online]. Available: http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf

[118] W. E. May (Apr. 1995). *Secure Hash Standard*. 2015. FIPS PUB 180-1, National Institute of Standards and Technology (NIST), U.S. Department of Commerce. Accessed: Jun. 2020. [Online]. Available: http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.180-4.pdf

[119] D. Johnson, A. Menezes, and S. Vanstone, "The elliptic curve digital signature algorithm (ECDSA)," *Int. J. Inf. Secur.*, vol. 1, no. 1, pp. 36–63, Aug. 2001.

[120] R. Gupta, S. Tanwar, S. Tyagi, and N. Kumar, "Machine learning models for secure data analytics: A taxonomy and threat model," *Comput. Commun.*, vol. 153, pp. 406–440, Mar. 2020.

[121] A. Kumari, S. Tanwar, S. Tyagi, and N. Kumar, "Verification and validation techniques for streaming big data analytics in Internet of Things environment," *IET Netw.*, vol. 8, no. 3, pp. 155–163, May 2019.

[122] S. K. Singh, S. Rathore, and J. H. Park, "BlockIoTIntelligence: A blockchain-enabled intelligent IoT architecture with artificial intelligence," *Future Gener. Comput. Syst.*, vol. 110, pp. 721–743, Sep. 2020.

Anusha Vangala received the M.Tech. degree in computer science and engineering from Jawaharlal Nehru Technological University, Kakinada, India. She is currently pursuing the Ph.D. degree in computer science and engineering with the Center for Security, Theory and Algorithmic Research, International Institute of Information Technology (IIIT) Hyderabad, India. Prior to joining Ph.D. program at IIIT Hyderabad, she had nearly five years of experience as an Assistant Professor of Computer Science and Engineering at various renowned institutes across India. Her research interests include cryptographic security in cloud computing, wireless sensor networks, the Internet of Things (IoT), and blockchain Technology.

Ashok Kumar Das (Senior Member, IEEE) received the M.Sc. degree in mathematics, the M.Tech. degree in computer science and data processing, and the Ph.D. degree in computer science and engineering from IIT Kharagpur, India. He is currently an Associate Professor with the Center for Security, Theory and Algorithmic Research, International Institute of Information Technology (IIIT) Hyderabad, Hyderabad, India. His current research interests include cryptography and network security, including security in smart grid, the Internet of Things (IoT), Internet of Drones (IoD), Internet of Vehicles (IoV), cyber-physical systems (CPS) and cloud computing, blockchain, and AI/ML security. He has authored over 230 articles in international journals and conferences in the above areas, including over 195 reputed journal articles. He was a recipient of the Institute Silver Medal from IIT Kharagpur. He is on the Editorial Board of the *KSII Transactions on Internet and Information Systems*, the *International Journal of Internet Technology and Secured Transactions* (Inderscience), and *IET Communications*, is a Guest Editor of *Computers & Electrical Engineering* (Elsevier) for the special issue on Big data and IoT in e-healthcare and of *ICT Express* (Elsevier) for the special issue on Blockchain Technologies and Applications for 5G Enabled IoT, and has served as a program committee member of many international conferences. He also severed as one of the technical program committee chairs of the first International Congress on Blockchain and Applications (BLOCKCHAIN'19), Avila, Spain, in 2019, and the second International Congress on Blockchain and Applications (BLOCKCHAIN'20), L'Aquila, Italy, in 2020.

Neeraj Kumar (Senior Member, IEEE) received the Ph.D. degree in CSE from Shri Mata Vaishno Devi University, Katra, India. He was a Postdoctoral Research Fellow at Coventry University, Coventry, U.K. He is working as Full Professor with the Department of Computer Science and Engineering, Thapar Institute of Engineering and Technology (Deemed to be University), Patiala, India. He has published more than 400 technical research articles in leading journals and conferences from IEEE, Elsevier, Springer, and John Wiley. Some of his research findings are published in top-cited journals, such as the IEEE TRANSACTIONS ON KNOWLEDGE AND DATA ENGINEERING, the IEEE TRANSACTIONS ON INDUSTRIAL ELECTRONICS, the IEEE TRANSACTIONS ON DEPENDABLE AND SECURE COMPUTING, the IEEE TRANSACTIONS ON INTELLIGENT TRANSPORTATION SYSTEMS, the IEEE TRANSACTIONS ON CONSUMER ELECTRONICS, the IEEE TRANSACTIONS ON INDUSTRIAL INFORMATICS, the IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY, the IEEE TRANSACTIONS ON INTELLIGENT TRANSPORTATION SYSTEMS, the IEEE NETWORK, the IEEE COMMUNICATIONS LETTERS, the IEEE WIRELESS COMMUNICATIONS LETTERS, the IEEE INTERNET OF THINGS JOURNAL, the IEEE SYSTEMS JOURNAL, *Future Generation Computing Systems*, the *Journal of Network and Computer Applications*, and *Computer Communications*. He has won many prestigious awards such as the Highly Cited Researcher 2019 from WoS, the Best Paper Award from the IEEE SYSTEM JOURNAL, the IEEE ICC Best Paper Award, and so on. He has written/edited more than 10 books from CRC, Elsevier, Springer, BPB, and so on. He is on the Editorial Board of *ACM Computing Survey*, the IEEE TRANSACTIONS ON SUSTAINABLE COMPUTING, the *IEEE Network Magazine*, the *IEEE Communication Magazine*, the *Journal of Networks and Computer Applications* (Elsevier), *Computer Communications* (Elsevier), the *International Journal of Communication Systems* (Wiley), and *Security and Privacy* (Wiley).

Mamoun Alazab (Senior Member, IEEE) received the Ph.D. degree in computer science from the School of Science, Information Technology and Engineering, Federation University of Australia. He is currently an Associate Professor with the College of Engineering, IT and Environment, Charles Darwin University, Australia. He is also a Cyber Security Researcher and a Practitioner with industry and academic experience. His research is multidisciplinary that focuses on cybersecurity and digital forensics of computer systems with a focus on cybercrime detection and prevention, including cyber terrorism and cyber warfare. He works closely with government and industry on many projects, including the Northern Territory (NT) Department of Information and Corporate Services, IBM, Trend Micro, and the Australian Federal Police (AFP). He is the Founder and the Chair of the IEEE Northern Territory (NT) Subsection Detection and Prevention.