Received November 18, 2021, accepted December 6, 2021, date of publication December 13, 2021,
date of current version January 12, 2022.

Digital Object Identifier 10.1109/ACCESS.2021.3135371

ProChain: Provenance-Aware Traceability Framework for IoT-Based Supply Chain Systems

MABROOK S. AL-RAKHAMI, (Member, IEEE), AND MAJED AL-MASHARI, (Member, IEEE)
Department of Information Systems, College of Computer and Information Sciences, King Saud University, Riyadh 11543, Saudi Arabia

Corresponding author: Mabrook S. Al-Rakhami (malrakhami@ksu.edu.sa)

This work was supported by Researchers Supporting Project number (RSP2022R517), King Saud University, Riyadh, Saudi Arabia.

ABSTRACT The current value of the world food system amounts to roughly $8 trillion, which represents approximately 10% of the global economies. Therefore, the quality of food and food products concerns not only all the end consumers but also millions of employees and entrepreneurs within the global food industry. Achieving the best possible quality of food throughout all the engaged processes requires constantly tracing and monitoring several crucial environmental conditions that may have a significant impact on the products' quality. The Industrial Internet of Things (IIoT) is a system of dedicated sensors paired with the Internet that can overcome and prevent issues within the food industry. The interconnected elements bear the responsibility for monitoring, evaluating, and tracking the conditions where the food products undergo processing, and it checks the products' quality throughout their life cycle. Nevertheless, even IIoT has its challenges. The first such challenge relates to the storage and accessibility of the obtained data. What can make the data readily available to all individuals and entities involved in the industry? The second significant challenge relates to tracing items that pass through numerous processes involving different parties. This work proposed ProChain, a Provenance-aware Traceability Framework for IoT-based Supply Chain Systems. A proposed comprehensive framework of all the information acquired by the sensors and the complete set of provenance data addressed these challenges. Additionally, a thorough simulation of the proposed framework on the Raspberry PI 3B IoT device reviewed the ProChain efficiency in the cloud and local simulation environments. ProChain demonstrated tractability, transparency, and complex security as examples of the principal attributes of the IOTA 2.0 protocol in the food industry.

INDEX TERMS Supply chain management, Internet of Things, traceability, provenance, IoT.

I. INTRODUCTION

The utilization of IoT technologies within the food industry creates a new paradigm known as the Industrial Internet of Things (IIoT) [1]. The sensors and other IoT devices produce, collect, and process a vast quantity of information, while they also communicate and interact with one another and remote devices [2]. IoT devices also trace and monitor numerous processes to overcome automation issues within the supply chain systems (SCs). For example, in the case of the food supply chain, the deployed IoT devices track and monitor the qualities of specific food items, such as various perishable products [3]. This type of control is crucial because all food products are required to comply with the strict global standards (e.g., Hazard Analysis and Critical Control Points – HACCP) [4]. If this process of monitoring and control fails, the products can become a health risk for the consumers.

In the light of the aforementioned issue, traceability constitutes an integral factor for successful and efficient management of the supply chain systems, which are, at the same time, constantly becoming more complex and complicated [5]. Currently, tons of globally produced food products are manufactured, transported, and sold with little to no awareness about their production, storage, or transportation [6]. Thus, traceability plays a crucial role in improving security within safety-sensitive fields such as food supply chains. Traceability is a fundamental tool for increasing transparency and ensuring excellence and safety in food [7]. The driving forces

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

This work is licensed under a Creative Commons Attribution 4.0 License. For more information, see https://creativecommons.org/licenses/by/4.0/

behind this evolution are the end consumers. Currently, consumers put high pressure on the supply chains to provide more transparency and grant access to detailed data on the production and distribution of their products. The concept of sustainability creates another crucial set of standards represented by various certifications, including Fairtrade, Organic, Bio, and so forth. This is yet another example of how consumers strive to understand and acknowledge the entire life cycle of food products to make conscientious decisions on their consumption and purchasing behaviors [8]. Certain areas of the world emphasize traceability as a cornerstone of their whole food safety policies and standards. For example, in 2002, the European Union made traceability tools mandatory for all businesses related to food and feed products within the union [9].

The traceability of a supply chain remains critical for numerous reasons. The first and potentially most crucial motivation behind this situation is the demand for the highest possible quality and safety within the food supply chain [10]. For instance, traceable food products are much easier to locate in case of recalls, and traceability can, at the same time, increase the optimization and control over various processes, including the production phase. The advantages of traceability within the food supply chain fall into different categories:

1) Reduced expenses on recalls
2) Market advantages
3) Minimization of lawsuits and liability claims
4) Improvement of the entire process [11]

Establishing efficient mechanisms of traceability means brands secure their reputation and obtain the opportunity to demonstrate their care and reliability to customers. Furthermore, traceability can promote trust and foster long-lasting relationships between the partners involved in the supply chain [12].

However, supply chains face other issues and challenges besides the traceability of the products. Such concerns include accessibility and validation of data, security issues, and challenges related to privacy [13]. Consequently, numerous frameworks have proposed the Blockchain mechanism – a distributed Ledger Technology [5], [14], [15] which can address these problems by connecting fragmented and isolated events within the supply chain events in a fixed trail for audit. However, blockchain technology encounters its own challenges, such as problematic scalability, the incapacity to reach the data offline, and the threat of possible attacks. Expensive fees associated with transactions represent yet another driving force behind the urge to find a solution and overcome the weaknesses of the blockchain scheme.

In this work, the authors proposed ProChain, a provenance-aware framework of traceability for IoT-based systems of the supply chain. The authors projected a new tool to monitor the items within the supply chain system according to their provenances to create a comprehensive line of information (origin, production, modifications, the process of custody, and so forth.). The ProChain framework uses the IOTA protocol, a third-generation DLT. It utilizes the Directed Acyclic Graph (DAG) structure of information instead of the linear structure used by the blockchain to overcome obstacles and promote a quantum-resistant, scalable, and attack-proof solution for the systems based on IoT [16].

The most integral contributions of our proposed framework include:

1) The proposed ProChain framework is a provenance-aware scheme of traceability designed for supply chain systems based on IoT. ProChain provides smooth traceability of food items from production to retailer with the assistance of multiple IoT sensors and provenance information at each involved process within the supply chain. ProChain also works as a guarantee of food quality and safety and increases and improves the control and optimization of all processes.
2) The ProChain concept was tested on the Raspberry Pi 3B platform by mimicking the IoT-deployed supply chain. Subsequently, the average measured time and consumed energy underwent an evaluation to review the practical efficiency of our framework.
3) A review and demonstration for the framework illustrates its usability within the supply chain systems relative to the pairing of supply chain information with the IOTA Tangle and creating provenance data by attaching information for different payload sizes.

The remaining sections of this paper proceed as follows: Section II provides a background of the work. Section III covers related works. Section IV describes the proposed IoT-based framework. Section V discusses the implementation and evaluation of the proposed framework. Section VI provides a discussion, and Section VII concludes the paper.

II. BACKGROUND

A. LEVERAGING DIGITAL INNOVATIONS FOR THE SUPPLY CHAIN SYSTEMS

Under the influence of worldwide globalization, contemporary supply chains comprise millions of global suppliers and contributors. Under these circumstances and facing considerable pressure, the networks have shown their weaknesses and limitations that, in turn, emphasize the demand for solutions that would reduce these issues, at least digitally [17]. For instance, ensuring complete transparency across the chain and real-time tracking of the assets would make it possible to avoid many of the current risks within the supply chain systems. Consequently, numerous disruptions could be prevented, significant losses diminished, and costs cut for many involved parties [18]. Moreover, there remains the possibility of calculating complex and accurate demand predictions for particular products. However, these forecast models would require the involvement and consideration of numerous other variables, which creates more space for mistakes due to the omission of various factors or undermining their importance [19]. Regardless, a suitable set of tools and access to the correct data would increase the accuracy of predictions and forecast models.

When the number of involved parties within the supply chain increases, their interconnection should also increase. Otherwise, the potential of the entire globalized marketplace remains at risk, the lead times increase dramatically, and the ability of the system to react and respond to any changes and adjustments becomes inadequate [20]. Such circumstances could also negatively impact the optimization of inventories by creating imbalance and complicating the process of proper price establishment that would meet demand. Automatically, these issues would also shift to the warehouse managing systems and entities, including the inventory and transportation logistics of the supply chain. Once the delivery times of crucial materials and components within the network become unclear, the risks of slowdowns and shortages in the production increase dramatically, resulting in lost time for all the involved stakeholders [21]. Digitalization, on the other hand, changes the way companies organize and arrange their supply chains and standard logistics operations, adjusting them to the required workloads and tempos. The evolution of the digital processes and the fourth industrial revolution gave birth to a whole new economic system [22]. Additionally, modern customers also ask for progressive, diversified, and ecologic products, which not only creates various new challenges but also produces opportunities to discover innovative solutions and processes that increase the efficiency and performance of the whole system. If we look at this development closely, we can identify these three reasons behind it:

1) The market is now heavily influenced by the rapid growth of worldwide trade, which stems from globalization, an ongoing process that has affected world trade for the last 50 years. This growth supplies the market with ever-increasing volumes of circulating products, which puts pressure on the industry to increase its efficiency when moving the products along the chain towards the end customers.
2) The substantial development and spread of mechanization and automatization mean there are more automated warehouses in operation across the planet.
3) Rapid growth and the ongoing modernization of e-commerce and various channels of digital distribution boost the entire sector and transform the physical warehouses into hotspots where material supplies satisfy virtual demands. The distribution points and sale centers can, in fact, exchange data and information directly, as the pull system shows increasing efficiency in responding rapidly to the customers' requests and demands. With the quick sharing of information, even the demands on aesthetics and visual appearance increase, forcing the involved parties to maintain the highest standards.

This inevitable development ultimately resulted in the birth of the so-called Industry 4.0, a new industrial revolution that provides smart, self-sufficient, and interconnected solutions. The digital transformation enables companies to trace the whole supply chain live, in real-time, so that they can, for instance, always track the current status of a particular product (e.g., in stock, ordered, or in transit) [23]. Modern tools allow the involved parties to locate the goods simply by collating status updates from partners within the supply chain and data from IoT devices.

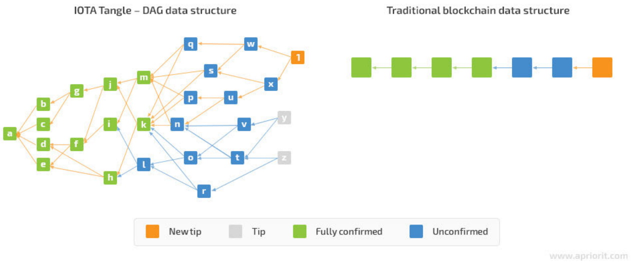

FIGURE 1. IOTA Tangle versus traditional blockchain.

B. IOTA: COMPOSING THE STORY OF THE PRODUCT

IOTA refers to the newest distributed ledger technology that should provide increased scalability and speed, the two qualities most current blockchain systems desperately lack [16]. At the core of IOTA is the Tangle, an original new technology that replaces the standard linear structure of data within the blockchains. The Tangle uses DAGs to apply a distinctively innovative approach to the formation of blockchain ledgers. This new data structure also allows the IOTA processes to work more effectively in comparison to the standard mechanisms within the blockchains [24].

IOTA avoids the standard method of placing blocks one immediately after the other seen in many blockchain systems. Instead, each of the blocks references the closest two blocks in front of it. Logically, the final structure of the network no longer mimics a chain, which now appears more like a tree or a Tangle instead. For a better visual understanding of the differences between a standard blockchain and the IOTA structure, see Figure 1. Achieving the consensus within a Tangle network requires checking whether the transactions are reachable in the DAGs from each open tip. To gain approval, each new transaction has to pick two tips; the network always has at least one tip.

The algorithm of the consensus applied by IOTA lets nodes freely pass their transactions onto the Tangle structure. Since the other nodes will not approve any invalid transactions, there exists no real risk of fraudulent activity. Most of the benefits associated with IOTA directly correspond to this innovative approach [16].

Reliable data should not solely result from provenance [25]. Proactively creating an efficient systematic story of the product based on the provenance information necessitates arranging the data in a product ledger that is immune to tampering and managed by IOTA 2.0. The data within the IOTA ledger are auditable to allow the identification of the parties responsible for the potential contamination of the data. This situation provides the trade flows with confidentiality, reasonable privacy, and constant access to reliable and tamper-proof data.

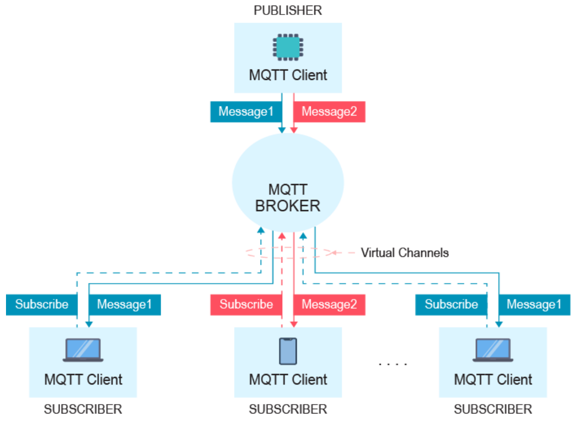

FIGURE 2. MQTT protocol model.

Therefore, collecting live provenance data (e.g., GPS location tracking, custody transfer, monitoring of the environment throughout storing and transportation with sensors for humidity and temperature, RFID tags, and so forth) can be a viable tool in the decision-making process and mitigation of risks.

C. MQTT PROTOCOL

In terms of messaging protocols, most of the IoT devices deploy the Message Queuing Telemetry Transport protocol (MQTT). This type of protocol is designed especially for IoT devices, taking into account the constraints these devices encounter, such as low bandwidth, which considerably complicates the adoption of HTTP protocol [26]. Unlike HTTP, MQTT represents lightweight protocols, cutting down the volume of messages and benefiting from its minimal requirements on the availability of connection. MQTT protocols tend to rely on TCP/IP. Nevertheless, some MQTT variants use Bluetooth or UDP instead [27]. MQTT protocols are officially standardized under ISO/IEC 20922:2016, and its sessions comprise four distinctive phases: (1) connecting, (2) authenticating, (3) communicating, and (4) terminating the connection. The protocol recognizes numerous kinds of messages. The most integral ones are "connect", "publish", "subscribe", and "disconnect".

MQTT architecture recognizes three primary roles of entities: (1) the broker, (2) the publisher, and (3) the subscriber. The server works as a broker, whereas all the involved subscribers and publishers are treated as clients. MQTT facilitates the transmission of data on a particular topic between the publishers and subscribers. All the information is neatly organized into different topics in hierarchical order. To register in the broker, subscribers and publishers pick one or several of these topics.

Figure 2 presents the standard architecture model of MQTT. Initially, the client connects to the broker using TCP/IP. Subsequently, the client will move to the stage of authentication. However, despite its numerous benefits and strengths, MQTT does not place much emphasis on security. Several aspects affecting its security influence MQTT solutions developers, which provides for many vulnerable points – including the MQTT protocol authentication procedure, which is comparatively thin.

To authenticate the username and password, MQTT passes this information to the broker in the "connect" message fields as plain text without any encryption or additional authentication requirements. MQTT does not require any particular security measures and leaves this matter to the designer of the application. Nevertheless, traditional mechanisms, such as transport security (SSL/TLS), can be combined at the cost of the increased weight of the protocol. According to [5], OTP authentication is a practical mechanism for preventing unauthorized access and inappropriate use of the device.

III. LITERATURE REVIEW

Production, packaging, transportation, distribution, consumption, and disposal are examples of the numerous processes involved in the worldwide food supply chain. Improving the safety, effectiveness, and economic benefits of each of these stages and processes constitutes an increasingly integral topic that draws the attention of numerous researchers and studies. For instance, Thakur and Hurburgh [28] address the need to make the upstream/downstream food supply chain activities management more transparent by proposing a system for the traceability of bulk grain within the supply chain. These authors deployed the Relational Database Management System (RDBMS) to store information in the scope of internal traceability. The authors also used the Extensible Markup Language (XML) for the data exchange between the involved parties as a part of the supply chain traceability. Kong *et al.* [29] focused on resolving issues relating to the safety and quality of food by suggesting the system of quality traceability specifically designed for bee products. Similarly, Storøy *et al.* [30] proposed the TraceFood Framework to manage the exchange of data. The system is based on sector-specific ontologies and TraceCore XML, and the entire framework comprises principles applied for identifying food products, various suggestions for "Good Traceability Practice", a universal standard for electronic data interchange (TraceCore XML), and the aforementioned sector-specific ontologies. To monitor and trace batches and units of food products across the supply chain, Bechini and Cimino (2008) created a traceability-focused web data system prototype.

The traceability in the supply chain systems has garnered significant attention in recent years - especially in the sectors where safety plays a crucial role, such as the food industry [31], pharmaceuticals [32], and perishable agricultural products [33], [34]. Researchers and authors found particular success in developing comprehensive traceability systems for monitoring, recording, and identifying critical food products, including meat [35], dairy products [36], and seafood [37]. Nevertheless, interesting SC mechanisms for traceability also focus on non-perishable goods, including textile products (especially clothing) [38] or electronics [39]. The rapid spread of RFID and IoT technologies reshapes contemporary supply chain systems, and it particularly impacts approaches towards traceability [40], [41]. For instance, IoT systems help

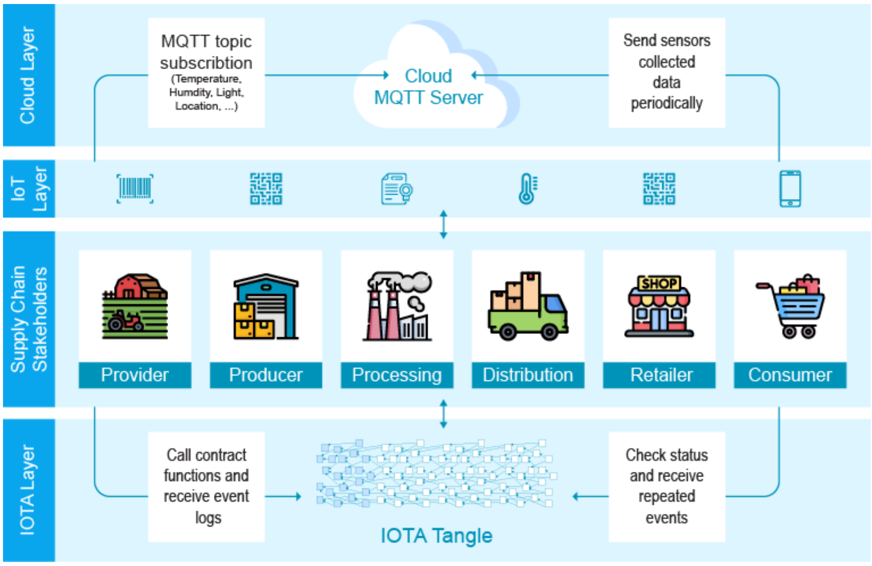
Cloud Layer
MQTT topic subscribtion (Temperature, Humdity, Light, Location, ...)
Cloud MQTT Server
Send sensors collected data periodically
IoT Layer
Supply Chain Stakeholders
Provider
Producer
Processing
Distribution
SHOP
Retailer
Consumer
IOTA Layer
Call contract functions and receive event logs
IOTA Tangle
Check status and receive repeated events

FIGURE 3. Overall system overview.

monitor products and track the conditions of their storage and transport, including the ambient temperature and humidity [42]. IoT tools can also assist with the identification of counterfeits and the provenance of SC [43].

The literature that focuses on blockchain-based traceability primarily centers around the food supply chain. For example, the authors of [44] created an original framework for agricultural traceability that deploys blockchain mechanisms, smart contracts, and coordination systems that manage the food tracking within the agricultural supply chain. The authors of [45] suggest a strategy of vendor-managed inventory based on the principles of blockchain, providing practical implementation of the food SC scenario. [46] proposes a system of food traceability built around the integration of IoT technology and blockchain mechanisms. The authors of [47] present a decentralized ''from-farm-to-fork'' traceability system for the sector of agricultural food products, using both blockchain mechanisms and IoT. Finally, [48] uses blockchain principles within the food supply chain to enable traceability and collect accurate data on the product's origins in order to allow end customers to make well-informed choices and purchases.

The possibilities and implications of using IoT devices within this sector have also undergone exploration by numerous studies and authors in the literature. Some of these works focus on the integration and use of QR codes and RFID to provide better traceability of food and increase product safety through SC management [49]–[51]. The technology of QR codes is considered highly convenient in the food supply chain thanks to its fast and smooth readability, huge storage capacity, and the low costs of its practical application. For instance, Qiao *et al.* [52] suggest a traceability system for the safety of vegetables that combines two-dimensional barcodes with web service technologies. To monitor and trace products within the farm food supply chain, Gao [53] explores the applicability of QR codes in this specific type of environment and creates an original code-based logistics data system. This system applies QR codes to facilitate the exchange of traceable data within the vegetable supply chain, covering all necessary processes from planting to packaging to distribution and retail.

Despite these valuable efforts and innovative proposals, the supply chain systems still await the development of universally effective tracing systems and tools. The demand for an economical and practical solution to the realization of tracking individual items in the IoT-based systems remains high, especially in the food supply chain sector.

IV. PROPOSED IOTA-BASED FRAMEWORK

A. SYSTEM OVERVIEW

Figure 3 depicts the overview of the proposed ProChain framework, while Figure 4 represents the data flow between different system components during the experimental simulation. To improve the essential flow of data across the network, we suggest using IoT-enabled XDK2MAM sensors with smart functionality. These devices will track the quality and state of the monitored products. The most vulnerable data we obtain will be safely stored in IOTA, whereas smart contracts automatize the process, initiate events, and manage the implementation of rules and conditions by each of the parties involved.

The primary stakeholders in the network, as Figure 3 shows, are the providers of raw products, organizations handling and processing these products, distributors of the products, retailers, and the end consumers. Initially, the administration created a contract inside the IOTA system. Subsequently, the mechanism of subscriptions to individual topics occurs across the whole storage and logistic chain.

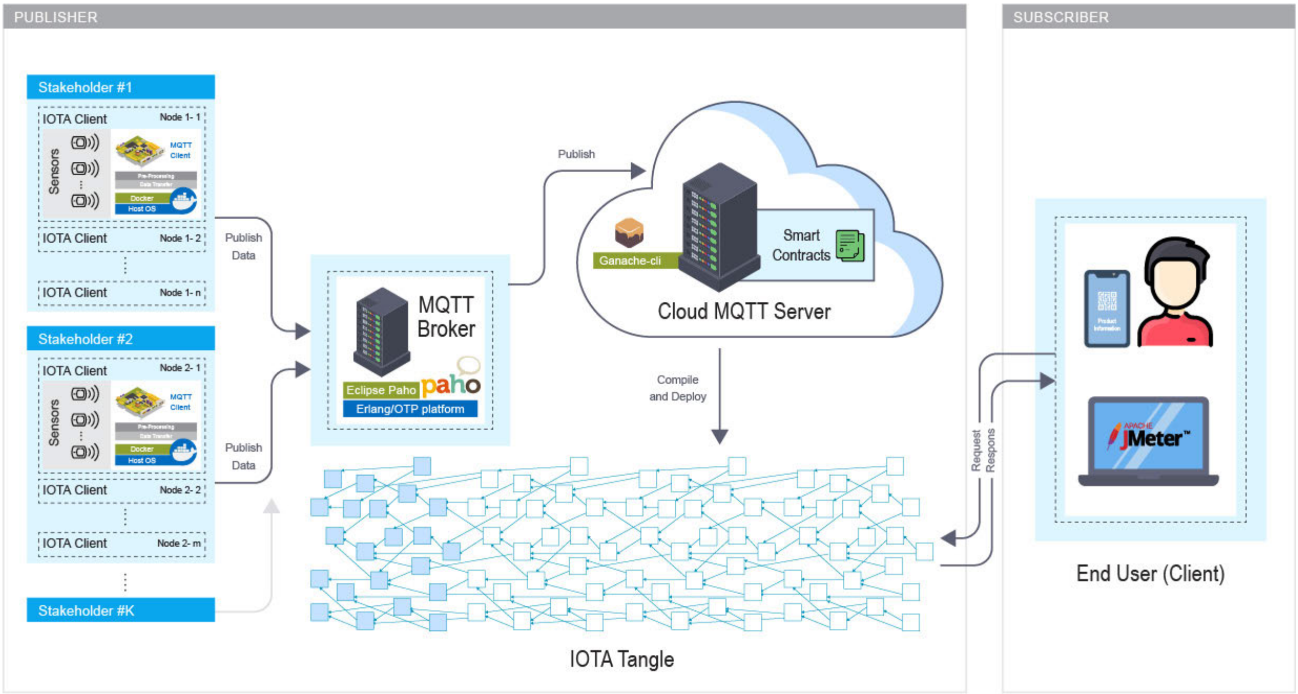

FIGURE 4. System components and data flow.

At this stage, IoT sensors connect to the network's server. Next, IoT sensors start to collect data and pass them to MQTT for storage. Some specific information will also remain stored in IOTA. Smart contracts periodically check the quality, traceability, and security of the system.

Stakeholders assign to the MQTT cloud-based storage by generating a publish/subscribe system based on the topics. Unlike the regular HTTP network, MQTT does not depend on the establishment of a new connection whenever the server receives a request [54]. Given that this system is based on subscriptions, the only element it requires is a single appropriate subscription to a topic created within the server.

Another difference between MQTT and HTTP protocols is that MQTT operates significantly faster in terms of the collection of the data provided by IoT sensors. The MQTT protocol is also preferred as a more lightweight solution in comparison to HTTP [55]. While most information is stored and accessed through MQTT servers, only IOTA can handle sophisticated and vulnerable data. The MQTT protocol assists with the storage, sharing, and publishing of the data that allows the information to be gathered across the whole network by all the involved parties.

B. ACTORS

Since the stakeholders are heterogeneous, creating a reliable, verifiable, and stable system can prove problematic. To overcome such issues and prevent various threats, our framework proposes the use of multiple mechanisms and resources to establish safe connections between the involved stakeholders. First, it is crucial to understand the unique characteristics of the involved stakeholders and their specific roles.

- Owner of the contract: This stakeholder has superior authority over the entire system. Such a person's role includes deploying the contract and monitoring the implementation of the rules and regulations.
- Producer: This stakeholder takes primary responsibility for storing the raw products. Agricultural products sensitive to direct sun exposure or shifts in temperature (e.g., seeds) are deposited on a medium or large scale in storehouses for a similarly long time.
- Processing stage organization: This phase primarily focuses on collecting large volumes of raw products and other necessary agricultural items (e.g., fertilizers) before selling them to the producers.
- Producers: In this context, our primary level producers are the farmers. They take responsibility for all the duties around planting and production of raw products.
- Distributors: Distribution primarily involves secure transportation of the products between various places.
- Retailers: The producer sells his products to the retailer who subsequently resells the items in small quantities on an open market to the end consumers.
- Wholesalers: These actors buy agricultural products and crops in large quantities to resell them to the retailers.
- Consumers: End consumers depend on purchasing agricultural products from retailers. They play a crucial role in the whole system since they are the ones who create the demand.

The primary goal of our framework is to create a system that would allow and encourage its stakeholders to exchange data in a manner that improves and facilitates the traceability of all

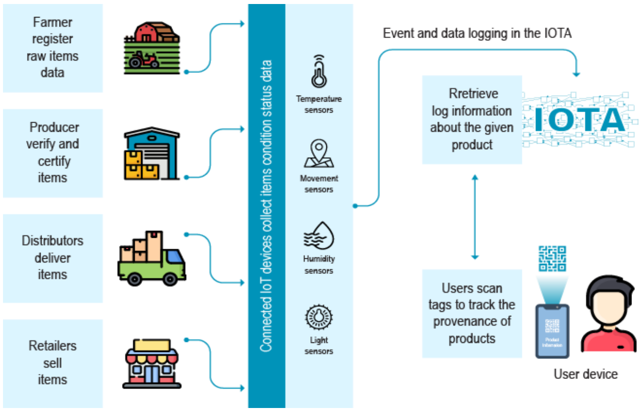
Farmer register raw items data
Producer verify and certify items
Distributors deliver items
Retailers sell items
Connected IoT devices collect items condition status data
Temperature sensors
Movement sensors
Humidity sensors
Light sensors
Event and data logging in the IOTA
Rretrieve log information about the given product
IOTA
Users scan tags to track the provenance of products
User device

FIGURE 5. System interactions with IOTA.

the items involved. To implement all the requirements of the system (e.g., accessibility, stability, immutability, security, automation, and elimination of third-party intermediates), the following components will be deployed:

C. IOTA

IOTA helps maintain the system's authenticity and reliability. Although most of the collected data within our system are stored and handled by MQTT, this protocol is not entirely secure since it does not execute or require any encryption of the stored data [56]. Since our goal is to improve the transparency and reliability of the collected data on the monitored agricultural items, it remains critical to ensure that the stored data will remain tamper-proof. In this specific regard, IOTA can be highly beneficial. Figure 5 depicts the interaction between the system and IOTA.

The central processes within the system trigger other events; the resulting data is recorded in the blockchain's transaction logs. These data are immutable since any attempt to tamper with them would break the entire nodes. This way, the collected traceable information in blockchain remains secure.

D. SMART CONTRACTS

These contracts automate the entire process and eliminate the need to deploy third-party intermediates by combining various roles, properties, conditioners, and events. In this context, properties stand for storage variables, role (or function) represents the performance of a set task, the event stands for the incidence of particular statements, and the conditioner (or modifier) is the authority of each actor. The system works with two specific smart contracts at its core: one focuses on storage, whereas the other is designed for the distribution process. Both were programmed using Solidity language and work on the basis of the Ethereum blockchain platform. Solidity allows the programming of smart contracts using complex, branched, and looped code instructions. Therefore, it is possible to create structures of any type and customize them in various ways. In our framework, we deployed the smart contacts in the cloud server to enhance the interchange of transactions and messages between different system components and the IOTA network.

E. IoT-ENABLED ENVIRONMENT

The deployed IoT devices, comprising primarily low-power sensors, will track the environment in real-time by the deployed IoT devices. The devices will interact with MQTT servers to provide live data on the environment surrounding the monitored products. Figures 3 and 4 demonstrate this interaction and show how the published data is sent or directed to the users of the system.

F. MQTT PROTOCOL

Our framework proposes the MQTT protocol to create and encourage collaboration between the IoT sensors, the actors of the system, and the whole blockchain structure. This network protocol requires only limited bandwidth, and it does not demand significant amounts of memory. This protocol also enables sharing of all the data collected by the sensors (e.g., humidity, temperature, exposure to light, and so forth) among all users of the whole system. MQTT works based on a subscription/publish mechanism, which means that the server stores topics requiring subscription by the clients if they wish to evaluate or publish data under the relevant topic.

V. EVALUATION OF THE IMPLEMENTATION AND PERFORMANCE OF THE SYSTEM

The following section further discusses implementing the suggested system, which is explained in Section IV. This section also describes the conducted experiments and simulations, as well as carrying out a practical evaluation of the performance of this implemented provenance-based system. However, in order to find out whether this system can comply with the demands and requirements of real-world usage, we must evaluate both its performance and the overhead costs of the IoT sensor interaction. The subsequent subsections describe all the details on the implementation of the system, completed experiments, metrics and data collection, and the evaluation of the system's performance.

A. PROTOTYPE OF IMPLEMENTATION

Our suggested system was implemented using Eclipse Paho[1] in combination with Python language, a simple yet efficient and reliable open-source IoT software programming language created by Eclipse Foundation. To implement this prototypal system and simplify its fast development, a preexisting package library has been adopted which contains both the Eclipse Paho server implementation and an MQTT protocol client.

B. SETUP FOR OUR EXPERIMENT

Table 1 depicts our experimental setup. The use of virtualization technology (Docker) helped simplify the

[1] https://www.eclipse.org/paho/

TABLE 1. Simulation environment.

Element	Value
Sensors	XDK2MAM
CPU max speed	3.40 GHz
CPU architecture	Core(TM) i7-3770
Memory	16 GB
OS	Ubuntu 16.04 LTS
Storage	1 TB

process [57]. This technology makes building and maintaining Virtual Machine (VM) containers more straightforward. That, in turn, conveniently facilitates running node clusters in the architecture [58]. The MQTT protocol provides a connection between the IoT devices and the IOTA network. To simulate the client's behavior authentically, the Ethereum's ganache-cli[2] client is used, which further simplifies the testing and deployment. To accommodate the virtual chain structure introduced in our architecture required making adjustments on the client. For example, we have implemented the technology of virtual chains in the client by porting the block stack open-source library from GitHub. Such a modified client allows the nodes to hold two chains simultaneously: the chain of genuine transactions and the virtual chain recorded in the network.

C. COLLECTION OF DATA

The following section describes in detail how we performed the experiment from the initial setup to the generation, collection, and aggregation of data. The authors conducted a simulation for the experiments to provide a practical example of the system's usability and efficiency in the real world: more precisely, in the IoT environment. For this purpose, Apache JMeter is used. Apache JMeter is an open-source software created to load and test the functions, behavior, and performance of the system using the client machine, an iMac. To ensure that the Apache Jmeter will support MQTT, a third-party library measures the performance. A dataset of different sizes of payloads has been selected as follows: 8/16/32/64/128/256/512 and 1024. The chosen range mimicked the type and volume of data realistically transmissible through the tiny IoT sensors. It was also based on the range of sizes currently enabled by MQTT, oriented toward smaller devices. The payload also illustrates a characteristic URI naming strategy which can help identify any IoT device within the system. We ran and repeated the application 20 times on the client with every considered size of the payload, resulting in the collection of significant volumes of data based on the payload sizes. Various actors affected this experiment, including the connectivity of the network, the amount of deployed devices, and the time required to input data to the database. We selected the metric data of a performance highlighted in the following sub-section.

To provide all simultaneous users with MQTT requests, we have chosen the throughput, the time required to respond, and amount of the users from 1/10/20/40 and 80. We collected these data in .csv form and saved them in a log file. The data collected in regard to the time of response and throughput were counted together and then averaged. We have also tested the effective scalability of our system using a varying number (20/40/60/80 and 100) of users to ensure that the system can support numerous users simultaneously.

D. PERFORMANCE METRICS

To simulate the performance of our system authentically in the real-life environment with all its typical constraints, we used different performance metrics, such as the time of response, the number of users connected to the system simultaneously, the throughput, and variable payload sizes. The considered metrics used for our evaluation are as follows:

- Response time: This metric considers the real-time required by a portable client device to transmit MQTT message towards the agent, then between the agent and the server, and the other way around, including the time it takes to log the data to the database in the network. The time is indicated in *ms* (milliseconds).
- Throughput: This refers to the overall volumes of MQTT information transmitted across the network in a second. This metric is indicated in *KB/S* (KiloBytes per second). Alternatively, throughput can be measured in transactions per second.
- Size of the payload: This metric measures the amount of MQTT data transmitted along with the request. It is indicated in bytes.
- User numbers: This indicates how many users concurrently use the system and send their requests across the network. This aspect also further implicates the system's realistic scalability.

E. PERFORMANCE EVALUATION

This section summarizes and analyzes the performance of our system based on the information gathered in the course of the experiment. To perfectly understand how the system acts and performs, we have decided to divide the evaluation into two stages: our system underwent individual assessment in both local and cloud environments. These are the metrics used when assessing the system:

- Time of response (indicated in milliseconds)
- Throughput (how many transactions per second)

First, we assessed the system in the local environment with payloads of 16/32/64/128/256/512 and 1024 bytes using the data we gathered in sec. 5.2.2. Their corresponding time of response was arranged as illustrated in Figure 6. This scheme considers a single user who sent his repeated request 20 times. For each of the considered payload sizes, the time of response was subsequently calculated by dividing the average response times by the number of repetitions. This evaluation showed that the payloads from 8 to 64 bytes sustain a stable slope of response times. Nevertheless, when we reached

[2] https://github.com/trufflesuite/ganache-cli

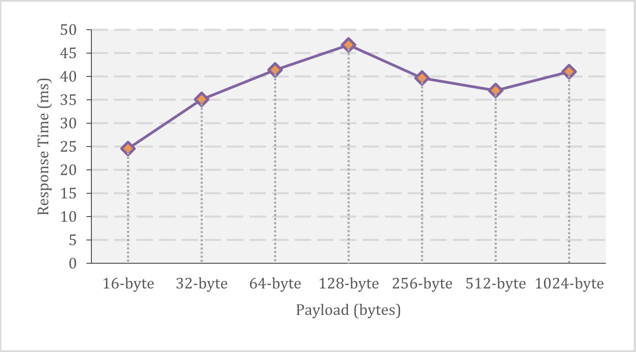

FIGURE 6. Evaluation of response times versus payload based on a single local user environment.

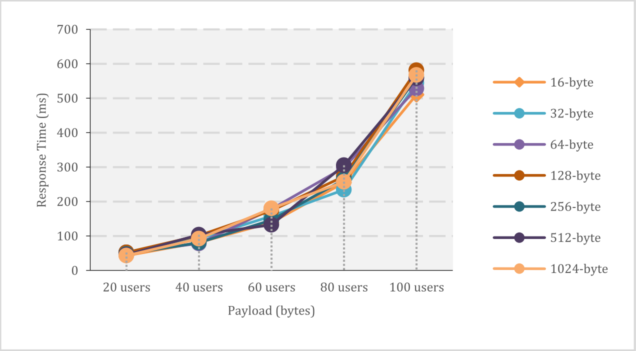

FIGURE 7. Evaluation of response times with various users' count payload on the local environment.

a 128-bytes payload, the time dropped and maintained its level up to 1024 bytes.

Afterward, to evaluate the average times for the different payloads in combination with various numbers of simultaneous users, we created a graph based on the gathered and calculated data. Figure 7 depicts this graph, where the *x-axis* stands for the number of users (20/40/60/80/100) and the *y-axis* stands for the time of response.

The graph shows that between 10 and 60 concurrent users, the response time increases continuously in linear slope, but for 100 users, the response time suddenly increases approximately 2.5 times. Next, we evaluated the performance of our system in the cloud environment. Similar to the previous evaluation, we considered payloads ranging from 16 to 1024 bytes and collected the data on their respective response times. These data were used in the graph depicted in Figure 8, which considers a single user who made 20 requests consecutively.

In Figure 9, we tested the response time and found it stays steadily between 330 and 350ms with payloads between 16 and 256 bytes. However, once we reach and exceed 256 bytes, the response times visibly increase. In comparison with our evaluation in the local environment, we have witnessed approximately ten times longer response times caused by long-distance communication over the shared network and server configuration in the cloud.

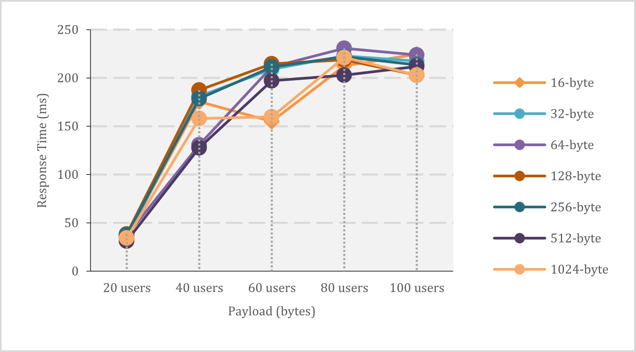

FIGURE 8. Evaluation of response times versus payload based on the cloud environment.

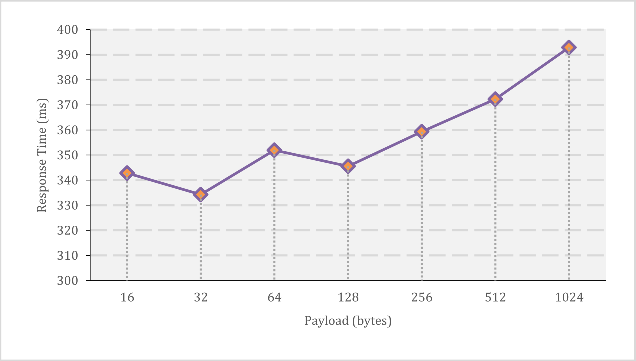

FIGURE 9. Evaluation of system scalability based on the transaction count per second in the local user environment.

Figure 10 shows a graph where x stands for the number of concurrent users (20/40/60/80/100) and y stands for the response time. According to the findings, increasing the number of users also increases the time the system needs to respond to their requests. This situation is particularly apparent from 60 users upwards. In comparison to the local environment, we see increased response time due to the interactions between the network, the cloud, and the Internet.

Network delays may rank among the factors that affect the response times of our system the most. Moreover, the resource allocation may also encounter limitations due to the controlled environments surrounding the shared virtual resources. We have also noticed that whenever the payload increases, the time of response will also rise.

Figure 11 contains a graph where x stands for the number of users (from 20 to 100), and y represents the throughput value (indicated in transactions per second). When comparing these graphs, we noticed that the substantially increased response times meant the throughput (number of transactions handled per second) visibly drops when the system is used by at least 100 users simultaneously.

VI. DISCUSSION

After considering and analyzing these factors and the requirements related to an application for tracing products in the supply chain system, the solution adopted in ProChain is

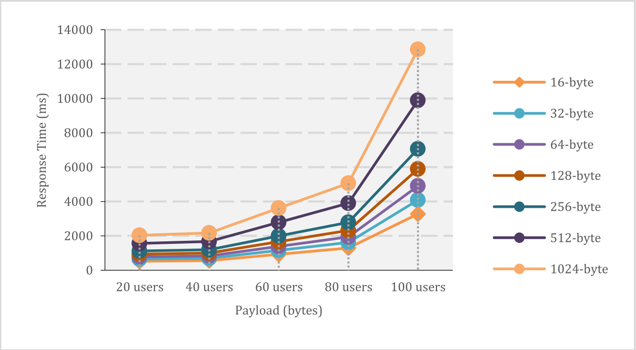

FIGURE 10. Evaluation of response times with various users' count payload on the cloud environment.

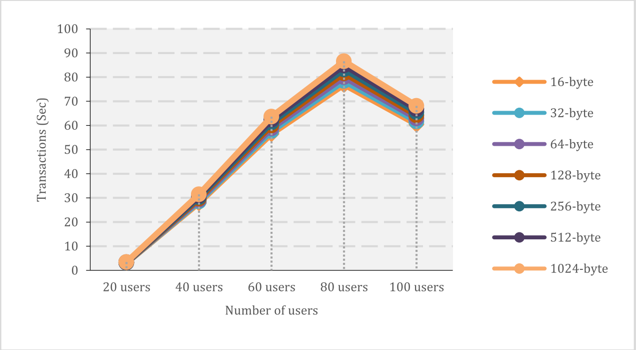

FIGURE 11. Evaluation of transactions per second with various users' count payload on the local environment.

based on IOTA. IOTA is a scalable DLT designed to support the transfer of data and value quickly and efficiently. It must be emphasized that in this solution, the transactions are not structured in blocks but connected individually to each other to form a network called the Tangle rather than a chain. From the experimental results presented in the previous section, the framework demonstrates excellent performance in terms of the scalability, throughput, and latency. Furthermore, the open structure of the Tangle is precisely the characteristic that allows it to record such high performances.

The proposed framework provides the following advantages:

- Authenticity: Each node can prove that it has sent data and / or that it possesses IOTA tokens. Each node of an IOTA network validates transactions and then sends them to other nodes that do the same. Consequently, valid transactions are agreed upon by all nodes, eliminating the requirement to rely on only one node in the network.
- Integrity: Each node can prove that the data has not changed. All transactions in the Tangle are immutable and transparent. Each transaction references the hashes of two others that precede it. Thus, changing the content of any transaction would invalidate the hashes, in turn making the transactions invalid.
- Confidentiality: Each user can control who accesses the data through encryption. IOTA uses single-use signatures to prevent attackers from stealing IOTA tokens. IOTA networks are peer-to-peer networks in which no central authority controls the Tangle. Conversely, all nodes can own a copy and reach a consensus on its content.
- Micropayments: It is possible to send small amounts of IOTA tokens without paying any fees. IOTA is free, meaning there is no need to pay for a subscription or sign any contracts. Transactions are also feeless. Users can store data in the Tangle without restrictions. All that is required is a node to receive the transactions. For each transaction attached to the Tangle, two previous transactions are validated. This process makes the structure scalable because more new purchases lead to faster validations and greater network security.

Although blockchains and the Tangle both fall into the DLT category, with two principal differences: firstly, the Tangle has no transaction costs. Secondly, IOTA networks have no miners.

VII. CONCLUSION

Our proposed framework, ProChain, relies on the IOTA Tangle network, which serves as its tailbone, whereas IoT sensors collect data in the field. To achieve the utmost transparency of the data shared among the participating parties, we use DLT IOTA-distributed ledger technology, which bears an association with other notable benefits, including scalability, low costs, and quantum resilience. All these advantages make the DLT-based solution a favorable candidate for integration in the IoT-based supply chain networks. To further validate the practical efficacy of our framework, we have evaluated its performance and measured the response time, payload, and throughput values in various situations. Moreover, we have also simulated ProChain in a real-life setting using the Raspberry PI 3B IoT platform, testing its performance by attaching and retrieving collected sensor data and provenance data at various time intervals. Our research has demonstrated the advantages of using IOTA-based solutions in the field of food supply chains. These benefits include tractability, transparency, and robust security. We have also highlighted the characteristics and strengths of the mechanisms deployed in the collaboration between supply chains and IoT devices. Experimental simulations show that the payload affects the response time for both environments (i.e., the local and the cloud). We have shown that whenever the payload increases, the time of response will also rise. Compared with the local environment, we have witnessed response times approximately ten times longer in the cloud environment. Such a situation is typical as it results from long-distance communication over the shared network and server configuration.

As a future work, more studies require deploying the proposed framework on a real case of a complete supply chain system. It is critical to test ProChain on infrastructures which may have different sensor types, different supply chain units, and different applications. More experimentation on the power and computation capacity is required, as numerous IoT applications are deployed on devices that run on limited power and computation resources.

REFERENCES

[1] F. Piccialli, N. Bessis, and E. Cambria, "Industrial Internet of Things (IIoT): Where we are and what's next," *IEEE Trans. Ind. Informat.*, vol. 17, no. 1, pp. 7700–7703, Nov. 2021.

[2] W. Ejaz, M. Naeem, and S. Zeadally, "On-demand sensing and wireless power transfer for self-sustainable industrial Internet of Things networks," *IEEE Trans. Ind. Informat.*, vol. 17, no. 10, pp. 7075–7084, Oct. 2021.

[3] Y. Liu, X. Ma, L. Shu, G. P. Hancke, and A. M. Abu-Mahfouz, "From industry 4.0 to agriculture 4.0: Current status, enabling technologies, and research challenges," *IEEE Trans. Ind. Informat.*, vol. 17, no. 6, pp. 4322–4334, Jun. 2021.

[4] Y. Dong, Z. Fu, S. Stankovski, S. Wang, and X. Li, "Nutritional quality and safety traceability system for China's leafy vegetable supply chain based on fault tree analysis and QR code," *IEEE Access*, vol. 8, pp. 161261–161275, 2020.

[5] Z. Wang, T. Wang, H. Hu, J. Gong, X. Ren, and Q. Xiao, "Blockchain-based framework for improving supply chain traceability and information sharing in precast construction," *Autom. Construct.*, vol. 111, Mar. 2020, Art. no. 103063.

[6] J. Qian, B. Dai, B. Wang, Y. Zha, and Q. Song, "Traceability in food processing: Problems, methods, and performance evaluations—A review," *Crit. Rev. Food Sci. Nutrition*, vol. 2020, pp. 1–14, Oct. 2020.

[7] J. Sunny, N. Undralla, and V. Madhusudanan Pillai, "Supply chain transparency through blockchain-based traceability: An overview with demonstration," *Comput. Ind. Eng.*, vol. 150, Dec. 2020, Art. no. 106895.

[8] L. Macchion, A. Moretto, F. Caniato, P. Danese, and A. Vinelli, "Static supply chain complexity and sustainability practices: A multitier examination," *Corporate Social Responsibility Environ. Manage.*, vol. 27, no. 6, pp. 2679–2691, Nov. 2020.

[9] J. Qian, L. Ruiz-Garcia, B. Fan, J. I. R. Villalba, U. McCarthy, B. Zhang, Q. Yu, and W. Wu, "Food traceability system from governmental, corporate, and consumer perspectives in the European union and China: A comparative review," *Trends Food Sci. Technol.*, vol. 99, pp. 402–412, May 2020.

[10] L. Manning, P. A. Luning, and C. A. Wallace, "The evolution and cultural framing of food safety management systems—Where from and where next?" *Comprehensive Rev. Food Sci. Food Saf.*, vol. 18, no. 6, pp. 1770–1792, Nov. 2019.

[11] T. K. Dasaklis, F. Casino, and C. Patsakis, "Defining granularity levels for supply chain traceability based on IoT and blockchain," in *Proc. Int. Conf. Omni-Layer Intell. Syst.*, May 2019, pp. 184–190.

[12] M. S. Memon, Y. H. Lee, and S. I. Mari, "Analysis of traceability optimization and Shareholder's profit for efficient supply chain operation under product recall crisis," *Math. Problems Eng.*, vol. 2015, pp. 1–8, Jan. 2015.

[13] M. S. Al-Rakhami and M. Al-Mashari, "A blockchain-based trust model for the Internet of Things supply chain management," *Sensors*, vol. 21, no. 5, p. 1759, Mar. 2021.

[14] F. Casino, V. Kanakaris, T. K. Dasaklis, S. Moschuris, S. Stachtiaris, M. Pagoni, and N. P. Rachaniotis, "Blockchain-based food supply chain traceability: A case study in the dairy sector," *Int. J. Prod. Res.*, vol. 59, no. 19, pp. 5758–5770, 2020.

[15] S. S. Kamble, A. Gunasekaran, and R. Sharma, "Modeling the blockchain enabled traceability in agriculture supply chain," *Int. J. Inf. Manage.*, vol. 52, Jun. 2020, Art. no. 101967.

[16] W. F. Silvano and R. Marcelino, "Iota tangle: A cryptocurrency to communicate Internet-of-Things data," *Future Gener. Comput. Syst.*, vol. 112, pp. 307–319, Nov. 2020.

[17] R. Raj, J. Wang, A. Nayak, M. K. Tiwari, B. Han, C. Liu, and W. Zhang, "Measuring the resilience of supply chain systems using a survival model," *IEEE Syst. J.*, vol. 9, no. 2, pp. 377–381, Jun. 2015.

[18] M. P. V. D. Oliveira and R. Handfield, "Analytical foundations for development of real-time supply chain capabilities," *Int. J. Prod. Res.*, vol. 57, no. 5, pp. 1571–1589, Mar. 2019.

[19] S. Makridakis, R. M. Hogarth, and A. Gaba, "Forecasting and uncertainty in the economic and business world," *Int. J. Forecasting*, vol. 25, no. 4, pp. 794–812, Oct. 2009.

[20] A. Qazi, A. Dickson, J. Quigley, and B. Gaudenzi, "Supply chain risk network management: A Bayesian belief network and expected utility based approach for managing supply chain risks," *Int. J. Prod. Econ.*, vol. 196, pp. 24–42, Feb. 2018.

[21] P. Dallasega, "Industry 4.0 fostering construction supply chain management: Lessons learned from engineer-to-order suppliers," *IEEE Eng. Manag. Rev.*, vol. 46, no. 3, pp. 49–55, Sep. 2018.

[22] D. Ivanov, A. Dolgui, and B. Sokolov, "The impact of digital technology and industry 4.0 on the ripple effect and supply chain risk analytics," *Int. J. Prod. Res.*, vol. 57, no. 3, pp. 829–846, Feb. 2019.

[23] A. Bougdira, I. Akharraz, and A. Ahaitouf, "A traceability proposal for industry 4.0," *J. Ambient Intell. Humanized Comput.*, vol. 11, no. 8, pp. 3355–3369, Aug. 2020.

[24] T. Alsboui, Y. Qin, R. Hill, and H. Al-Aqrabi, "Towards a scalable iota tangle-based distributed intelligence approach for the Internet of Things," in *Proc. Sci. Inf. Conf.*, 2020, pp. 487–501.

[25] S. Suhail, R. Hussain, A. Khan, and C. S. Hong, "Orchestrating product provenance story: When IOTA ecosystem meets electronics supply chain space," *Comput. Ind.*, vol. 123, Dec. 2020, Art. no. 103334.

[26] V. Gupta, S. Khera, and N. Turk, "MQTT protocol employing IoT based home safety system with ABE encryption," *Multimedia Tools Appl.*, vol. 80, no. 2, pp. 2931–2949, Jan. 2021.

[27] F. Buccafurri and C. Romolo, "A blockchain-based OTP-authentication scheme for constrainded IoT devices using MQTT," in *Proc. 3rd Int. Symp. Comput. Sci. Intell. Control*, Sep. 2019, pp. 1–5.

[28] M. Thakur and C. R. Hurburgh, "Framework for implementing traceability system in the bulk grain supply chain," *J. Food Eng.*, vol. 95, no. 2, pp. 617–626, 2009.

[29] Y. G. Kong, X. F. Hu, T. J. Chen, and Z. T. You, "Research and development of quality traceability system based on intelligent services for bee products," in *Applied Mechanics and Materials*. Switzerland: Trans Tech, 2013, pp. 694–699.

[30] J. Storøy, M. Thakur, and P. Olsen, "The TraceFood framework—Principles and guidelines for implementing traceability in food value chains," *J. Food Eng.*, vol. 115, no. 1, pp. 41–48, Mar. 2013.

[31] R. Badia-Melis, P. Mishra, and L. Ruiz-García, "Food traceability: New trends and recent advances. A review," *Food Control*, vol. 57, pp. 393–401, Nov. 2015.

[32] M. Solanki and C. Brewster, "OntoPedigree: Modelling pedigrees for traceability in supply chains," *Semantic Web*, vol. 7, no. 5, pp. 483–491, Jun. 2016.

[33] J. Hu, X. Zhang, L. M. Moga, and M. Neculita, "Modeling and implementation of the vegetable supply chain traceability system," *Food Control*, vol. 30, no. 1, pp. 341–353, Mar. 2013.

[34] X. Xiao, Q. He, Z. Li, A. O. Antoce, and X. Zhang, "Improving traceability and transparency of table grapes cold chain logistics by integrating WSN and correlation analysis," *Food Control*, vol. 73, pp. 1556–1563, Mar. 2017.

[35] A. Mousavi, M. Sarhadi, A. Lenk, and S. Fawcett, "Tracking and traceability in the meat processing industry: A solution," *Brit. Food J.*, vol. 104, no. 1, pp. 7–19, Feb. 2002.

[36] A. J. McHugh, C. Feehily, M. A. Fenelon, D. Gleeson, C. Hill, and P. D. Cotter, "Tracking the dairy microbiota from farm bulk tank to skimmed milk powder," *mSystems*, vol. 5, no. 2, Apr. 2020, Art. no. e00226.

[37] M. Bailey, S. R. Bush, A. Miller, and M. Kochen, "The role of traceability in transforming seafood governance in the global south," *Current Opinion Environ. Sustainability*, vol. 18, pp. 25–32, Feb. 2016.

[38] T. K. Agrawal, L. Koehl, and C. Campagne, "A secured tag for implementation of traceability in textile and clothing supply chain," *Int. J. Adv. Manuf. Technol.*, vol. 99, nos. 9–12, pp. 2563–2577, Dec. 2018.

[39] D. DiMase, Z. A. Collier, J. Carlson, R. B. Gray, and I. Linkov, "Traceability and risk analysis strategies for addressing counterfeit electronics in supply chains for complex systems," *Risk Anal.*, vol. 36, no. 10, pp. 1834–1843, Oct. 2016.

[40] R. Gautam, A. Singh, K. Karthik, S. Pandey, F. Scrimgeour, and M. K. Tiwari, "Traceability using RFID and its formulation for a kiwifruit supply chain," *Comput. Ind. Eng.*, vol. 103, pp. 46–58, Jan. 2017.

[41] G. Alfian, M. Syafrudin, U. Farooq, M. R. Ma'arif, M. A. Syaekhoni, N. L. Fitriyani, J. Lee, and J. Rhee, "Improving efficiency of RFID-based traceability system for perishable food by utilizing IoT sensors and machine learning model," *Food Control*, vol. 110, Apr. 2020, Art. no. 107016.

[42] Y. Li, Y. Peng, L. Zhang, J. Wei, and D. Li, "Quality monitoring traceability platform of agriculture products cold chain logistics based on the Internet of Things," *Chem. Eng. Trans.*, vol. 46, pp. 517–522, Dec. 2015.

[43] K. Yang, D. Forte, and M. M. Tehranipoor, "CDTA: A comprehensive solution for counterfeit detection, traceability, and authentication in the IoT supply chain," *ACM Trans. Des. Autom. Electron. Syst.*, vol. 22, no. 3, pp. 1–31, May 2017.

[44] R. Casado-Vara, J. Prieto, F. De la Prieta, and J. M. Corchado, "How blockchain improves the supply chain: Case study alimentary supply chain," *Proc. Comput. Sci.*, vol. 134, pp. 393–398, Aug. 2018.

[45] T. Dasaklis and F. Casino, "Improving vendor-managed inventory strategy based on Internet of Things (IoT) applications and blockchain technology," in *Proc. IEEE Int. Conf. Blockchain Cryptocurrency (ICBC)*, May 2019, pp. 50–55.

[46] F. Tian, "A supply chain traceability system for food safety based on HACCP, blockchain & Internet of Things," in *Proc. Int. Conf. Service Syst. Service Manage.*, Jun. 2017, pp. 1–6.

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

[48] R. Bettín-Díaz, A. E. Rojas, and C. Mejía-Moncayo, "Methodological approach to the definition of a blockchain system for the food industry supply chain traceability," in *Proc. Int. Conf. Comput. Sci. Appl.*, May 2018, pp. 19–33.

[49] Z. Li, G. Liu, L. Liu, X. Lai, and G. Xu, "IoT-based tracking and tracing platform for prepackaged food supply chain," *Ind. Manage. Data Syst.*, vol. 117, no. 9, pp. 1906–1916, Oct. 2017.

[50] B. Fan, J. Qian, X. Wu, X. Du, W. Li, Z. Ji, and X. Xin, "Improving continuous traceability of food stuff by using barcode-RFID bidirectional transformation equipment: Two field experiments," *Food Control*, vol. 98, pp. 449–456, Apr. 2019.

[51] A. Iftekhar, X. Cui, M. Hassan, and W. Afzal, "Application of blockchain and Internet of Things to ensure tamper-proof data availability for food safety," *J. Food Qual.*, vol. 2020, pp. 1–14, May 2020.

[52] S. Qiao, Z. Wei, and Y. Yang, "Research on vegetable supply chain traceability model based on two-dimensional barcode," in *Proc. 6th Int. Symp. Comput. Intell. Design*, Oct. 2013, pp. 317–320.

[53] H. M. Gao, "Study on the application of the QRcode technology in the farm product supply chain traceability system," in *Applied Mechanics and Materials*. Switzerland: Trans Tech, 2013, pp. 3056–3060.

[54] T. H. Pranto, A. A. Noman, A. Mahmud, and A. B. Haque, "Blockchain and smart contract for IoT enabled smart agriculture," *PeerJ Comput. Sci.*, vol. 7, p. e407, Mar. 2021.

[55] B. Wukkadada, K. Wankhede, R. Nambiar, and A. Nair, "Comparison with HTTP and MQTT in Internet of Things (IoT)," in *Proc. Int. Conf. Inventive Res. Comput. Appl. (ICIRCA)*, Jul. 2018, pp. 249–253.

[56] S. Andy, B. Rahardjo, and B. Hanindhito, "Attack scenarios and security analysis of MQTT communication protocol in IoT system," in *Proc. 4th Int. Conf. Electr. Eng., Comput. Sci. Informat. (EECSI)*, Sep. 2017, pp. 1–6.

[57] M. Al-Rakhami, M. Alsahli, M. M. Hassan, A. Alamri, A. Guerrieri, and G. Fortino, "Cost efficient edge intelligence framework using Docker containers," in *Proc. IEEE 16th Int. Conf. Dependable, Autonomic Secure Comput., 16th Intl Conf Pervasive Intell. Comput., 4th Intl Conf Big Data Intell. Comput. Cyber Sci. Technol. Congress(DASC/PiCom/DataCom/CyberSciTech)*, Aug. 2018, pp. 800–807.

[58] M. Al-Rakhami, A. Gumaei, M. Alsahli, M. M. Hassan, A. Alamri, A. Guerrieri, and G. Fortino, "A lightweight and cost effective edge intelligence architecture based on containerization technology," *World Wide Web*, vol. 23, pp. 1341–1360, Mar. 2020.

MABROOK S. AL-RAKHAMI (Member, IEEE) received the master's degree in information systems from King Saud University, Riyadh, Saudi Arabia, where he is currently pursuing the Ph.D. degree with the Information Systems Department, College of Computer and Information Sciences. He has worked as a Lecturer and taught many courses, such as programming languages in computer and information science, King Saud University, Muzahimiyah Branch. He has authored several articles in peer-reviewed IEEE, ACM, Springer, and Wiley journals and conferences. His research interests include edge intelligence, social networks, cloud computing, the Internet of Things, big data, and health informatics.

MAJED AL-MASHARI (Member, IEEE) is currently a Professor of information systems. He offers many consultations in various fields of information technology. He has authored many scientific papers in highly reputed journals and conferences. His research interests include business process management, ERP systems, requirement engineering. He has presented many public lectures and received several international and regional scientific awards. He acted as a reviewer of many scientific papers and research thesis. He is the Editor-in-Chief of the *Business Process Management Journal*. He is also on the editorial boards of several scientific journals and participated as a member of many scientific committees of conferences. He chaired several IT-related national conferences and forums.