IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 11 November 2023, accepted 27 November 2023, date of publication 1 December 2023,
date of current version 12 December 2023.

Digital Object Identifier 10.1109/ACCESS.2023.3338861

RESEARCH ARTICLE

Exploring Synergy of Blockchain and 6G Network for Industrial Automation

MANO YADAV[1], UDIT AGARWAL[2], VINAY RISHIWAL[2], (Senior Member, IEEE), SUDEEP TANWAR[3], (Senior Member, IEEE), SUMAN KUMAR[4], FAYEZ ALQAHTANI[5], AND AMR TOLBA[6], (Senior Member, IEEE)

[1]Department of Computer Science, Bareilly College, Bareilly 243001, India
[2]Department of Computer Science and Information Technology, MJP Rohilkhand University, Bareilly 243006, India
[3]Department of Computer Science and Engineering, Institute of Technology, Nirma University, Ahmedabad 382481, India
[4]Computer Science Department, Troy University, Troy, AL 36082, USA
[5]Software Engineering Department, College of Computer and Information Sciences, King Saud University, Riyadh 12372, Saudi Arabia
[6]Computer Science Department, Community College, King Saud University, Riyadh 11437, Saudi Arabia

Corresponding authors: Suman Kumar (skumar@troy.edu), Vinay Rishiwal (vrishiwal@mjpru.ac.in), and Sudeep Tanwar (sudeep.tanwar@nirmauni.ac.in)

This work was supported in part by King Saud University, Riyadh, Saudi Arabia, through the Researchers Supporting Project under Grant RSP2023R509; and in part by Troy University, Troy, Alabama.

ABSTRACT Automating industrial tasks have become critical for organizations due to the inefficiencies and risks associated with conventional procedures. The proliferation of connected devices and machines brings forth a range of security concerns, including data tampering and unauthorized access. Establishing confidential and trustworthy communication between these devices becomes particularly difficult as they rely on the open channel of the Internet. Numerous established security measures, such as antivirus software, access control systems, intrusion detection systems (IDS), and intrusion prevention systems (IPS), have been identified in the literature as facing issues like centralized vulnerabilities, latency challenges, reliability issues, and single points of failure. As technology advances rapidly, the convergence of emerging technologies holds immense potential to revolutionize industrial automation. Among these promising technologies, blockchain and 6G stand out for their immense potential. With its decentralized and tamper-proof nature, blockchain has disrupted various sectors, while 6G offers unprecedented connectivity and lightning-fast data transfer speeds. Motivated by these developments, this paper explores the potential impact of integrating blockchain technology with 6G in industrial automation, paving the way for the future of smart factories and intelligent supply chains. Our proposed work aims to provide a holistic understanding of this emerging amalgamation's key benefits, challenges, offered solutions, and prospects.

INDEX TERMS Industrial automation, blockchain technology, 6G, IoT, smart services.

I. INTRODUCTION

In the past decade, the Internet's rapid expansion and communication technology breakthroughs have paved the way for a remarkable flow in automation across different industries. Healthcare, agriculture, smart cities, supply chain and logistics, and finance have witnessed unprecedented growth by adopting automation tools and techniques [1]. Industrial automation has emerged as a pivotal force in these domains, offering many advantages, including cost-effectiveness, adaptability, heightened productivity, exceptional quality, enhanced security, and precise data collection. By harnessing the power of computers, digital devices, actuators, and sensors, industrial automation facilitates the efficient group, distribution, and dissemination of critical information, empowering efficient and effective decision-making processes. Industrial automation offers a solution to the constraints associated with conventional production, manufacturing, and logistics methods. The traditional approaches often need help with tasks such as ensuring a sufficient workforce, reducing employee turnover, minimizing human errors, and averting disasters. Countries actively encourage

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

stakeholders to adopt automation-driven practices in their industrial sectors to address these issues. Initially, industries relied on wired Ethernet systems to establish communication with industrial devices, machines, and processes. Nevertheless, these systems presented augmented risks, necessitated manual setup, and entailed elevated maintenance expenses. As a result, industries have shifted towards automation to optimize workflows and procedures. In the contemporary era, 5G technology has emerged as the favored communication network infrastructure for automation on a global scale, primarily due to its many advantages, including remarkably low latency, extensive connectivity, minimal jitter, and enhanced data rates. The convergence of machine learning, 5G, and robotics amplifies service delivery to end-users and facilitates large-scale production improvements. While wireless technologies like 4G and 5G have advantages, they have yet to be widely adopted as the primary technologies for industrial automation. On the contrary, the forthcoming 6G communication network architecture exhibits potential as a feasible and widely adopted technology for achieving real-time and efficient industrial automation. According to the authors [2], [3], 6G networks are expected to offer low latency of less than 0.1m, extremely high reliability such as 99.9999%, and a peak data rate of 1 Tbps. These attributes position 6G as a potential game-changer in industrial automation.

The wireless connectivity that facilitates automation also exposes it to various security threats. These threats include Sybil attacks, where malicious entities impersonate legitimate devices; replay attacks that involve the playback of previously captured data; spoofing attacks that deceive systems into accepting false information; and denial-of-service (DoS) attacks that disrupt normal operations. Furthermore, external attacks can deliberately hinder production processes and compromise the speed and quality of products. Blockchain emerges as a viable solution to fulfill the fundamental needs of industrial automation, providing crucial features such as security, immutability, transparency, privacy, and trust. By leveraging blockchain technology (BT), industries can ensure a robust and secure environment for their automation systems while maintaining high data integrity, transaction transparency, and privacy protection. The inherent trust and reliability offered by blockchain make it a compelling choice for meeting the essential requirements of industrial automation.

A. SCOPE OF THIS PAPER

We have comprehensively analyzed the existing literature on blockchain-based solutions for industrial automation in the context of 6G technology. Our study encompasses the period from 2010 up until the present. Throughout our research, we have explored various security concerns in industrial automation and investigated scholarly papers relevant to the intersection of blockchain and 6G-enabled industrial automation. It was observed that BT significantly influences a wide range of industrial activities. Table 1 gives a comparative study of the significant industrial automation studies. Mao and Xiao [4] proposed the application of blockchain for enhancing the reliability, security, efficiency, and cost-effectiveness of the industrial control system (ICS) through network security measures. Dorri et al. [5] introduced a safe and lightweight framework based on BT for IoT in the automotive industry. Regarding communication networks, Brown et al. [6] analyzed low-latency 5G-based infrastructures and their impact on industrial operations. Mistry et al. [1] discussed state-of-the-art approaches that combine 5G and blockchain technologies to enhance the performance and security of industrial processes. You et al. [7] provided a comprehensive overview of the visions and enabling technologies of 6G, offering valuable insights into the future of this technology. Authors of [2] examined the advantages of 6G communication technology over 5G, including improvements in spectrum distribution, connection density, communication latency, and data rate, contributing to enhanced service quality. Researchers also explored the utilization of 6G qualities for improving communication networks. Astarita et al. [8] conducted an extensive review of the applications of blockchain-based systems in the transportation sector. Hussain et al. [9] surveyed different resource management aspects in cellular and IoT networks that leverage machine learning techniques. Manogaran et al. [10] proposed a blockchain-assisted secure data sharing (BSDS) model that enhances security in data acquisition and dissemination for industrial applications. Hariharan and Rajkumar [11] explored various research challenges of adopting blockchain for 5G IoT-enabled industrial automation. Javaid et al. [12] discussed the integration of BT in manufacturing automation. Brown et al. [6] emphasized integrating 5G technology with industrial standards to improve effectiveness and reliability. Alsharif et al. [13] examined the key features of 6G in industrial automation and other domains. However, it is essential to note that existing research primarily focuses on utilizing blockchain with IoT for security or decentralized storage. The potential of combining blockchain with 6G for industrial automation has not been thoroughly explored. Motivated by this gap, we conducted a comprehensive study of the significance of BT in 6G-enabled industrial automation, covering difficulties with implementation challenges, application scenarios, and future perspectives.

B. RESEARCH CONTRIBUTION

In recent years, a few blockchain studies have appeared in communications using 6G, showing that industry-oriented research is still in its early phases. Besides its advantages in identification, accountability, and asset tracking, BT is vital in facilitating secure information transmission across participant nodes in the context of intelligent organizations. This paper investigates the possible synergy between BT and 6G in industrial automation. Our research has made significant contributions in the following areas:

TABLE 1. Comparative study of the state-of-the-art surveys on industrial automation with the proposed work.

Paper	Year	Objectives	Industry	Security	Pros	Limitations
Dorri et al. [5]	2017	Blockchain-based novel secured architecture for the automobile industry.	Automobile	Yes	The privacy of the users is maintained through this proposed architecture.	More exploration was required about congestion control.
Mao et al. [4]	2018	To use BT for industrial control systems to secure transactions.	General	Yes	Reliable, safe, highly efficient, and low cost.	The experimental analysis could have been better.
Zhao et al. [14]	2019	Investigate the important qualities of 6G mobile communication in industrial areas.	General	No	Higher efficiency and good throughput.	Security aspects for Industrial automation should have been discussed.
Schuetz et al. [15]	2019	To comprehend the significance of safe industrial automation with BT	Automobile	Yes	Comprehensive analysis and research findings on blockchain-based automobile industries.	Not discussed various attacks such as Sybil attacks .
Nguyen et al. [16]	2020	Issues regarding data privacy and security in 6G networks.		Yes	Advantages and disadvantages of using blockchain in 6G networks.	Not much focused on Industrial automation.
Yrj¨ol¨a et al. [17]	2020	Use of blockchain to create an open business model comprising multiple stakeholders in the 6G ecosystem.		Yes	A decentralized and trust-less business model for 6G.	Security aspects for Industrial automation should have been covered.
Alsharif et al. [13]	2020	Investigate the important features of 6G in Industrial automation.	General	Yes	High security and energy efficiency	No Real-time implementation.
Sekaran et al. [18]	2020	Security-related issues in blockchain-enabled IoT in 6G.		Yes	A special emphasis will be placed on blockchain-enabled IoT solutions in future 6G networks.	Not much focused on Industrial automation.
Xu et al. [19]	2020	Use of blockchain in 6G for infrastructure and resource management in 6G.	General	No	Highlighting the significance of blockchain in enhancing resource management within the 6G network.	Not much focused on Industrial automation.
Hewa et al. [20]	2020	6G challenges and what blockchain offers to 6G networks.		No	6G uses cases that can be improved by blockchain.	Not much focused on Industrial automation.
Javaid et al. [12]	2021	Acceptance of BT in the manufacturing industry.	Manufacturing	Yes	Eradication of third-party.	Network discrepancies in the Industrial automation process were not covered.
Hariharan and Rajkumar [11]	2021	Challenges for blockchain-driven 5G IoT-enabled industrial automation.	General	No	Effective tracing of transaction logs	security challenges
Manogaran et al. [10]	2022	Introducing a secure data-sharing strategy tailored for the smart industry.	General	Yes	Statistical analysis is extensively studied.	In-depth security concerns still need to be fully addressed.
Proposed survey	2023	Blockchain and 6G for Industrial automation		Yes	Coordination of blockchain and 6G to improve industrial automation.	

1) We provide a comprehensive and systematic review of prevailing state-of-the-art surveys on industrial automation, focusing on their security and privacy concerns.
2) We discuss various applications that involve blockchain integration with 6G-enabled IoT.
3) We propose a decentralized and secure industrial automation architecture incorporating 6G technology. A Case study of strengthening industrial automation and intelligent supply chain management is also presented.
4) Lastly, our research aims to address the challenges related to scalability, interoperability, and other aspects of blockchain applications in the context of 6G-enabled IoT for industrial automation.

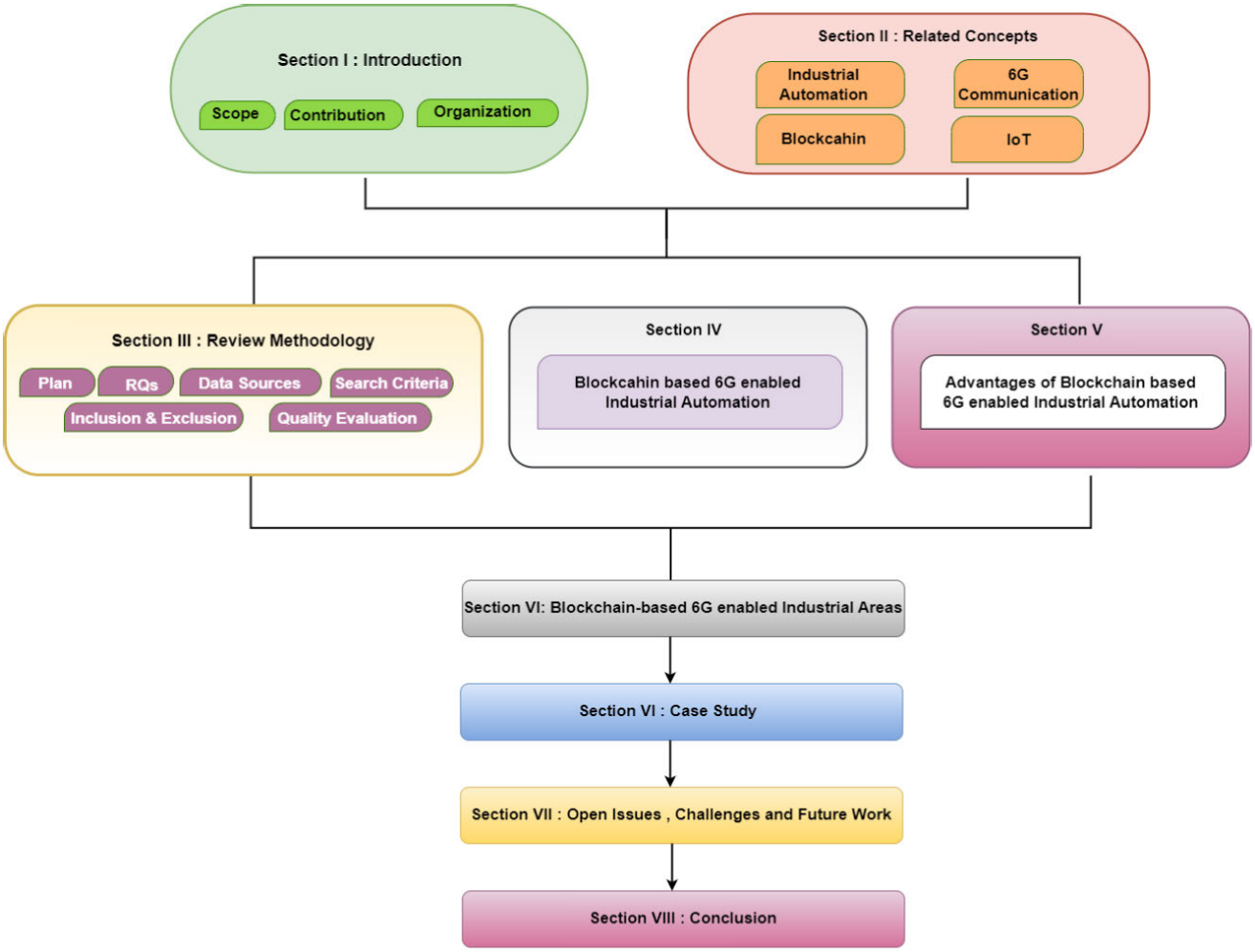


FIGURE 1. Outline of the paper.

C. ORGANIZATION AND READING MAP

The rest of the paper is structured as follows. The second section outlines the key ideas of the central concepts relating to industrial automation, 6G communication, Blockchain, IoT, and the role of 6G in IoT. Section III discusses the benefits of integrating Blockchain with 6G-enabled IoT devices in industrial automation. Section IV delves into a comprehensive discussion of the significant areas where 6G-enabled IoT is combined with Blockchain in various industries such as smart healthcare, smart city, Autonomous vehicles, smart agriculture, and smart and secure supply chain management. Section V presents a case study of secure supply chain management with the amalgamation of 6G-based IoT and BT. Section VI examines several unresolved issues and outlines potential future guidelines for amalgamating Blockchain and 6G in industrial automation. Finally, in Section VII, we summarize the main findings and contributions. Fig. 1 shows the basic outline of the paper.

II. RELATED CONCEPTS

Several ideas and technologies are addressed in this section to implement industrial automation operations.

A. INDUSTRIAL AUTOMATION

Industrial automation involves the application of advanced technologies, such as robotics, artificial intelligence, machine learning, and sensors, to automate tasks traditionally performed manually by humans. Its primary objectives include optimizing operations, reducing the need for manual labor, minimizing errors, and improving overall performance across various industries. Industrial automation has progressed remarkably from the first industrial revolution to the anticipated Industry 5.0, as shown in Fig. 2. Each phase has brought significant advancements, transformed the manufacturing landscape, and driven us toward a more interconnected, efficient, and human-centered future. In this sub-section, we will explore the historical timeline of the Industrial Revolution and its different phases. The emergence of Industry 1.0 in 1974 marked a significant shift in industrial production. It evolved by introducing mechanical production infrastructures powered by water and steam. Industry 2.0 emerged around 1870, adopting electric power and assembly line production. The focus shifted to mass production and workload distribution, resulting in improved productivity for manufacturing companies. 1969 Industry 3.0 integrated

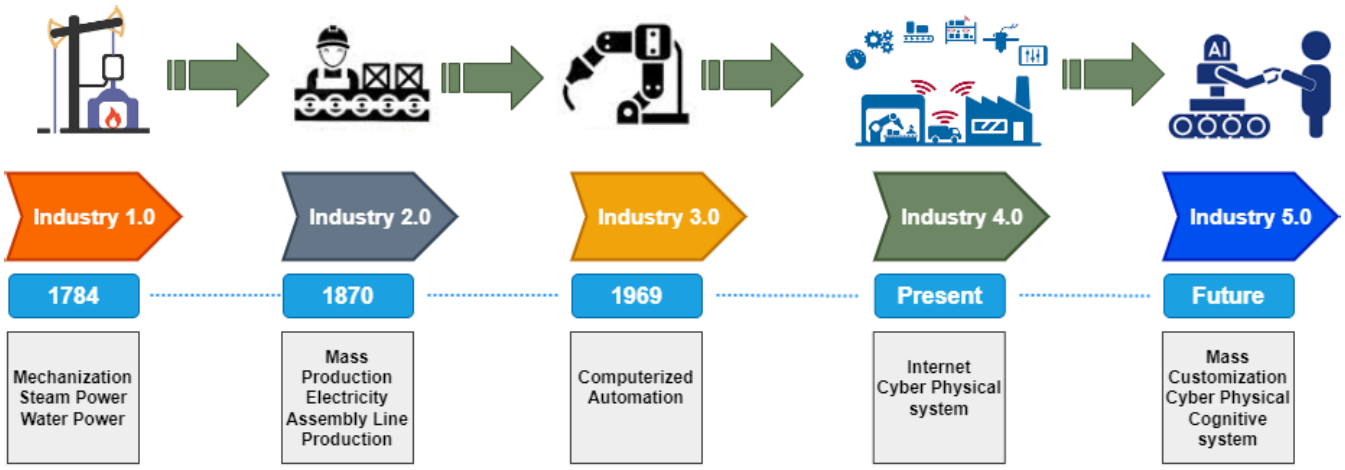


FIGURE 2. Timeline of industrial automation (Industry 1.0 to Industry 5.0).

electronics, partial automation, and information technologies. The advent of Industry 4.0 has reformed the manufacturing segment by combining various techniques such as artificial intelligence (AI), the IoT, cloud computing, cyber-physical systems (CPSs), and cognitive computing [21], [22]. The core concept of Industry 4.0 is to create a ''smart'' manufacturing process through interconnected technologies and devices that can control each other throughout their life cycle [23].

FIGURE 3. Advantages of industrial automation.

The concept of Industry 5.0 is now being explored, aiming to combine the unique creativity of human experts with the capabilities of powerful, intelligent machinery. One of the main contributions of Industry 5.0 is mass personalization, where customers can customize and personalize products according to their preferences and needs. In this new era, repetitive and monotonous tasks are assigned to robots and machines, while humans focus on critical thinking and customization. Industry 5.0 takes a human-centric approach, promoting collaboration between ideal human companions and collaborative robots (cobots) to achieve personalized and autonomous manufacturing through enterprise social networks. Cobots can sense and recognize the human presence, making them suitable for tedious and labor-intensive tasks, while humans are better equipped for tasks requiring creativity and problem-solving skills [24].

Industrial automation provides many advantages, such as boosting productivity, enhancing product quality, reducing costs, increasing production capacity, shortening lead times, enabling data-driven decision-making, offering flexibility, gaining a competitive edge, and supporting sustainable practices. The benefits of industrial automation are illustrated in Figure 3.

1) SECURITY AND PRIVACY ISSUES

Security and privacy concerns within industrial automation have become essential issues in today's increasingly interconnected and automated industrial environment [25]. With industries leaning heavily on automated systems to enhance efficiency, vulnerabilities have come to the forefront. The emergence of cyber threats targeting industrial control systems (ICS) poses a substantial risk, potentially resulting in production interruptions, compromise of sensitive data, or even physical harm. The integration of IoT devices and the convergence of IT and operational technology (OT) systems further heighten these concerns by broadening the potential attack points. Striking a balance between accessibility, convenience, and safeguarding sensitive information and critical infrastructure presents a complex challenge. The wireless connectivity enabling automation also exposes it to various security threats, including Sybil attacks (malicious entities impersonating legitimate devices), replay attacks (playback of previously captured data), spoofing attacks (tricking systems into accepting false information), and

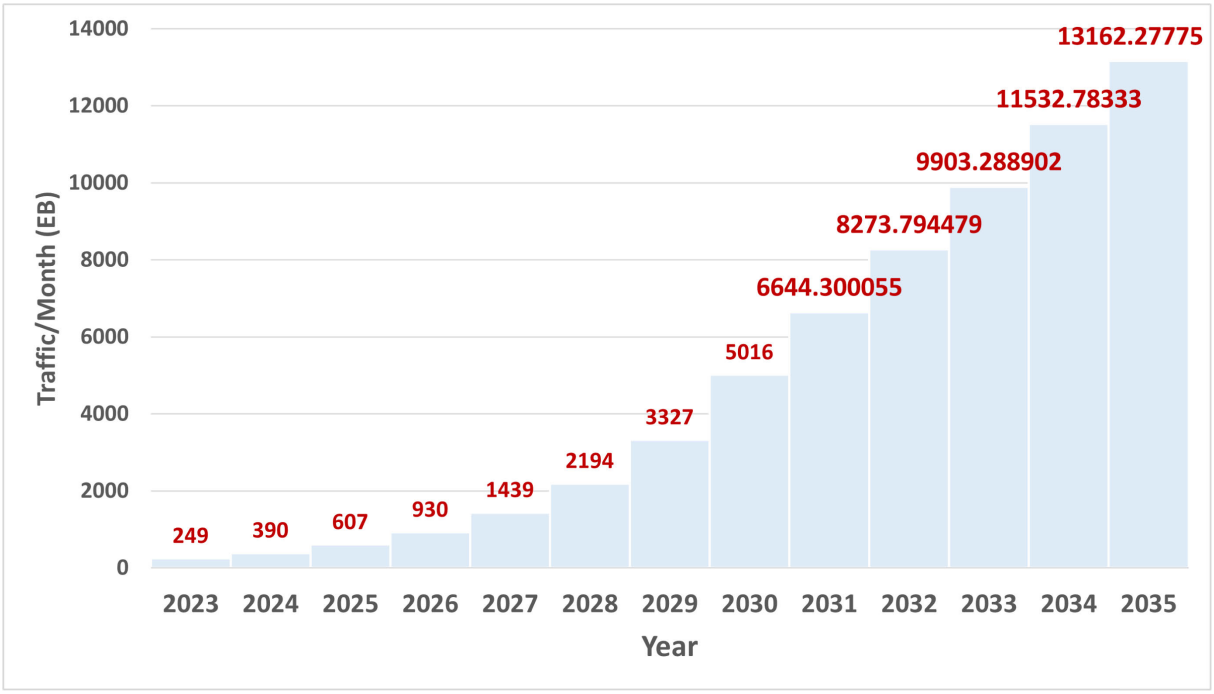


FIGURE 4. The future trajectory of worldwide mobile data traffic prediction.

denial-of-service (DoS) attacks (disrupting normal operations) [26]. Additionally, external attacks can intentionally disrupt production processes, compromising product speed and quality. Ensuring the integrity, confidentiality, and availability of sensitive data and critical operations is paramount. Industrial automation systems responsible for overseeing processes and machinery in manufacturing, energy, and transportation must navigate a delicate balance between efficiency and defense against cyber threats. Addressing these concerns entails implementing robust security protocols, continuous monitoring, and ongoing education to safeguard industrial operations' physical and digital aspects, thereby ensuring a more secure and resilient industrial ecosystem.

In the following subsections, we provide a concise overview of 6G communication and Blockchain technology, highlighting their significance in the realm of industrial automation.

B. 6G COMMUNICATION

Mobile communications have progressed from analog voice calls to high-speed, data-intensive networks that support a wide range of applications and services. Each generation has brought significant improvements, transforming how we interact and work with the environment [27]. Figure 5 shows the evolution of mobile communication. 6G (Sixth Generation) communication is the successor to 5G communication. 6G communications are expected to offer improved data speed and coverage services, enabling users to stay connected anytime and anywhere. The advancements in 6G systems aim to shift wireless communication technology from merely connecting devices to fostering intelligent connections. This means that 6G networks will be crucial in supporting pervasive AI-based services, extending from the network's core to end devices. In 6G, eMBB-Plus will surpass the capabilities of 5G's eMBB, delivering a high-quality user experience and setting new standards for data utilization. 6G's URLLC capabilities can provide a highly dependable

TABLE 2. Comparison of 6G with 4G and 5G communication systems.

	4G	5G	6G
Applications	HD Videos, Mobile Internet	VR/AR/IoT Devices	Industrial Internet
Peak Data Rate	6 GHz	90 GHz	10 THz
Maximum Frequency	100 Mbps	20 Gbps	1 Tbps
Multiplexing	OFDMA	OFDMA	SMART OFDMA + IM
Spectrum Efficiency	1X	3X	15X
Latency (ms)	10 ms	1 ms	0.1 ms
Satellite Communication	No	No	Yes
Mobility Support	as much as 350 km/hrs	as much as 500 km/hrs	as much as 1000 km/hrs
Haptic Communication	No	Partial	Fully
Usage	MBB	eMBB, mMTC, URLLC	FeMBB, umMTC,ERLLC

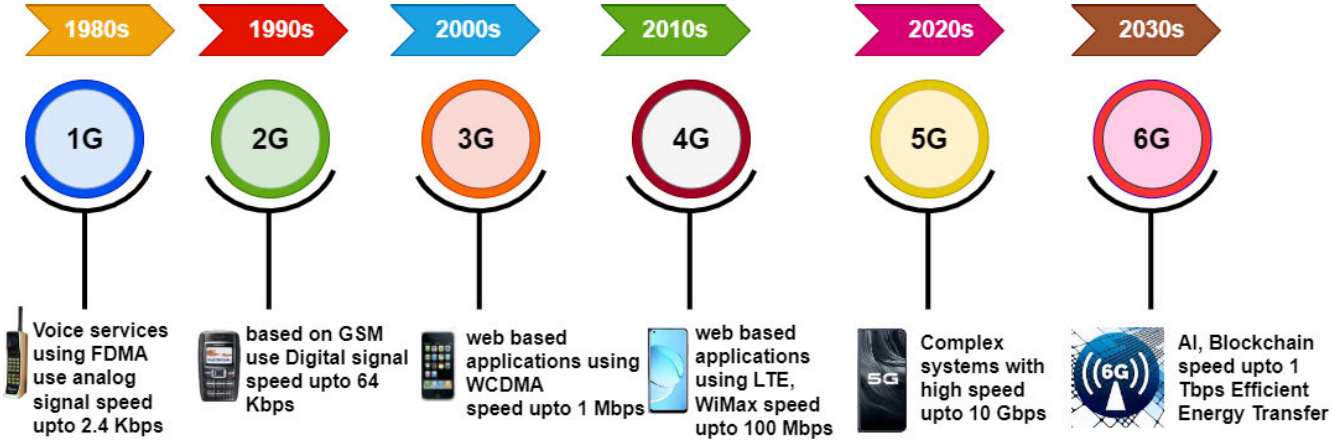


FIGURE 5. Evolution of mobile communications.

and near-real-time communication infrastructure, enabling seamless connectivity between machines, sensors, and control systems in industrial settings. The mMTC feature in 6G allows massive connectivity, enabling many devices and sensors to communicate simultaneously. 6G's high data rates, low latency, and ultra-high definition capabilities open up possibilities for immersive AR and VR experiences in industrial automation. 6G's technological advancements in communication, sensing, and AI can greatly benefit industrial robotics and autonomous systems. High-speed and reliable connectivity enables efficient control, coordination, and synchronization of robots and autonomous vehicles. This paves the way for complex automation tasks, such as collaborative robots (cobots), autonomous material handling, and intelligent transportation systems within factories and industrial facilities. Table 2 compares 6G with 4G and 5G communication networks based on technical specifications.

To meet the substantial increase in mobile data traffic expected to surpass 5016 EB/month by 2030 and 13162 EB/month in 2035, as depicted in Figure 4, the upcoming 6G networks will be essential. These networks must effectively utilize resources to accommodate the projected high density of interconnections (1 million/km2). Exploring high-frequency bands ranging from 73-140 GHz and 1-3 THz becomes crucial for offering user-centric scenarios with exceptional reliability (99.99%) and a 1 ms user plane latency.

C. BLOCKCHAIN

Blockchain represents an unalterable and highly secure interconnected list that continually grows with every transaction. This decentralized ledger technology ensures the monitoring and execution of transactions on a reliable platform. Unlike traditional systems, where a single entity governs the proceedings, blockchain operates on a distributed ledger model shared among all participants. This decentralized and unalterable nature allows parties to engage in independent transactions and validate data on the ledger without relying on intermediaries for similar tasks. Blockchain aims to establish and validate trust without relying on a central authority, instead entrusting this responsibility to a decentralized network. Consequently, this approach bolsters security, efficiency, and scalability.

According to Balandina et al., [28], blocks in a blockchain are interconnected through self-executable smart contracts that rely on cryptographic protocols. Persistence is a fundamental attribute of blockchain technology. Once records are accepted and added to the distributed ledger, they become immutable and cannot be deleted or altered. This permanence is maintained across multiple network nodes, ensuring the data's integrity and security. The structure of the blockchain allows for both anonymity and traceability. This is achieved through the use of hashes to interconnect different blocks. Each block contains a collection of transactions organized in a Merkle tree format [29]. The Merkle tree enables efficient verification and validation of each transaction's authenticity against its known origin, facilitating traceability throughout the blockchain. The consensus mechanism of blockchain ensures transaction integrity and consistency. Transaction throughput, security, and scalability are key performance parameters of the consensus mechanism, which vary based on application scenarios. Commonly used consensus mechanisms include PoW, PoS, and Byzantine fault tolerance. BT can be classified into three main categories: public, consortium, and private. In a public blockchain, often referred to as a permissionless blockchain, participation is open to anyone. Anyone can join the network, view the transactions, contribute to the consensus process, and suggest changes to the underlying software. Although it offers high data immutability, efficiency is relatively low. Consortium blockchain, on the other hand, provides high efficiency but is more susceptible to data tampering. Priyadarshan et al. [30] and Drosatos and Kaldoudi [31] have mentioned that private blockchain restricts participation to particular nodes within a distributed network organized by a single organization with centralized authority over all transactions. Kumar and Majumder [32] highlight the use of blockchain in

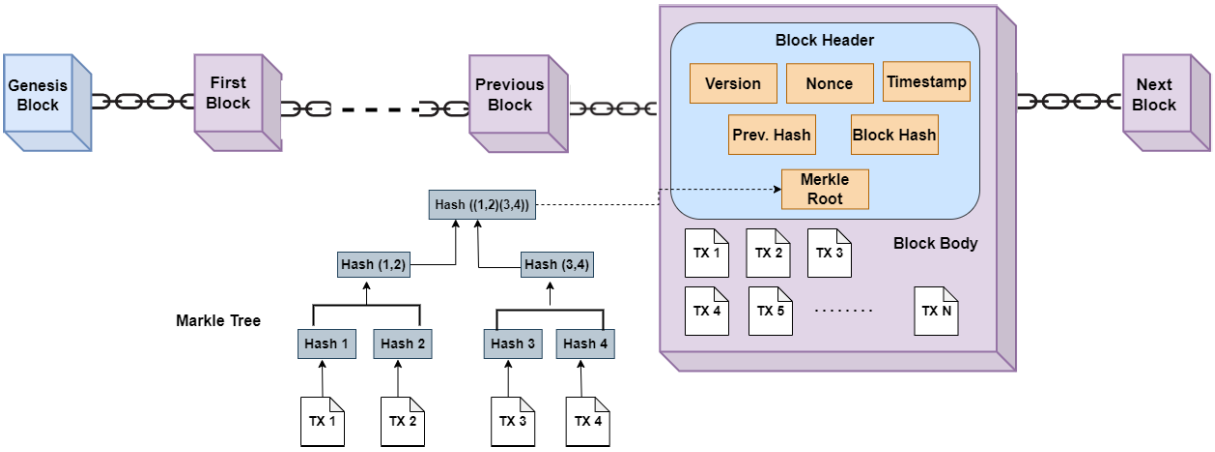


FIGURE 6. Blockchain network.

IoT networks for recording, examining, and transmitting real-time data from different objects, such as humans or sensors. This enables the automation of various assignments or tasks.

In the subsequent subsection, we will present a concise overview of IoT networks and highlight the significance of 6G within this domain.

D. INTERNET OF THINGS (IoT)

The IoT encompasses a system of physical objects like devices, vehicles, appliances, and other items equipped with sensors, software, and connectivity capabilities. These features enable them to connect to the Internet and exchange data. Connectivity can be achieved through various communication technologies such as Wi-Fi, Bluetooth, cellular networks, Zigbee, or other wireless protocols. IoT allows ordinary objects to connect to the Internet, enabling communication between objects and humans. Unlike traditional systems, IoT is a self-configuring network where devices automatically configure themselves without human intervention. This technology facilitates a deeper understanding of the environment and enables machines to better sense and report conditions. According to Cocosila and Archer [33], organizations are adopting IoT to improve operational efficiency, address customer concerns, make informed decisions, and enhance overall business outcomes. IoT devices find widespread application in various fields, including manufacturing, industrial automation, businesses, wearable technology, and the healthcare sector. These devices have enhanced efficiency, automation, and data collection in diverse industries and everyday life. Key characteristics of an IoT network include dynamic and self-adapting behavior, self-configuring capabilities, inter-operable communication protocols, and unique object identities within the network. An IoT device can have multiple interfaces, including sensors, actuators, memory, and audio/video connections to wired and wireless devices. Sensors collect environmental data, measuring temperature, humidity, pressure, motion, and light. Conversely, actuators allow devices to respond or take action based on the received data physically. For instance, a smart thermostat's sensor measures the temperature, and the actuator adjusts it accordingly.

1) ROLE OF 6G IN IoT

The IoT is experiencing rapid growth, facilitating enhanced connectivity between devices and individuals through the Internet. Wireless networks have evolved to accommodate the expanding technology landscape, offering improved features. Integrating 6G into IoT ecosystems holds immense potential for transformative impacts. It significantly enhances IoT security, boosts data transfer speeds, improves cellular operations with increased bandwidth, and resolves various network challenges encountered in previous generations of mobile communication networks. Given the substantial amount of data exchanged among connected devices in IoT applications, there is a pressing need for improved capabilities, higher data rates, and enhanced connectivity. Consequently, 6G is recognized as a vital enabler for IoT, allowing devices to communicate intelligently in connected environments through intelligent sensors. Furthermore, it expands the coverage area and scale of IoT applications by delivering superior communication and capabilities.

Key characteristics of 6G include a minimum data rate of 1 terabit per second and a low latency of 1 millisecond. Operating in the frequency range of gigahertz (GHz) to terahertz (THz), 6G optimizes network spectrum utilization and facilitates connections for many interconnected devices, enabling the realization of the Internet of Everything. These advancements improve connectivity and introduce novel applications focusing on privacy and security. The promise of 6G networks lies in their ability to deliver very high data transfer rates, low latency, and robust integrity. Additionally, the heterogeneous connectivity offered by 6G cellular networks further supports the diverse requirements of IoT applications.

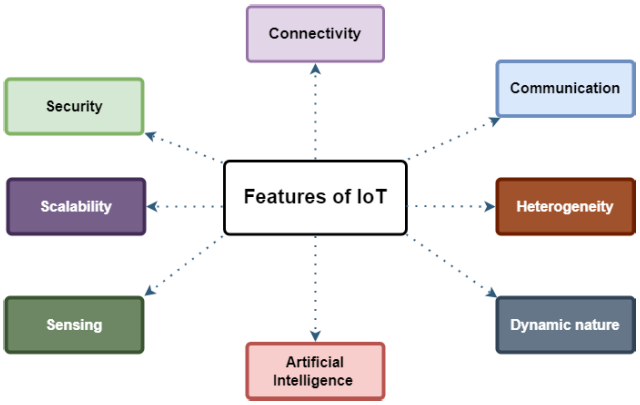


FIGURE 7. Features of IoT.

So, the role of 6G in IoT is transformative, revolutionizing connectivity and driving advancements in various sectors. By offering enhanced connectivity, lower latency, increased device density, and seamless integration with edge computing and AI, 6G unlocks the full potential of IoT, fueling innovation and empowering the connected world of the future.

III. REVIEW METHODOLOGY

This section outlines the review methodology, which draws upon the guidelines suggested by Kitchenham et al. [34], [35].

A. REVIEW PLAN

We have outlined the proposed survey systematically, following these steps for the literature: Defining research questions, identifying data sources, applying search constraints to collected data, implementing inclusion and exclusion criteria, and evaluating the quality of identified materials.

By conducting this survey, we successfully identified appropriate publications, studies, and research. Our approach involves initially assessing the quality of the materials, after which we selectively extract the relevant data for the intended survey. This structured review process is designed to aid researchers in achieving impartial and unbiased results.

B. RESEARCH QUESTIONS

The projected survey outlines the current literature regarding 6G and Blockchain in various industry automation. The research questions (RQs) and their corresponding objectives for this systematic survey can be found in Table 3.

C. DATA SOURCES

We have determined digital libraries, such as IEEEXplore, Springer, ACM, Science Direct, Elsevier, and numerous others, as our primary data sources. These academic repositories offer a wide array of literature we thoroughly examined to conduct the proposed survey. This approach aligns with Kitchenham et al. [34], [35] recommendation to leverage electronic data sources for comprehensive literature surveys. Additionally, we consulted various resources, including articles, technical reports, blogs, books, and patent contributions, to ensure an exhaustive survey within our relevant field.

TABLE 3. Research questions and objectives.

Sr. No.	Research Question	Objective
RQ1	What are the advantages that automation brings to industrial operations?	The objective is to investigate the importance of incorporating automation into industrial processes.
RQ2	How does 6G communication technology play a key role in the progression of industrial automation?	It is expected to provide insights into the impact of 6G communication on industrial automation.
RQ3	In what ways does blockchain enhance security within industrial procedures?	The focus is examining diverse, secure methods for implementing blockchain in industrial processes.
RQ4	What makes the synergy between blockchain and a 6G communication network crucial for industrial automation?	The goal is to investigate the need for integrating blockchain and 6G technologies to enhance industrial automation.
RQ5	What are the primary challenges associated with integrating blockchain and 6G-enabled IoT for industrial automation?	The study is expected to address the multiple challenges associated with integrating blockchain and 6G-enabled IoT in the context of industrial automation.

D. SEARCH CRITERIA

Initially, a comprehensive exploration is conducted on different digital libraries, including IEEE Xplore, ACM, ScienceDirect, and Wiley, employing a range of keywords as depicted in Fig 8. Several research papers were not found when using the search string depicted in Fig 8, as occasionally, this string was not present in the abstract and title. To address this, a manual search was conducted in digital sources using the specified keywords to identify these papers.

FIGURE 8. Search string.

E. INCLUSION AND EXCLUSION

The objective is to identify relevant contributions that align with the proposed survey, focusing on recent years. The search employs keywords individually or in conjunction with BOOLEAN operators, such as "industrial automation" with "6G," with "blockchain," combining "6G" with "Blockchain," combining "5G" with "Blockchain," and combining "5G" with "Blockchain." The search yields a total of 124 articles of interest; of these, 97 are selected for the proposed work based on their cutting-edge methodologies

and innovative research on 6G-enabled, blockchain-based industrial automation and its applications.

F. QUALITY EVALUATION

In this section, we conducted a quality evaluation of the reference papers under the recommendations from the Database of Abstracts of Reviews of Effects (DARE) and the Center for Reviews and Dissemination [34].

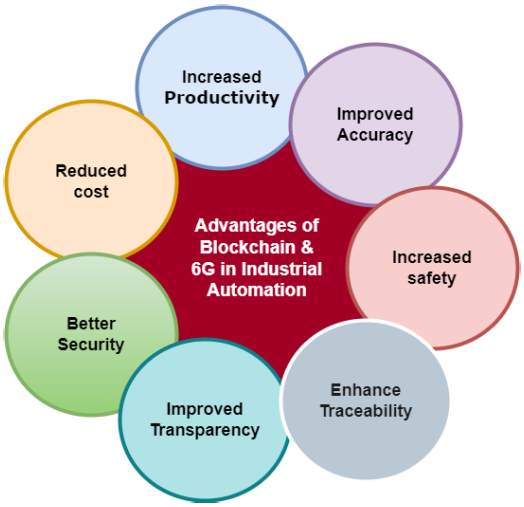


FIGURE 9. Advantages of blockchain and 6G-Enabled IoT devices in industrial automation.

IV. ADVANTAGES OF BLOCKCHAIN INTEGRATION WITH 6G-ENABLED IoT DEVICES IN INDUSTRIAL AUTOMATION

The convergence of BT and 6G-enabled IoT devices has emerged as a promising strategy to transform industrial automation. In a study by Khan et al. [36], [37], [38], the authors emphasized the importance of integrating BT and communication networks to enable efficient, secure, and dependable data exchange in industrial automation. Combining blockchain and 6G-enabled IoT devices facilitates improved data integrity and authenticity. Utilizing blockchain's distributed ledger makes data resistant to tampering, creating a trustworthy and transparent record of transactions, measurements, and events throughout industrial processes [39]. This fosters trust among stakeholders and minimizes the risk of fraudulent activities or data manipulation. Furthermore, blockchain's immutable nature and cryptographic features ensure data integrity, preventing unauthorized access, tampering, or fraudulent behavior. Consequently, this establishes a strong foundation for secure communication, trust, and authentication among interconnected IoT devices within industrial ecosystems. Hence, combining these technologies offers numerous advantages that enhance productivity, accuracy, cost-efficiency, safety, security, transparency, and traceability [40]. Let's explore these advantages in more detail:

1) Increased Productivity: Blockchain and 6 G-enabled IoT devices facilitate seamless communication and coordination among various industrial components and systems [37]. Real-time data sharing, automated processes, and intelligent decision-making capabilities enable efficient resource allocation, streamlined workflows, and optimized production cycles. This increased productivity results in higher output, faster time-to-market, and improved overall operational efficiency.
2) Improved Accuracy: By leveraging blockchain and IoT devices, industrial automation systems can collect, record, and analyze data with a high level of accuracy. IoT sensors capture real-time information from machines, equipment, and environmental parameters, ensuring precise monitoring and control. The decentralized nature of blockchain ensures data integrity and eliminates the risk of tampering or manipulation [41]. As a result, decision-makers can rely on accurate data insights for better operational planning, predictive maintenance, and quality control.
3) Reduced Cost: Blockchain and 6G-enabled IoT devices offer cost-saving benefits in industrial automation [42]. Through real-time monitoring and predictive maintenance, potential equipment failures can be detected in advance, minimizing downtime and reducing maintenance costs. Additionally, smart contracts enabled by BT automate payment processing, supply chain transactions, and inventory management, eliminating intermediaries and associated fees. These cost optimizations contribute to improved profitability and sustainability.
4) Increased Safety: By utilizing IoT devices and blockchain, real-time monitoring of safety parameters such as temperature, pressure, and hazardous conditions becomes possible [43]. IoT sensors can detect anomalies or potential hazards, triggering automatic alerts or shutting down processes to prevent accidents. Blockchain's immutability ensures that safety-related data cannot be altered, providing a trustworthy record of compliance and adherence to safety protocols.
5) Better Security: BT enhances security in industrial automation by offering robust encryption, data integrity, and decentralized control. The distributed ledger ensures that data records cannot be tampered with or modified without consensus, making it highly resistant to hacking or unauthorized access [36], [38]. Blockchain-based identity management solutions also enable secure access control, reducing the risk of unauthorized personnel interfering with critical systems or sensitive information.
6) Improved Transparency: Blockchain's transparent and auditable nature promotes trust and transparency in industrial processes [44]. Every transaction or data exchange recorded on the blockchain is visible to authorized parties, ensuring accountability and preventing fraud. Smart contracts enable automated verification and execution of predefined rules, eliminating the need for intermediaries and reducing the potential

for disputes. This transparency fosters more vital collaboration among suppliers, manufacturers, and customers.

7) Enhanced Traceability: The combination of blockchain and IoT devices enables end-to-end traceability of goods, materials, and components throughout the supply chain. Each production, handling, and transportation step can be recorded on the blockchain, creating an immutable audit trail [44]. This transparency helps identify bottlenecks, optimize logistics, and address quality issues promptly [45]. In industries where authenticity and non-plagiarism are critical, such as pharmaceuticals or luxury goods, blockchain-based traceability ensures the integrity of products and protects against counterfeit or plagiarized items [46].

V. APPLICATION OF BLOCKCHAIN IN 6G ENABLED SERVICES

The implementation of BT and the integration of 6G-enabled IoT offer various opportunities for industrial applications. These applications span several domains, including autonomous vehicles, smart supply chain management, smart cities, smart healthcare, and smart agriculture. In these areas, the combined use of blockchain and 6G provides enhanced security, increased bandwidth, and reduced operational and capital costs. Further elaboration on these applications can be found in the subsequent subsections.

A. SMART HEALTHCARE

Healthcare plays a crucial role in any nation's overall development, reflecting its society's well-being. As population and illness rates increase, the demand for smart healthcare systems intensifies. In the past, patient-doctor communication primarily relied on in-person visits, phone calls, or text messages, which limited healthcare providers' ability to monitor patients continuously [1]. The emergence of IoT has revolutionized this landscape by introducing wearable healthcare devices that enable continuous patient monitoring. This remote monitoring capability has improved the ease and efficiency of doctor-patient interactions, reducing hospital stays and readmissions. Additionally, IoT has facilitated the use of smart beds equipped with sensors, which continually monitor vital signs like blood pressure, temperature, and heart rate. The integration of 6G and IoT holds promise as a potential solution to address the challenges faced by the healthcare system. One such solution involves remote health monitoring, where IoT sensor devices are utilized to measure and analyze various health parameters of individuals remotely. Electronic health records (EHR) [47] consist of digital versions of patients' health information, while personal health records (PHR) pertain to the digital records of individual patients.

Sun et al. [48] conducted a comprehensive study on the vulnerabilities related to security and privacy in healthcare devices based on the IoT. To mitigate potential issues arising from using IoT-based wearable devices in healthcare monitoring systems, they proposed the integration of BT. This integration ensures the secure storage of patient information, promoting a safe and protected environment for utilizing IoT devices in healthcare systems. In another study [49], the authors discovered the advantages of employing BT to combat safety and confidentiality attacks in electronic healthcare record systems. They studied various blockchain-based systems that enhance the security of information storage, sharing, and audit functionalities within healthcare systems. Furthermore, Bhuiyan et al. [50] conducted an extensive survey on IoT-based healthcare systems. Subramanian and Thampy [51] developed a blockchain-based system specifically designed to safeguard the data of diabetic patients. The authors of [52] proposed a secure solution that employs the Ethereum protocol and utilizes smart contracts to simplify the analysis and control of wearable sensors while protecting medical data. In [53], the authors addressed the urgent need for advanced medical facilities during the COVID-19 global pandemic. They developed an IoT-based healthcare monitoring system that suggests hybrid communication, extensive medical screening, and cloud-based data centers. This architecture supports hospitals, rescue teams, and first aid units in managing the crisis effectively. Costa et al. [54] also proposed a Fog and blockchain-based system to effectively control global vaccination efforts, ensuring secure and efficient vaccination administration.

The mentioned studies shed light on the essential role of BT in enhancing the security and privacy of healthcare systems that rely on IoT-based devices. By incorporating BT, these systems can guarantee the secure storage of patient data, safeguarding it against potential vulnerabilities and attacks. Furthermore, BT has proven effective in protecting electronic healthcare records and providing certain functionalities for storing, sharing, and auditing information. The introduction of 5G/6G-enabled IoT devices and blockchain-based systems for global vaccination efforts further underscores the potential of BT in ensuring secure and efficient healthcare administration on a worldwide scale. In summary, integrating BT is a promising solution to address security and privacy concerns in IoT-based healthcare systems, paving the way for safer and more dependable healthcare services.

B. SMART CITY

Integrating blockchain and IoT technologies in smart cities holds immense potential to enhance various aspects of urban life [58]. By combining these technologies, smart cities can improve traffic management, optimize energy consumption, strengthen waste management practices, and empower citizens with greater control over their data. These advancements contribute to developing efficient, sustainable, and citizen-centric urban environments.

In smart cities, IoT sensors and devices are strategically deployed throughout road infrastructure, vehicles, and parking areas to gather valuable data on traffic flow, availability,

TABLE 4. Comparative analysis of current methodologies for smart healthcare systems.

Author	Year	Objective	Pros	Cons
Saravanan et al. [55]	2017	Proposed a new approach to monitor diabetes in healthcare.	The model's functionality in emergency scenarios is addressed.	Considerations beyond emergencies were not addressed.
Capossele et al. [56]	2018	Introduced a framework for promoting the expansion of S-health applications.	Comprehensive descriptions of the major issues affecting the S-health environment.	The security features of S-health applications were not specifically defined.
Sun et al. [48]	2019	A review of the security needs for the Internet of Medical Things was conducted.	Various Security attacks are discussed.	Explored concise security attacks in detail.
Bhuiyan et al. [50]	2021	A thorough examination of medical applications, security standards, and market potential in IoT-based healthcare systems was conducted.	Studied device compromise, data leakage, and authentication threats in terms of security vulnerabilities.	Advanced security vulnerabilities can hinder the implementation of the proposed solution.
Subramanian et al. [51]	2021	Implemented a blockchain-based solution to secure the data of diabetes patients.	Established a continuous monitoring system for diabetic patients who were particularly affected by the COVID-19 pandemic using BT.	The suggested system must reduce transaction fees and power usage.
Jagathee saperumal et al. [57]	2022	Investigated new technologies for safeguards in healthcare systems.	IoT, future networks, AI, and big data analytics were explored and their roles in offering efficient healthcare security solutions.	Examined security attacks to a certain extent.
Tomasicchio et al. [53]	2022	Discussed a healthcare emergency management system for monitoring widespread epidemics.	Suggested an IoT-based healthcare monitoring architecture that provides hospitals, rescue teams, and first aid units with hybrid connectivity, massive medical screening, and cloud-based data centers.	The cost of communication and computation needs to be addressed.

and congestion [59]. This data, crucial for effective traffic management, can be stored on a blockchain, guaranteeing its integrity and providing a reliable platform for authorities to analyze and optimize traffic management strategies. Similarly, IoT devices play a vital role in monitoring and collecting real-time data on energy consumption within smart cities [60]. By integrating these devices with BT, energy producers, consumers, and grid operators can establish a decentralized energy management system. Smart contracts executed on the blockchain enable automatic and transparent energy trading, leading to optimized energy distribution and reduced waste [61], [62]. IoT sensors embedded in waste bins continuously monitor waste levels and promptly send notifications when they require emptying. Recording this data on a blockchain allows waste management authorities to streamline their collection routes, significantly reducing unnecessary trips and promoting more efficient and environmentally friendly waste management practices. BT also empowers citizens by giving them better control over their data. By securely storing identity information and access controls on the blockchain, individuals can grant specific entities or services permission to access their data, enhancing privacy and mitigating the risks of data breaches [63]. This streamlined process of accessing public services benefits both citizens and service providers.

Fan et al. [64] introduced a simulated environment utilizing BT on the Ethereum platform to effectively manage IoT data systems on a large scale. Habibzadeh et al. [65] conducted an extensive survey focusing on security and policy concerns in implementing smart cities. Their findings emphasized the vulnerabilities of smart city applications and highlighted the importance of collaboration between technology and government policies to address these vulnerabilities. Biswas and Muthukkumarasamy [71]devised a framework based on blockchain to enable protected communication between entities in smart cities while ensuring privacy. Khan et al. [68] developed a system that leveraged BT to authenticate data from CCTV cameras in smart cities. Lazaroiu and Roscia [72] introduced a blockchain-based model for smart parking systems, where transactional information regarding parking fees was stored securely in the blockchain. Pham et al. [73] introduced an algorithm that improved the effectiveness of cloud-based smart parking methods using IoT technology. Yuan and Wang [74] proposed a seven-layered blockchain-based Intelligent Transport System (ITS) that integrated advanced technologies to enhance the overall efficiency of transportation systems. The system aimed to optimize transportation systems by ensuring efficiency, safety, speed, convenience, cost-effectiveness, profitability, and connectivity. Rahman et al. [66] presented a blockchain framework

TABLE 5. Comparative analysis of current methodologies for smart city.

Author	Year	Objective	Pros	Cons
Fan et al. [64]	2018	Introduced a simulated environment based on BT for managing large-scale IoT data systems.	IoT data management in a smart city.	The framework needed to be explained in detail.
Habibzadeh et al. [65]	2019	Performed a survey on security and policy issues for the IoT systems deployed in the smart city.	Visualized a smart city as a multi-level system having a certain security level.	Technical and policy difficulties for a secure smart city should be investigated further.
Rahman et al. [66]	2019	A blockchain-based model is proposed to preserve security and privacy in smart city applications.	Smart contracts were employed to facilitate decentralized messaging services.	Does not investigate 6G networks.
Malik et al. [67]	2019	Introduced an original framework for examining the patterns of users' physical activity within a compact urban setting	The suggested approach has the potential to verify a user's identity passively.	Does not investigate 6G enabled IoT networks
Khan et al. [68]	2020	Devised a Blockchain-driven system to authenticate data from CCTV cameras in smart cities.	The suggested approach creates a blockchain interface between CCTV nodes and users.	It does not include a 6G-based solution.
Esposito et al. [69]	2021	Leveraged BT to address authentication and authorization challenges in smart city applications.	A proposed solution utilizes BT to store security rules within the system and integrate it with the FIWARE platform.	Does not include a solution based on 6G.
Asif et al. [70]	2022	Proposed a robust and dependable authentication and trust management mechanism tailored for smart cities.	The strategy improved safety performance.	Does not investigate 6G networks.

for maintaining secure and privacy-oriented smart contract assistance in IoT-enabled cooperative markets, particularly emphasizing applications within smart cities. Malik et al. [67] developed a framework for analyzing users' physical activity patterns in a small city environment, which could be utilized for passive user authentication. Esposito et al. [69] explored the application of BT for authentication and authorization in smart city applications. Asif et al. [70] also proposed a secure and reliable authentication and trust management mechanism in smart cities.

The studies highlighted that integrating BT with IoT devices has revolutionized various aspects of smart cities. The deployment of IoT sensors and devices in road infrastructure, vehicles, and parking areas has enabled the collection of crucial data on traffic flow, parking availability, and congestion. When stored on a blockchain, this data ensures its integrity and provides a reliable platform for authorities to analyze and optimize traffic management strategies. Furthermore, IoT devices have played a pivotal role in monitoring and collecting real-time data on energy consumption within smart cities. A decentralized energy management system has been established through the integration with BT, allowing for automatic and transparent energy trading. This has led to optimized energy distribution and reduced waste.

C. SMART AGRICULTURE

Smart agriculture is an innovative approach to farming that reduces human effort and maximizes available resources. It can address workforce shortages, enhance agricultural resilience, and support small farmers through advanced technology. Traditional agriculture can be more intelligent using sensors, gateways, cloud servers, and mobile or computer platforms. Farmers often face unpredictable weather conditions that can impact crop survival. Installing agricultural weather stations on farms helps generate crucial data like temperature, rainfall, wind speed, atmospheric pressure, etc. This data is recorded and stored securely in the blockchain, providing transparent access to farmers. IoT technology and blockchain integration enable the monitoring soil quality, pests, irrigation, and other factors using specialized devices. BT enhances various farm operations, fostering a trusted and ecologically intelligent agriculture system. It improves food safety through traceability and can be utilized in tracking food supply chains.

Thejaswini and Ranjitha [91] recommended using decentralized applications to tackle agricultural challenges. Vangala et al. [92] proposed employing smart contracts and BT to support smart agriculture. Caro et al. [93] introduced AgriBlockIoT, a proposal for integrating a vast array of IoT devices to automate smart contract implementation, ensuring transparency and immutable data storage. Nagpure et al. [94] utilized IoT to monitor water systems, including temperature and soil moisture, and analyzed sensor data to make informed decisions regarding irrigation. Giordano et al. [76] introduced an IoT application for protecting crops, utilizing an ultrasound-repellent system to prevent damage caused by animals. Iqbal and Butt [95] discussed the application of IoT and BT in precision agriculture, specifically in tracking

TABLE 6. Comparative analysis of current methodologies for smart agriculture.

Author	Year	Objective	Pros	Cons
Encinas et al. [75]	2017	Collect data on aquatic organism reproduction to better understand the factors that influence production, avoid environmental disasters, and optimize pond care resources.	Checks water quality using IoT and WSN.	Security and privacy issues.
Giordano et al. [76]	2018	To address potential farming damage caused by wild animal attacks and adverse climate conditions, a robust defense and repelling system was designed.	The proposed system does no physical or biological harm to animals and makes no audible noise to people.	Security and privacy issues.
Pathak et.al [77]	2019	The suggested system uses an IoT platform to monitor several factors such as pH, humidity, etc. The information is collected via sensors and transmitted to the machine through Arduino.	Under climate change circumstances, the proposed system manages water resources and allocates water for crops.	Does not comprise Blockchain and 6G solution.
Bai et al. [78]	2021	To control data security and integrity, a green supply chain architecture based on a non-cooperative game was proposed.	Ensures the accuracy of data given by various sensors.	Does not include a solution based on a 6G network.
Zeng et al. [79]	2021	Using IoT and blockchain technologies, an advanced seed quality monitoring and water management system was developed.	A smart water management system based on IoT was developed.	Does not include a solution based on Blockchain and 6G.
Chaganti et al. [80]	2022	To monitor devices and detect sensor irregularities, a cloud-based smart-farm surveillance system was presented.	Implemented the smart farm security monitoring framework prototype.	The IoT gateway was not implemented.
Algarni et al. [81]	2022	The system includes an asymmetric key exchange technique based on an ECC authentication algorithm and SHA-256 hash function cryptography to provide safe communication between sensors and drones in the agricultural sector.	A secure blockchain-based architecture is proposed to build trust among smart farming users.	It is difficult to verify a user's identity.
Zeeshan et al. [82]	2023	A theoretical multilayered architecture for the food supply chain was proposed in order to automate and digitize intra- and inter-organizational operations in the agricultural food supply chain.	The health and environment of a product may be tracked throughout the supply chain using blockchain, smart contracts, and IoT.	Privacy and interoperability issues.
Encinas et al. [75]	2017	Collect data on aquatic organism reproduction to better understand the factors influencing production, avoid environmental disasters, and optimize pond care resources.	Checks water quality using IoT and WSN.	Security and privacy issues.
Giordano et al. [76]	2018	A robust defense and repelling system was designed to address potential farming damage caused by wild animal attacks and adverse climate conditions.	The proposed system does no physical or biological harm to animals and makes no audible noise to people.	Security and privacy issues.
Pathak et.al [77]	2019	The suggested system uses an IoT platform to monitor factors such as pH, humidity, etc. The information is collected via sensors and transmitted to the machine through Arduino.	Under climate change, the proposed system manages water resources and allocates water for crops.	Does not comprise Blockchain and 6G solution.
Bai et al. [78]	2021	To control data security and integrity, a green supply chain architecture based on a non-cooperative game was proposed.	Ensures the accuracy of data given by various sensors.	Does not include a solution based on a 6G network.
Zeng et al. [79]	2021	An advanced seed quality monitoring and water management system was developed using IoT and blockchain technologies.	A smart water management system based on IoT was developed.	Does not include a solution based on Blockchain and 6G.
Chaganti et al. [80]	2022	A cloud-based smart-farm surveillance system was presented to monitor devices and detect sensor irregularities.	Implemented the smart farm security monitoring framework prototype.	The IoT gateway was not implemented.
Algarni et al. [81]	2022	The system includes an asymmetric key exchange technique based on an ECC authentication algorithm and SHA-256 hash function cryptography to provide safe communication between sensors and drones in the agricultural sector.	A secure blockchain-based architecture is proposed to build trust among smart farming users.	It isn't easy to verify a user's identity.
Zeeshan et al. [82]	2023	A theoretical multilayered architecture for the food supply chain was proposed to automate and digitize intra- and inter-organizational operations in the agricultural food supply chain.	The health and environment of a product may be tracked throughout the supply chain using Blockchain, smart contracts, and IoT.	Privacy and interoperability issues.

animal attacks through a Repelling and Notifying System. Osmanoglu et al. [96] proposed a blockchain-based solution to improve the estimation of agricultural yields. Bai et al. [78] developed a sustainable supply chain framework that utilized blockchain to ensure data security and integrity. Chaganti et al. [80] presented a monitoring framework for smart farm security, enabled by cloud technology, which can detect device status and sensor anomalies and mitigate security threats. Alqarni et al. [81] suggested a safe blockchain-based architecture to build trust among users in

smart farming. Zeng et al. [79] developed a system based on IoT and blockchain to monitor seed quality and effectively manage water resources in communities.

The studies mentioned emphasize the significant potential of integrating BT and IoT applications to address agricultural challenges and bring about a transformative impact on smart farming. The collaborative integration of IoT and BT has played a pivotal role in promoting more efficient and sustainable agricultural practices. These advancements not only hold the promise of enhancing productivity but also play a crucial role in fostering trust among users in the field of smart farming. Moreover, the application of IoT in monitoring water systems has illustrated the capacity for automation, transparency, and secure data storage in agricultural operations. Additionally, innovations like ultrasound-repellent systems and precision agriculture techniques have provided novel means to safeguard crops and monitor potential threats effectively.

D. AUTONOMOUS VEHICLES

Automobile manufacturers are actively exploring the advantages of integrating Blockchain and IoT technologies into the automotive industry, particularly in autonomous vehicles and systems. The aim is to enhance their products, improve customer satisfaction, and provide valuable experiences. Autonomous vehicles offer numerous benefits to both vehicle owners and car companies. They can operate without human intervention, reducing human errors and accidents while saving drivers time. This time can be utilized for more productive activities such as sleeping, reading, eating, or relaxing. Additionally, autonomous vehicles can navigate independently to refuel or recharge at electric stations.

However, despite these advantages, autonomous vehicles also pose certain risks. Their communication relies on a centralized vehicular network called VANET, which is susceptible to cyber-attacks. Such attacks can lead to data loss and road accidents. To address these concerns, BT can be implemented in autonomous vehicles in various ways. Vehicle sensor data, for example, may be safely stored on the blockchain, allowing all users to track and exchange safety information. This implementation ensures that car owners use their vehicles responsibly. By leveraging blockchain's transparency and data security, telematics can facilitate secure data dissemination and collaboration across several self-driving vehicles, regional authorities, and public facilities. Lu et al. [102] proposed a privacy-preserving solution for message confidentiality within a vehicular network by introducing a blockchain-based anonymous reputation system. Similarly, Yang et al. [86] presented the idea of a proof-of-event consensus mechanism based on BT in vehicular networks, aiming to uphold data integrity. Oham et al. [88] employed a permissioned blockchain approach to enhance the security of smart vehicles. Their technique involved a challenge-response data exchange mechanism between roadside units and vehicles, enabling monitoring of the vehicle's internal state and detecting any malicious activity in the network.

The studies highlighted that integrating blockchain with IoT can be crucial in preventing and predicting equipment failures in manufacturing plants. Using equipment sensors to detect abnormal conditions such as excessive vibration or heat can identify potential failures or operator injuries. Critical threshold data collected by these sensors can be recorded on the blockchain, enabling the detection of failure trends and enabling proactive maintenance and repairs before catastrophic breakdowns occur. Data analytics and cognitive information collected from manufacturing floor devices give precise insights into asset performance to reliability, maintenance, and operational personnel. Equipment information stored on the blockchain may be accessed by regulators and providers, permitting prompt inspections and certifications to assure equipment trustworthiness. Third-party repair partners may use the blockchain to track and record preventative maintenance decisions transparently.

E. SMART SUPPLY CHAIN MANAGEMENT

Supply chain management (SCM) is a sophisticated and intricate system involving many entities, including manufacturers, suppliers, distributors, and retailers. The primary goal of SCM is to ensure the efficient fulfillment of customer orders while maximizing customer value. Integrating 6G-enabled Internet of Things (IoT) technology into SCM offers numerous benefits. These advantages encompass the ability to instantaneously track and authenticate items and shipments, continuously monitor storage surroundings like moisture and temperature, and make necessary adjustments to meet specific requirements. These advancements have the potential to improve overall supply chain management significantly. To address these opportunities, Arumugam et al. [103] proposed an innovative logistics system that incorporates freight planners, intelligent contracts, and asset condition tracking within the domain of SCM. When combined with IoT, BT can allow various application cases to improve supply-chain confidence and transparency. IoT and Blockchain technologies, when coupled, can enhance the effectiveness and productivity of existing supply chains.

In their research, Wamba and Queiroz [104] found that implementing BT has significantly enhanced various aspects of SCM. These improvements include increased transparency and seamless information sharing among supply chain members, enhanced accountability, reduced uncertainty, strengthened trust and security, and improved fraud prevention and process confidence. By leveraging blockchain, the supply chain can efficiently store and transmit data to other parties, such as suppliers and customers. Additionally, it allows for verifying data received by comparing it with information from other nodes or external sources. According to the study by Senyo et al. [105], blockchain enables the digital linkage of information to each unique product in the supply chain. This creates a comprehensive digital record demonstrating

TABLE 7. Comparative analysis of current methodologies for autonomous vehicles.

Author	Year	Objective	Pros	Cons
Kuzmin et al. [83]	2018	Presented the idea of blockchain in unnamed aerial vehicles.	Each automotive device was considered an autonomous node, allowing it to read and create transactions on the blockchain network effectively.	Information Security and Air Traffic.
Buzachis et al. [84]	2018	A Multi-Agent AIM (MA-AIM) system that communicates from vehicle to intersection and vice versa was proposed to safely manage vehicles crossing intersections by exploiting Blockchain capacities.	Used for verifying, negotiating, and facilitating among the consent entities.	Not well suited for 6G communications.
Shivers et al. [85]	2019	A framework for a decentralized ride-hailing network has been proposed.	The proposed framework was utilized in AVs to improve ride quality.	The problem of authentication and centralization.
Yang et al. [86]	2019	The concept of proof-of-event consensus based on blockchain was proposed to assure data integrity in in-vehicle networks.	When compared to the PoW technique, the proposed PoE solution can save a significant amount of power.	Not well suited to various types and formats of data originating from various sources.
Pokhrel and Choi [87]	2020	A blockchain-based concept for AVs has been proposed.	Federated Learning is used to protect data privacy while enhancing the efficiency of vehicular communication.	Not much suitable for 6G connectivity.
Oham et al. [88]	2021	To protect smart vehicles, a permissioned blockchain was used.	This system employs a challenge-response data exchange mechanism between roadside devices and automobiles to monitor internal vehicle conditions and detect malicious activities in the network.	Not well suited to 6G communication.
Yang et al. [89]	2021	A conceptual framework enabling the complete classification of underwater autonomous vehicles was presented.	This framework may be utilized for choosing communication-related formations for many applications.	Problems with security.
Haigen Min et al. [90]	2023	A framework is proposed to diagnose defects in autonomous vehicles equipped with sensor self-diagnosis.	This framework uses a residual consistency checking technique to detect and isolate faulty sensors within the self-diagnostic system by effectively leveraging sensor redundancy.	Security concerns

the product's provenance, compliance, authenticity, and overall quality. This valuable information is accessible to all stakeholders involved and remains associated with the product throughout its entire journey in the supply chain.

In summary, the integration of BT and IoT has emerged as a pivotal catalyst in elevating different facets of SCM. Extensive research underscores the significant advantages of leveraging smart SCM. These encompass heightened transparency, effortless information exchange, bolstered accountability, diminished uncertainty, reinforced trust and security, and heightened proficiency in preventing fraud and ensuring process integrity. Moreover, blockchain facilitates creating a digital connection for every unique product within the supply chain, establishing a thorough digital record that confirms the product's origin, adherence to standards, genuineness, and overall quality.

VI. CASE STUDY: SMART SUPPLY CHAIN

This section explores the case study of smart supply chain within the realm of industry automation. The motivation behind selecting this case study lies in its potential to revolutionize businesses across various sectors. The integration of automation, data-informed decision-making, and seamless connectivity not only assures heightened efficiency but also bolsters resilience, elevates customer satisfaction, and fosters a competitive advantage. Many industrial automation systems heavily rely on external vendors for their hardware, software, and components. Vulnerabilities within any part of this supply chain could be exploited, putting the entire system at risk. In today's increasingly digital landscape, supply chains rely heavily on electronic communication and data management systems. Security breaches, including theft, cyber-attacks, or even natural disasters, can potentially

TABLE 8. Comparative analysis of current methodologies for smart supply chain management.

Author	Year	Objective	Pros	Cons
Caro et al [93]	2018	Developed a traceability system for the agricultural supply chain, utilizing BT.	Utilized IoT sensors integrated into the entire supply chain to record and store data on the blockchain directly.	The system may need to address privacy protection and regulator settings to ensure compliance and safeguard sensitive information.
Wu et al. [97]	2019	Presented a solution for enhancing traceability in the food supply chain.	This proposed system grants customers, members, and regulators distinct access rights, effectively managed by smart contracts.	It is unsuitable for Complex supply chains with relatively large amounts of data.
Zhang et al. [98]	2020	Proposed a grain supply chain traceability system.	The BT and coding at each link allowed for highly efficient tracking and tracing of product information.	Issues in trusted data collection and the credibility of data.
Yang et al. [99]	2021	Created a robust blockchain-based traceability system specifically tailored for fruits and vegetables.	To optimize blockchain storage and protect privacy, the information uploaded by members is categorized as public or private.	Costly
Subramanian et al. [100]	2021	Designed a system for the Pharma supply chain based on blockchain.	Introduces the concept of crypto medicine, which is using crypto money in selling and purchasing pharmaceuticals.	The proposed system is not cost-effective.
Cocco et al. [101]	2021	Develop a blockchain-based system for managing the supply chain of packaged agricultural products.	Sensor-equipped nodes immediately convey their data to Raspberry Pi units, which elaborate and transfer it to the Interplanetary File System and the Ethereum Blockchain.	Scalability.

disrupt the supply chain's flow. This can lead to delays in the delivery of products and services, ultimately impacting customer satisfaction and revenue. Security issues may also open the door to introducing counterfeit or substandard goods into the supply chain. Theft or tampering with goods in transit can result in an inventory loss, causing a direct financial hit and potential shortages, stockouts, and delays in fulfilling customer orders. Therefore, it is imperative to prioritize security and privacy throughout the supply chain to mitigate these risks. The combination of AI, blockchain, and 6G networks establishes a powerful environment. AI boosts security through the analysis of 6G network traffic, optimizes blockchain transactions by intelligently allocating resources, and adjusts settings in real-time for smooth processing. It anticipates and averts network problems, ensuring resilience. This collaboration fosters innovation across various industries.

In this case study, we delve into the amalgamation of blockchain and 6G network technologies to strengthen industrial automation and intelligent supply chain management. The objective is to showcase the potential of these technologies in enhancing efficiency, transparency, and security throughout different stages of the supply chain. In this case study, we have selected an SCM dataset from a manufacturing company specializing in electronic devices, including smartphones and tablets. This company procures raw materials and components from various suppliers worldwide. Their primary objectives are to optimize supply chain operations, enhance production efficiency, and establish a robust system for verifying the authenticity and traceability of their products.

A. PROBLEM STATEMENT

Let's consider a scenario where we have a number of manufacturing companies, denoted as 'n', and a variety of product types produced by these companies denoted as 'm'. We can represent the manufacturing companies as the set

$$C = c_1, c_2, \ldots, c_n$$

and the set of product types as

$$M = m_1, m_2, \ldots, m_m.$$

Each manufacturing company c_i produces a specific subset of product types from the set 'M.' Additionally, we have a number of distributors, denoted as 'k,' who receive products from these manufacturing companies. The set of distributors is represented as

$$D = d_1, d_2, \ldots, d_k.$$

Each distributor d_j receives products from a subset of the manufacturing companies. Let w be the number of wholesalers that receive products from the distributors. We can represent the set of wholesalers as

$$W = w_1, w_2, \ldots, w_w.$$

Just like the distributors, each wholesaler w_i receives products from a subset of the distributors. However, it's worth noting that due to the lack of proper regulation and monitoring, there's a probability that some products may be counterfeit and fail to meet the required quality standards.

To address this issue, when a manufacturing company produces a new product, it assigns a unique Barcode or QR code to it. This code enables individual product identification and tracking at any point within the supply chain network. The products are sealed in containers equipped with sensors to ensure their integrity. These sensors, including a biosensor for monitoring the product's biological content, a temperature sensor to check temperature, and GPS sensors for tracking logistics during shipment, are integrated and linked to the QR code. In the context of smart transportation, where various smart sensors are represented as $\{s_1, s_2, s_3, \ldots, s_n\} \in S$, we gather sensor data to monitor various environmental conditions like temperature and humidity throughout the product's journey.

Let $\Psi(p, t)$ denote the sensor data collected for product p at time t. However, concerns may arise regarding the consistency and accuracy of this sensor data. These concerns can be expressed as:

$$\exists p, t : \Psi'(p, t) \tag{1}$$

where $\Psi'(p, t)$ is unreliable or inaccurate sensor data. The sensor (s_i) also employs a network interface to transmit data. This network is susceptible to various network-related attacks, including session hijacking, data integrity breaches, malware, and DDoS, potentially compromising the system's performance. An attacker ($) may exploit the communication channel C and tamper with sensor data.

$$\$ \xrightarrow{\text{exploits}} C \xrightarrow{\text{manipulates}\Psi(p,t)} \Psi'(p, t) \tag{2}$$

Furthermore, $ can introduce a sensor node within the system, denoted as $\$_{sk}$. This node functions as an intermediary, allowing for manipulation of the data exchange $\Psi(p, t)$.

$$\$_{sk} \xrightarrow{\text{manipulates}} \Psi(p, t) \rightarrow \Psi'(p, t) \tag{3}$$

Another significant challenge is effectively handling incidents involving contamination, adulteration, or safety concerns. We can express these challenges as:

$$\exists p \in P : \neg £(p) \tag{4}$$

where $£(p)$ signifies the mechanism for handling incidents involving product p.

These challenges underscore the critical need for improved product traceability and reduced transmission delays, emphasizing the importance of robust solutions.

The primary objective of this work is to establish a secure data exchange system among stakeholders and implement intelligent tracking mechanisms for this data. To achieve this objective, an objective function OB is defined as,

$$OB = \sum_{\text{MAX(secure)}} \Psi(p, t) + \text{Smart Tracing} \tag{5}$$

TABLE 9. Comparative analysis of accuracy and recall.

Model	Accuracy	Recall
SVM	98.27	96.93
Random forest	99.99	98.99
Perceptron	95.94	96.10
LDA	96.20	96.25
Logistic Regression	98.24	96.93
Gaussian Naive Bayes	94.58	91.21

B. DATA ANALYSIS

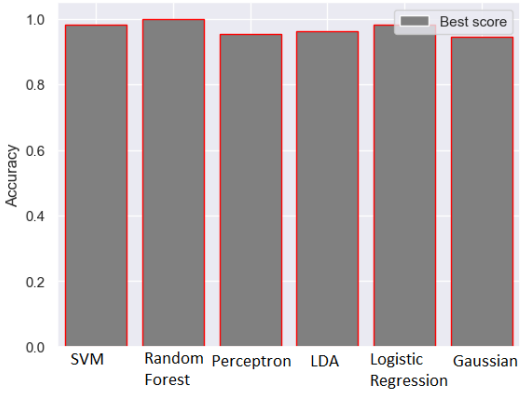
Analyzing the company's supply chain data can enhance its operational efficiency and streamline its processes. By identifying patterns and trends in past shipment data, the supply chain can make informed predictions about future requirements, prevent disruptions and stock shortages, and improve inventory management. Supply chains can optimize their routes, schedules, and performance tracking by utilizing data analytics, leading to overall improvements.

A significant aspect of this analysis involves the "late delivery" parameter, a metric indicating the frequency or percentage of deliveries that do not meet their scheduled timelines. This parameter measures how often goods or products are delivered after their expected delivery dates. Understanding the late delivery parameter offers valuable insights into the supply chain's efficiency, reliability, and overall performance. By addressing and mitigating late deliveries, companies can elevate customer satisfaction, reduce costs, and strengthen their competitive edge in the market.

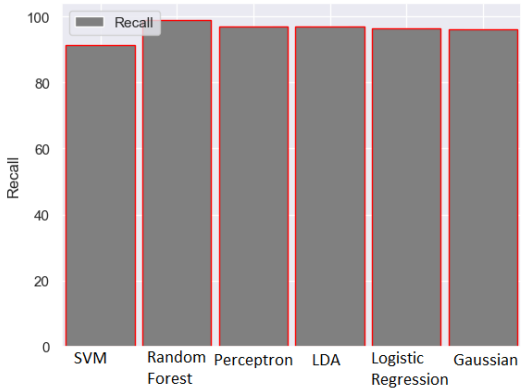
The dataset includes a column called "Late Delivery" with values of 0 and 1, where 1 indicates a delayed order, while 0 means no delay. Based on the data, the average of this feature is calculated to be 0.658. This suggests that the number of uncertainties is relatively high, which can have negative consequences such as customer loss and a subsequent decline in profits. This study employed various classification models to predict "Late Delivery" using accuracy, recall, and F1 score metrics. The models utilized include Support Vector Machines, Gaussian Naive Bayes, Logistic Regression, Linear Discriminant Analysis, Perceptron, and Random Forest classification.

Explanation of Metrics:

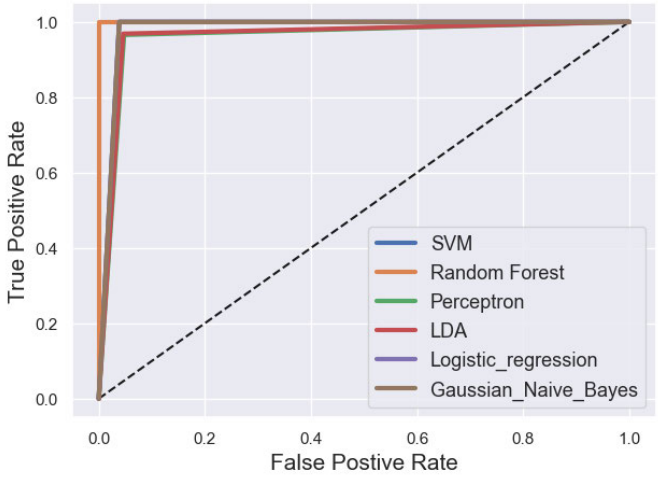
1) True Positive (TP): This refers to the cases where the model accurately predicts that "Late Delivery" will happen. This prediction is valuable for the company's supply chain, as it allows them to prepare in advance and mitigate the potential impact of delays.
2) True Negative (TN): This indicates the instances where the model correctly predicts that "Late Delivery" will not occur. It demonstrates the model's ability to make accurate predictions for on-time deliveries.



(a) Accuracy comparison.



(b) Recall comparison.



(c) ROC-AUC curve

FIGURE 10. **Comparison of ML classifiers on different evaluation metrics.**

3) False Positive (FP): This represents the situations where the model incorrectly predicts that "Late Delivery" will occur, while it won't. Such predictions may lead to allocating unnecessary resources, resulting in resource wastage.
4) False Negative (FN): This corresponds to the cases where the model incorrectly predicts that "Late Delivery" will not occur, even though it actually will. This outcome is desirable since it means the model needs to identify potential late deliveries, leading to unpreparedness and potential disruptions in the supply chain.

The performance of the models is assessed using three main metrics: accuracy, recall, and F1 score. Accuracy measures the ratio of correct predictions to the total number of samples analyzed. It provides a valuable measure of how well a classifier correctly identifies and categorizes instances within the dataset. Recall signifies the ratio of correct optimistic predictions to the total positive instances in the dataset. Precision is a metric that evaluates the ability of a system to correctly identify positive samples compared to the total positive samples it predicts. When improved precision improves, the proposed system can generate a more significant number of genuine warnings or positive outcomes, enhancing its effectiveness in correctly identifying relevant instances. The F1 score is computed as follows:

$$F1 - score = \frac{2 * (precision * recall)}{(precision + recall)} \tag{6}$$

The F1 score integrates precision and recall within a single metric, utilizing their harmonic mean. The tests conducted with various classifiers display their performance in Figure 10. The accuracy chart shown in Figure 10a visually compares how well each machine learning classifier performed. By looking at the accuracy values on the chart, we can observe that the random forest classifier achieved the highest accuracy, followed by SVM and Logistic Regression. On the other hand, the perceptron, LDA, and Gaussian Naive Bayes classifiers had lower accuracies in comparison. Figure 10b shows the Recall value chart. Looking at these values on the chart, we can observe that the random forest classifier achieved the highest value, followed by SVM and Logistic Regression. On the other hand, the perceptron, LDA, and Gaussian Naive Bayes classifiers had lower Recall values in comparison.

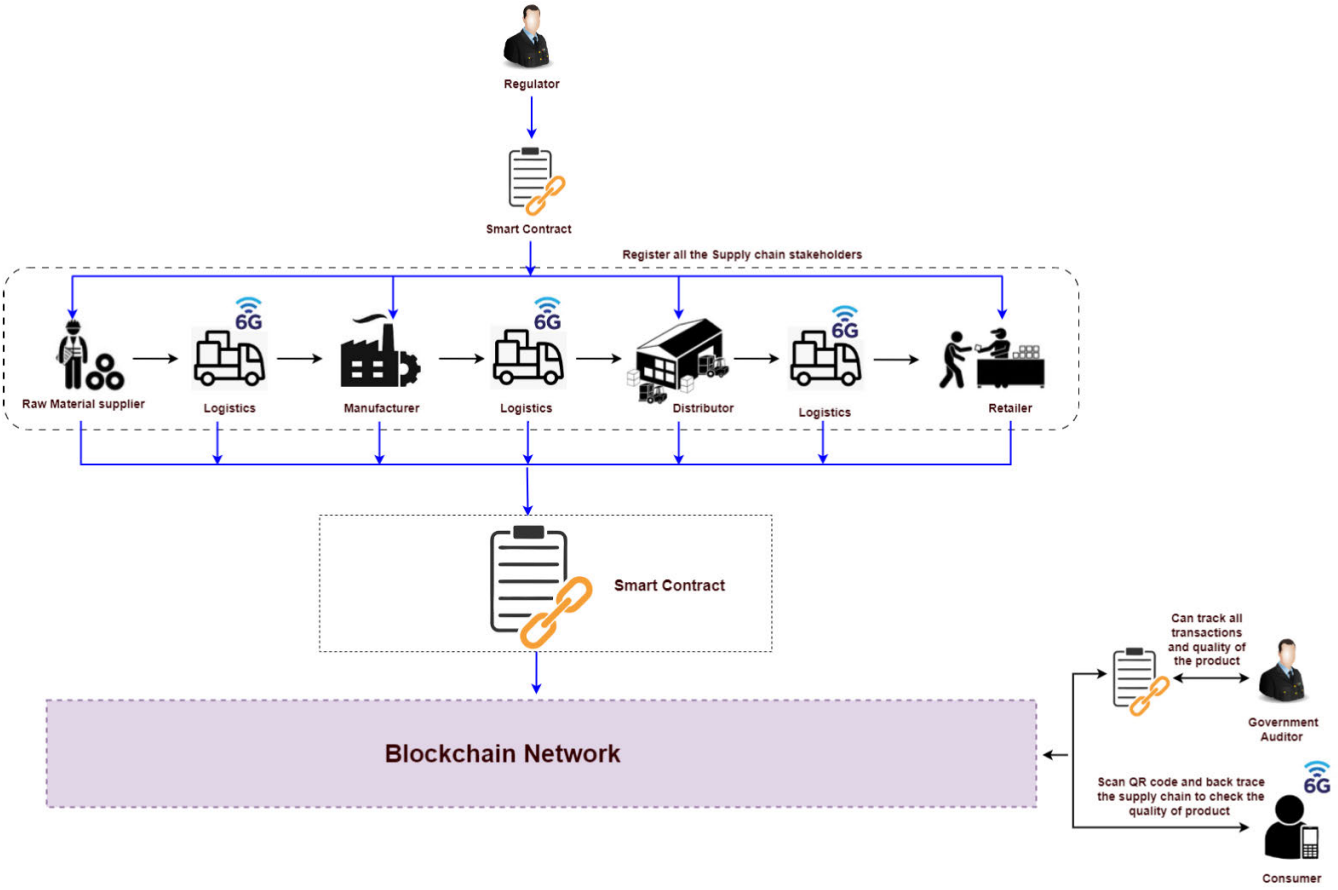


FIGURE 11. Supply chain management using blockchain and 6G-Enabled IoT devices.

In Figure 10c, we have the Receiver Operating Characteristic (ROC) curve, which compares the TP to the FP at different threshold values. The ROC curve's area under the curve (AUC) reflects the classifier's performance. Observing the ROC curves shows that the random forest classifier has the highest AUC, indicating it has the best overall performance among all the classifiers. Table 9 shows the comparative analysis of different classifiers.

C. IMPLEMENTATION

For industry automation, this manufacturing unit will be well-equipped with state-of-the-art automation systems, IoT devices, and robotics, ensuring smooth and efficient production processes. Leveraging the power of the 6G network, the facility benefits from ultra-high-speed and low-latency connectivity, allowing seamless real-time communication between machines, IoT sensors, and control systems. The company will implement a blockchain-based system to manage its supply chain efficiently. Various supply chain processes such as procurement, order tracking, quality control, and payment settlement are automated using smart contracts. Crucial supply chain data, including order details, shipment information, and production status, is securely recorded on the blockchain, guaranteeing transparency and preserving the integrity of the data. Combining these technologies brings significant advantages to the supply chain, making it more transparent, efficient, and trustworthy. Here are some key benefits:

1) Component Tracking and Tracing: Every component and raw material used in production is given a unique identifier or RFID tag linked to the blockchain. This allows real-time tracking and tracing throughout the supply chain, ensuring authenticity and quality control.
2) Real-Time Inventory Management: Thanks to the 6G network, inventory levels are constantly monitored at different supply chain stages. As components and finished products move through the chain, inventory data is updated on the blockchain, optimizing stock levels and reducing the risk of shortages or excess inventory.
3) Secure Data Exchange and Collaboration: Blockchain and 6G technology enable secure data exchange and collaboration between supply chain stakeholders, such as suppliers, manufacturers, logistics providers, and customers. Sensitive information is protected through cryptographic mechanisms, ensuring data privacy and security.

4) Anti-Counterfeiting Measures: BT helps combat product counterfeiting by recording product information on the blockchain, including serial numbers and manufacturing details. This allows customers and retailers to verify product authenticity before purchase.
5) Improved Supply Chain Efficiency and Cost Savings: Using blockchain and 6G technologies, the manufacturing company can optimize supply chain processes, reduce delays, and minimize manual interventions. This increases operational efficiency, shorter lead times, and cost savings.
6) Sustainability and Compliance: The transparent nature of the blockchain enables the company to trace the origin of raw materials and components, promoting sustainable and ethical sourcing practices. Additionally, auditable records on the blockchain ensure compliance with industry standards and regulations.

To commence, the initial step involves identifying the primary stakeholders within the logistics network, which encompasses manufacturers, suppliers, distributors, transporters, customs authorities, and customers. Assigning a distinct identity to each participant within the blockchain network is imperative, ensuring their unique presence and accountability. Following establishing participant identities, the subsequent phase involves assigning a unique identity number (ID) to every individual item or product within the IoT-based blockchain network. This step guarantees a comprehensive and reliable tracking mechanism for each item throughout its journey. Technologies like QR Codes, RFID trackers, and NFC Chips can be introduced to successfully implement the tracking and tracing mechanism. These IoT devices must have built-in confidentiality features, as the code generation follows the established blockchain protocol. As the items progress through the supply chain, they pass from one stakeholder to another until they eventually reach the end user. The blockchain service provider maintains an updated record of the item's journey, ensuring transparency and accountability at each process step.

The manufacturer can now send the item to the authorized distributor and update the blockchain database. The distributor scans the QR code and uses the smart contract to approve the drug by changing its status. Once approved, the distributor ships the item to the next authorized actor, which is the wholesaler. The wholesaler scans the QR code, authorizes the item, updates its status, and ships it to the retailer. The retailer scans the QR code with a special code, authorizes the item, and records customer details in the blockchain before selling the item to them. Consumers are not directly involved in blockchain transactions, but they can verify the authenticity of an item by scanning the QR code on its container. When consumers scan the QR code, they will be directed to a webpage that interacts with the smart contract. Fig 11 shows the Blockchain and IoT-based Secure supply chain management system.

While the amalgamation of blockchain and 6G presents advantages like heightened security, transparency, and decentralized control for industrial automation, addressing concerns regarding the potential supplementary costs in computation and storage is crucial. The subsequent section delves into the primary challenges of integrating blockchain and 6G-enabled IoT for industrial automation.

VII. CHALLENGES IN INTEGRATING BLOCKCHAIN AND 6G-ENABLED IOT FOR INDUSTRIAL AUTOMATION

The combination of BT and the 6G-enabled IoT holds great potential for enhancing industrial automation systems. Blockchain provides decentralized and transparent data management, while 6G-enabled IoT offers ultra-fast and low-latency communication capabilities. However, integrating these technologies successfully poses a unique set of challenges that must be overcome to fully utilize their benefits in industrial automation.

1) Scalability: One of the main obstacles is scalability. BT, known for its distributed ledger system, requires substantial computational power and storage resources. When combined with the large data generated by 6G-enabled IoT devices in an industrial automation environment, scalability becomes a more pressing issue. Addressing this challenge involves developing solutions capable of handling the increasing transaction volume and data throughput without sacrificing performance.
2) Latency and Real-Time Processing: Real-time data processing and decision-making are crucial in industrial automation. Although 6G-enabled IoT networks offer ultra-low latency, integrating BT introduces additional processing time due to consensus mechanisms and validation processes. This can impede real-time capabilities. Overcoming this challenge requires the design of efficient consensus algorithms and optimizing blockchain protocols to minimize latency and ensure the timely execution of industrial automation tasks.
3) Security and Privacy: BT is renowned for its security features, including data integrity and transparency. However, integrating 6G-enabled IoT devices brings forth new security and privacy challenges. Industrial automation systems handle sensitive data and require strict access controls and secure communication channels. Balancing the confidentiality of data transmitted between IoT devices and blockchain networks while maintaining the integrity and traceability provided by blockchain is a complex task. Robust encryption mechanisms, access management protocols, and privacy-enhancing technologies are crucial to address this challenge.
4) Interoperability and Standardization: The successful integration of blockchain and 6G-enabled IoT for industrial automation relies on achieving

interoperability between different systems, protocols, and devices. Seamless communication, data exchange across diverse platforms, and compatibility between blockchain implementations and IoT devices are vital. Establishing industry-wide standards and protocols that promote interoperability is essential to realize the full potential of this integration and foster collaboration between stakeholders.

5) Energy Efficiency: Industrial automation systems consist of numerous energy-consuming IoT devices. Integrating blockchain, which requires significant computational resources, can consume additional energy. Ensuring energy efficiency is critical for sustainable blockchain and 6G-enabled IoT deployment in industrial settings. Exploring energy-efficient consensus algorithms, optimizing resource utilization, and leveraging technologies like edge computing can help mitigate this challenge.

VIII. CONCLUSION

Integrating BT and 6G-enabled IoT holds great potential for transforming industrial automation. This work highlighted the benefits and challenges associated with combining these advanced technologies. Blockchain offers decentralized data management, while 6G-enabled IoT provides fast communication. Together, they enhance efficiency, security, and scalability in industrial automation. However, addressing scalability, latency, security, interoperability, and energy efficiency is crucial for maximizing these benefits. Robust systems, efficient algorithms, encryption, and industry-wide standards are needed to overcome these challenges. Energy-efficient algorithms and edge computing can minimize additional energy consumption for sustainable deployment. Integrating blockchain and 6G-enabled IoT presents an exciting opportunity for industrial automation.

In the future, we plan to transform these concepts into practical implementations, potentially reshaping how industries operate in the era of 6G and Blockchain. Therefore, our future endeavors will focus on creating personalized solutions for sectors like supply chain management, smart manufacturing, energy grid management, and healthcare. Additionally, we will explore the integration of edge computing with blockchain and 6G networks to facilitate real-time data processing and decision-making at the edge. This advancement would lead to reduced latency and improved responsiveness in industrial applications.

REFERENCES

[1] 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.

[2] M. Z. Chowdhury, Md. Shahjalal, S. Ahmed, and Y. M. Jang, "6G wireless communication systems: Applications, requirements, technologies, challenges, and research directions," *IEEE Open J. Commun. Soc.*, vol. 1, pp. 957–975, 2020.

[3] L.-H. Shen, K.-T. Feng, and L. Hanzo, "Five facets of 6G: Research challenges and opportunities," *ACM Comput. Surv.*, vol. 55, no. 11, pp. 1–39, Nov. 2023.

[4] M. Mao and H. Xiao, "Blockchain-based technology for industrial control system CyperSecurity," in *Proc. Int. Conf. Netw., Commun., Comput. Eng. (NCCE)*, 2018, pp. 903–907.

[5] A. Dorri, M. Steger, S. S. Kanhere, and R. Jurdak, "BlockChain: A distributed solution to automotive security and privacy," *IEEE Commun. Mag.*, vol. 55, no. 12, pp. 119–125, Dec. 2017.

[6] G. Brown, P. Analyst, and H. Reading, "Ultra-reliable low-latency 5G for industrial automation," *Technol. Rep. Qualcomm*, vol. 2, Sep. 2018, Art. no. 52065394.

[7] X.-H. You, "Towards 6G wireless communication networks: Vision, enabling technologies, and new paradigm shifts," *Sci. China Inf. Sci.*, vol. 64, no. 1, pp. 1–74, Jan. 2021.

[8] V. Astarita, V. P. Giofrè, G. Mirabelli, and V. Solina, "A review of blockchain-based systems in transportation," *Information*, vol. 11, no. 1, p. 21, Dec. 2019.

[9] F. Hussain, S. A. Hassan, R. Hussain, and E. Hossain, "Machine learning for resource management in cellular and IoT networks: Potentials, current solutions, and open challenges," *IEEE Commun. Surveys Tuts.*, vol. 22, no. 2, pp. 1251–1275, 2nd Quart., 2020.

[10] G. Manogaran, M. Alazab, P. M. Shakeel, and C.-H. Hsu, "Blockchain assisted secure data sharing model for Internet of Things based smart industries," *IEEE Trans. Rel.*, vol. 71, no. 1, pp. 348–358, Mar. 2022.

[11] U. Hariharan and K. Rajkumar, "Background and research challenges for blockchain-driven 5G IoT-enabled industrial automation," in *Blockchain for 5G-Enabled IoT: The New Wave for Industrial Automation*. Cham, Switzerland: Springer, 2021, pp. 33–59.

[12] M. Javaid, A. Haleem, R. P. Singh, S. Khan, and R. Suman, "Blockchain technology applications for Industry 4.0: A literature-based review," *Blockchain, Res. Appl.*, vol. 2, no. 4, Dec. 2021, Art. no. 100027.

[13] M. H. Alsharif, A. H. Kelechi, M. A. Albreem, S. A. Chaudhry, M. S. Zia, and S. Kim, "Sixth generation (6G) wireless networks: Vision, research activities, challenges and potential solutions," *Symmetry*, vol. 12, no. 4, p. 676, Apr. 2020.

[14] Y. Zhao, G. Yu, and H. Xu, "6G mobile communication network: Vision, challenges and key technologies," 2019, *arXiv:1905.04983*.

[15] Y. Schuetz, P. Katarina, E. Leon, E. Manuel, and M. Moritz, "The automotive sector and blockchain," MHP Riddle Code, Austria, Joint White Paper, 2019.

[16] T. Nguyen, N. Tran, L. Loven, J. Partala, M.-T. Kechadi, and S. Pirttikangas, "Privacy-aware blockchain innovation for 6G: Challenges and opportunities," in *Proc. 2nd 6G Wireless Summit (6G SUMMIT)*, Mar. 2020, pp. 1–5.

[17] S. Yrjölä, "How could blockchain transform 6G towards open ecosystemic business models?" in *Proc. IEEE Int. Conf. Commun. Workshops (ICC Workshops)*, Jun. 2020, pp. 1–6.

[18] R. Sekaran, R. Patan, A. Raveendran, F. Al-Turjman, M. Ramachandran, and L. Mostarda, "Survival study on blockchain based 6G-enabled mobile edge computation for IoT automation," *IEEE Access*, vol. 8, pp. 143453–143463, 2020.

[19] H. Xu, P. V. Klaine, O. Onireti, B. Cao, M. Imran, and L. Zhang, "Blockchain-enabled resource management and sharing for 6G communications," *Digit. Commun. Netw.*, vol. 6, no. 3, pp. 261–269, Aug. 2020.

[20] T. Hewa, G. Gur, A. Kalla, M. Ylianttila, A. Bracken, and M. Liyanage, "The role of blockchain in 6G: Challenges, opportunities and research directions," in *Proc. 2nd 6G Wireless Summit (6G SUMMIT)*, Mar. 2020, pp. 1–5.

[21] Y. Lu, "Industry 4.0: A survey on technologies, applications and open research issues," *J. Ind. Inf. Integr.*, vol. 6, pp. 1–10, Jun. 2017.

[22] C. Zhang and Y. Chen, "A review of research relevant to the emerging industry trends: Industry 4.0, IoT, blockchain, and business analytics," *J. Ind. Integr. Manage.*, vol. 5, no. 1, pp. 165–180, Mar. 2020.

[23] L. D. Xu, "Industry 4.0-frontiers of fourth industrial revolution," *Syst. Res. Behav. Sci.*, vol. 37, no. 4, pp. 531–534, 2020.

[24] K. A. Demir, G. Döven, and B. Sezen, "Industry 5.0 and human-robot co-working," *Proc. Comput. Sci.*, vol. 158, pp. 688–695, Jan. 2019.

[25] P. M. Rao and B. D. Deebak, "Security and privacy issues in smart cities/industries: Technologies, applications, and challenges," *J. Ambient Intell. Humanized Comput.*, vol. 14, no. 8, pp. 10517–10553, Aug. 2023.

[26] A.-R. Sadeghi, C. Wachsmann, and M. Waidner, "Security and privacy challenges in industrial Internet of Things," in *Proc. 52nd ACM/EDAC/IEEE Design Autom. Conf. (DAC)*, Jun. 2015, pp. 1–6.

[27] H. Türkmen, M. S. J. Solaija, A. Tusha, and H. Arslan, "Wireless sensing—Enabler of future wireless technologies," *TURKISH J. Electr. Eng. Comput. Sci.*, vol. 29, no. 1, pp. 1–17, Jan. 2021.

[28] E. Balandina, S. Balandin, Y. Koucheryavy, and D. Mouromtsev, "IoT use cases in healthcare and tourism," in *Proc. IEEE 17th Conf. Bus. Informat.*, vol. 2, Jul. 2015, pp. 37–44.

[29] S. Chaudjary, R. Kakkar, R. Gupta, S. Tanwar, S. Agrawal, and R. Sharma, "Blockchain and federated learning-based security solutions for telesurgery system: A comprehensive review," *Turkish J. Electr. Eng. Comput. Sci.*, vol. 30, no. 7, pp. 2446–2488, Nov. 2022.

[30] D. M. J. Priyadharsan, K. K. Sanjay, S. Kathiresan, K. K. Karthik, and K. S. Prasath, "Patient health monitoring using IoT with machine learning," *Int. Res. J. Eng. Technol. (IRJET)*, vol. 6, no. 3, pp. 7514–7520, Mar. 2019.

[31] G. Drosatos and E. Kaldoudi, "Blockchain applications in the biomedical domain: A scoping review," *Comput. Struct. Biotechnol. J.*, vol. 17, pp. 229–240, Jan. 2019.

[32] S. M. Kumar and D. Majumder, "Healthcare solution based on machine learning applications in IoT and edge computing," *Int. J. Pure Appl. Math.*, vol. 119, no. 16, pp. 1473–1484, 2018.

[33] M. Cocosila and N. Archer, "Adoption of mobile ICT for health promotion: An empirical investigation," *Electron. Markets*, vol. 20, nos. 3–4, pp. 241–250, Dec. 2010.

[34] B. Kitchenham, O. P. Brereton, D. Budgen, M. Turner, J. Bailey, and S. Linkman, "Systematic literature reviews in software engineering—A systematic literature review," *Inf. Softw. Technol.*, vol. 51, no. 1, pp. 7–15, 2009.

[35] B. Kitchenham, "Systematic literature reviews in software engineering—A tertiary study," *Inf. Softw. Technol.*, vol. 52, no. 8, pp. 792–805, 2010.

[36] A. H. Khan, N. Ul Hassan, C. Yuen, J. Zhao, D. Niyato, Y. Zhang, and H. V. Poor, "Blockchain and 6G: The future of secure and ubiquitous communication," *IEEE Wireless Commun.*, vol. 29, no. 1, pp. 194–201, Feb. 2022.

[37] H. H. Pajooh, S. Demidenko, S. Aslam, and M. Harris, "Blockchain and 6G-enabled IoT," *Inventions*, vol. 7, no. 4, p. 109, Nov. 2022.

[38] S. K. T. Mehedi, A. A. M. Shamim, and M. B. A. Miah, "Blockchain-based security management of IoT infrastructure with Ethereum transactions," *Iran J. Comput. Sci.*, vol. 2, no. 3, pp. 189–195, Sep. 2019.

[39] M. A. Uddin, A. Stranieri, I. Gondal, and V. Balasubramanian, "A survey on the adoption of blockchain in IoT: Challenges and solutions," *Blockchain, Res. Appl.*, vol. 2, no. 2, Jun. 2021, Art. no. 100006.

[40] V. Maurya, V. Rishiwal, M. Yadav, D. S. Jat, U. Agarwal, and V. R. Verma, "Blockchain-powered solution to safeguard IoT devices against attacks," in *Proc. Int. Conf. Emerg. Trends Netw. Comput. Commun. (ETNCC)*, Aug. 2023, pp. 209–215.

[41] B. Bhushan, C. Sahoo, P. Sinha, and A. Khamparia, "Unification of blockchain and Internet of Things (BIoT): Requirements, working model, challenges and future directions," *Wireless Netw.*, vol. 27, no. 1, pp. 55–90, Jan. 2021.

[42] A. Jahid, M. H. Alsharif, and T. J. Hall, "The convergence of blockchain, IoT and 6G: Potential, opportunities, challenges and research roadmap," *J. Netw. Comput. Appl.*, vol. 217, Aug. 2023, Art. no. 103677.

[43] W. Li, Z. Su, R. Li, K. Zhang, and Y. Wang, "Blockchain-based data security for artificial intelligence applications in 6G networks," *IEEE Netw.*, vol. 34, no. 6, pp. 31–37, Nov. 2020.

[44] U. Agarwal, V. Rishiwal, S. Tanwar, R. Chaudhary, G. Sharma, P. N. Bokoro, and R. Sharma, "Blockchain technology for secure supply chain management: A comprehensive review," *IEEE Access*, vol. 10, pp. 85493–85517, 2022.

[45] A. Kaur, G. Singh, V. Kukreja, S. Sharma, S. Singh, and B. Yoon, "Adaptation of IoT with blockchain in food supply chain management: An analysis-based review in development, benefits and potential applications," *Sensors*, vol. 22, no. 21, p. 8174, Oct. 2022.

[46] C.-L. Chen, L.-H. Guo, M. Zhou, W.-J. Tsaur, H. Sun, W. Zhan, Y.-Y. Deng, and C.-T. Li, "Blockchain-based anti-counterfeiting management system for traceable luxury products," *Sustainability*, vol. 14, no. 19, p. 12814, Oct. 2022.

[47] J. J. Hathaliya, S. Tanwar, S. Tyagi, and N. Kumar, "Securing electronics healthcare records in healthcare 4.0: A biometric-based approach," *Comput. Electr. Eng.*, vol. 76, pp. 398–410, Jun. 2019.

[48] Y. Sun, F. P.-W. Lo, and B. Lo, "Security and privacy for the Internet of Medical Things enabled healthcare systems: A survey," *IEEE Access*, vol. 7, pp. 183339–183355, 2019.

[49] S. Shi, D. He, L. Li, N. Kumar, M. K. Khan, and K.-K.-R. Choo, "Applications of blockchain in ensuring the security and privacy of electronic health record systems: A survey," *Comput. Secur.*, vol. 97, Oct. 2020, Art. no. 101966.

[50] M. N. Bhuiyan, M. M. Rahman, M. M. Billah, and D. Saha, "Internet of Things (IoT): A review of its enabling technologies in healthcare applications, standards protocols, security, and market opportunities," *IEEE Internet Things J.*, vol. 8, no. 13, pp. 10474–10498, Jul. 2021.

[51] G. Subramanian and A. S. Thampy, "Implementation of blockchain consortium to prioritize diabetes patients' healthcare in pandemic situations," *IEEE Access*, vol. 9, pp. 162459–162475, 2021.

[52] J. B. Awotunde, C. Chakraborty, and S. O. Folorunso, "A secured smart healthcare monitoring systems using blockchain technology," in *Intelligent Internet of Things for Healthcare and Industry*. Cham, Switzerland: Springer, 2022, pp. 127–143.

[53] G. Tomasicchio, A. Ceccarelli, A. D. Matteis, and L. Spazzacampagna, "A space-based healthcare emergency management system for epidemics monitoring and response," in *Proc. 38th Int. Commun. Satell. Syst. Conf. (ICSSC)*, vol. 2021, Sep. 2021, pp. 195–199.

[54] H. J. D. M. Costa, C. A. Da Costa, R. D. R. Righi, R. S. Antunes, J. F. De Paz Santana, and V. R. Q. Leithardt, "A fog and blockchain software architecture for a global scale vaccination strategy," *IEEE Access*, vol. 10, pp. 44290–44304, 2022.

[55] M. Saravanan, R. Shubha, A. M. Marks, and V. Iyer, "SMEAD: A secured mobile enabled assisting device for diabetics monitoring," in *Proc. IEEE Int. Conf. Adv. Netw. Telecommun. Syst. (ANTS)*, Dec. 2017, pp. 1–6.

[56] A. Capossele, A. Gaglione, M. Nati, M. Conti, R. Lazzeretti, and P. Missier, "Leveraging blockchain to enable smart-health applications," in *Proc. IEEE 4th Int. Forum Res. Technol. Soc. Ind. (RTSI)*, Sep. 2018, pp. 1–6.

[57] S. K. Jagatheesaperumal, P. Mishra, N. Moustafa, and R. Chauhan, "A holistic survey on the use of emerging technologies to provision secure healthcare solutions," *Comput. Electr. Eng.*, vol. 99, Apr. 2022, Art. no. 107691.

[58] A. Kumari, R. Gupta, and S. Tanwar, "Amalgamation of blockchain and IoT for smart cities underlying 6G communication: A comprehensive review," *Comput. Commun.*, vol. 172, pp. 102–118, Apr. 2021.

[59] A. S. Syed, D. Sierra-Sosa, A. Kumar, and A. Elmaghraby, "IoT in smart cities: A survey of technologies, practices and challenges," *Smart Cities*, vol. 4, no. 2, pp. 429–475, Mar. 2021.

[60] R. P. Janani, K. Renuka, and A. Aruna, "IoT in smart cities: A contemporary survey," *Global Transitions Proc.*, vol. 2, no. 2, pp. 187–193, Nov. 2021.

[61] H. Treiblmaier, A. Rejeb, and A. Strebinger, "Blockchain as a driver for smart city development: Application fields and a comprehensive research agenda," *Smart Cities*, vol. 3, no. 3, pp. 853–872, Aug. 2020.

[62] M. S. Alnahari and S. T. Ariaratnam, "The application of blockchain technology to smart city infrastructure," *Smart Cities*, vol. 5, no. 3, pp. 979–993, Aug. 2022.

[63] D. Kundu, "Blockchain and trust in a smart city," *Environ. Urbanization ASIA*, vol. 10, no. 1, pp. 31–43, Mar. 2019.

[64] L. Fan, J. R. Gil-Garcia, D. Werthmuller, G. B. Burke, and X. Hong, "Investigating blockchain as a data management tool for IoT devices in smart city initiatives," in *Proc. 19th Annu. Int. Conf. Digit. Government Res., Governance Data Age*, May 2018, pp. 1–2.

[65] H. Habibzadeh, B. H. Nussbaum, F. Anjomshoa, B. Kantarci, and T. Soyata, "A survey on cybersecurity, data privacy, and policy issues in cyber-physical system deployments in smart cities," *Sustain. Cities Soc.*, vol. 50, Oct. 2019, Art. no. 101660.

[66] M. A. Rahman, M. M. Rashid, M. S. Hossain, E. Hassanain, M. F. Alhamid, and M. Guizani, "Blockchain and IoT-based cognitive edge framework for sharing economy services in a smart city," *IEEE Access*, vol. 7, pp. 18611–18621, 2019.

[67] M. N. Malik, M. A. Azam, M. Ehatisham-Ul-Haq, W. Ejaz, and A. Khalid, "ADLAuth: Passive authentication based on activity of daily living using heterogeneous sensing in smart cities," *Sensors*, vol. 19, no. 11, p. 2466, May 2019.

[68] P. Khan, Y.-C. Byun, and N. Park, "A data verification system for CCTV surveillance cameras using blockchain technology in smart cities," *Electronics*, vol. 9, no. 3, p. 484, Mar. 2020.

[69] C. Esposito, M. Ficco, and B. B. Gupta, "Blockchain-based authentication and authorization for smart city applications," *Inf. Process. Manage.*, vol. 58, no. 2, Mar. 2021, Art. no. 102468.

[70] M. Asif, Z. Aziz, M. B. Ahmad, A. Khalid, H. A. Waris, and A. Gilani, "Blockchain-based authentication and trust management mechanism for smart cities," *Sensors*, vol. 22, no. 7, p. 2604, Mar. 2022.

[71] K. Biswas and V. Muthukkumarasamy, "Securing smart cities using blockchain technology," in *Proc. IEEE 18th Int. Conf. High Perform. Comput. Commun., IEEE 14th Int. Conf. Smart City; IEEE 2nd Int. Conf. Data Sci. Syst. (HPCC/SmartCity/DSS)*, Dec. 2016, pp. 1392–1393.

[72] C. Lazaroiu and M. Roscia, "Smart district through IoT and blockchain," in *Proc. IEEE 6th Int. Conf. Renew. Energy Res. Appl. (ICRERA)*, Nov. 2017, pp. 454–461.

[73] T. N. Pham, M.-F. Tsai, D. B. Nguyen, C.-R. Dow, and D.-J. Deng, "A cloud-based smart-parking system based on Internet-of-Things technologies," *IEEE Access*, vol. 3, pp. 1581–1591, 2015.

[74] Y. Yuan and F.-Y. Wang, "Towards blockchain-based intelligent transportation systems," in *Proc. IEEE 19th Int. Conf. Intell. Transp. Syst. (ITSC)*, Nov. 2016, pp. 2663–2668.

[75] C. Encinas, E. Ruiz, J. Cortez, and A. Espinoza, "Design and implementation of a distributed IoT system for the monitoring of water quality in aquaculture," in *Proc. Wireless Telecommun. Symp. (WTS)*, Apr. 2017, pp. 1–7.

[76] S. Giordano, I. Seitanidis, M. Ojo, D. Adami, and F. Vignoli, "IoT solutions for crop protection against wild animal attacks," in *Proc. IEEE Int. Conf. Environ. Eng. (EE)*, Mar. 2018, pp. 1–5.

[77] A. Pathak, M. AmazUddin, M. J. Abedin, K. Andersson, R. Mustafa, and M. S. Hossain, "IoT based smart system to support agricultural parameters: A case study," *Proc. Comput. Sci.*, vol. 155, pp. 648–653, Jan. 2019.

[78] Y. Bai, K. Fan, K. Zhang, X. Cheng, H. Li, and Y. Yang, "Blockchain-based trust management for agricultural green supply: A game theoretic approach," *J. Cleaner Prod.*, vol. 310, Aug. 2021, Art. no. 127407.

[79] H. Zeng, G. Dhiman, A. Sharma, A. Sharma, and A. Tselykh, "An IoT and blockchain-based approach for the smart water management system in agriculture," *Expert Syst.*, vol. 40, no. 4, 2023, Art. no. e12892.

[80] R. Chaganti, V. Varadarajan, V. S. Gorantla, T. R. Gadekallu, and V. Ravi, "Blockchain-based cloud-enabled security monitoring using Internet of Things in smart agriculture," *Future Internet*, vol. 14, no. 9, p. 250, 2022.

[81] K. S. Alqarni, F. A. Almalki, B. O. Soufiene, O. Ali, and F. Albalwy, "Authenticated wireless links between a drone and sensors using a blockchain: Case of smart farming," *Wireless Commun. Mobile Comput.*, vol. 2022, pp. 1–13, Sep. 2022.

[82] Z. Raza, I. U. Haq, and M. Muneeb, "Agri-4-all: A framework for blockchain based agricultural food supply chains in the era of fourth industrial revolution," *IEEE Access*, vol. 11, pp. 29851–29867, 2023.

[83] A. Kuzmin and E. Znak, "Blockchain-base structures for a secure and operate network of semi-autonomous unmanned aerial vehicles," in *Proc. IEEE Int. Conf. Service Oper. Logistics, Informat. (SOLI)*, Jul. 2018, pp. 32–37.

[84] A. Buzachis, A. Celesti, A. Galletta, M. Fazio, and M. Villari, "A secure and dependable multi-agent autonomous intersection management (MA-AIM) system leveraging blockchain facilities," in *Proc. IEEE/ACM Int. Conf. Utility Cloud Comput. Companion (UCC Companion)*, Dec. 2018, pp. 226–231.

[85] R. M. Shivers, "Toward a secure and decentralized blockchain-based ride-hailing platform for autonomous vehicles," Ph.D. thesis, Dept. Comput. Sci., Tennessee Technol. Univ., Cookeville, TN, USA, 2019.

[86] Y.-T. Yang, L.-D. Chou, C.-W. Tseng, F.-H. Tseng, and C.-C. Liu, "Blockchain-based traffic event validation and trust verification for VANETs," *IEEE Access*, vol. 7, pp. 30868–30877, 2019.

[87] S. R. Pokhrel and J. Choi, "Federated learning with blockchain for autonomous vehicles: Analysis and design challenges," *IEEE Trans. Commun.*, vol. 68, no. 8, pp. 4734–4746, Aug. 2020.

[88] C. Oham, R. A. Michelin, R. Jurdak, S. S. Kanhere, and S. Jha, "B-FERL: Blockchain based framework for securing smart vehicles," *Inf. Process. Manage.*, vol. 58, no. 1, Jan. 2021, Art. no. 102426.

[89] Y. Yang, Y. Xiao, and T. Li, "A survey of autonomous underwater vehicle formation: Performance, formation control, and communication capability," *IEEE Commun. Surveys Tuts.*, vol. 23, no. 2, pp. 815–841, 2nd Quart., 2021.

[90] H. Min, Y. Fang, X. Wu, X. Lei, S. Chen, R. Teixeira, B. Zhu, X. Zhao, and Z. Xu, "A fault diagnosis framework for autonomous vehicles with sensor self-diagnosis," *Expert Syst. Appl.*, vol. 224, Aug. 2023, Art. no. 120002.

[91] S. Thejaswini and K. R. Ranjitha, "Blockchain in agriculture by using decentralized peer to peer networks," in *Proc. 4th Int. Conf. Inventive Syst. Control (ICISC)*, Jan. 2020, pp. 600–606.

[92] A. Vangala, A. K. Das, N. Kumar, and M. Alazab, "Smart secure sensing for IoT-based agriculture: Blockchain perspective," *IEEE Sensors J.*, vol. 21, no. 16, pp. 17591–17607, Aug. 2021.

[93] 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.

[94] S. Nagpure, S. Ingale, S. Pahurkar, A. M. Bobade, M. Ghosal, and T. Dhope, "Smart agriculture using IoT," *Helix*, vol. 9, no. 3, pp. 5081–5083, 2019.

[95] R. Iqbal and T. A. Butt, "Safe farming as a service of blockchain-based supply chain management for improved transparency," *Cluster Comput.*, vol. 23, no. 3, pp. 2139–2150, Sep. 2020.

[96] M. Osmanoglu, B. Tugrul, T. Dogantuna, and E. Bostanci, "An effective yield estimation system based on blockchain technology," *IEEE Trans. Eng. Manag.*, vol. 67, no. 4, pp. 1157–1168, Nov. 2020.

[97] H. Wu, J. Cao, Y. Yang, C. L. Tung, S. Jiang, B. Tang, Y. Liu, X. Wang, and Y. Deng, "Data management in supply chain using blockchain: Challenges and a case study," in *Proc. 28th Int. Conf. Comput. Commun. Netw. (ICCCN)*, Jul. 2019, pp. 1–8.

[98] X. Zhang, P. Sun, J. Xu, X. Wang, J. Yu, Z. Zhao, and Y. Dong, "Blockchain-based safety management system for the grain supply chain," *IEEE Access*, vol. 8, pp. 36398–36410, 2020.

[99] X. Yang, M. Li, H. Yu, M. Wang, D. Xu, and C. Sun, "A trusted blockchain-based traceability system for fruit and vegetable agricultural products," *IEEE Access*, vol. 9, pp. 36282–36293, 2021.

[100] G. Subramanian, A. S. Thampy, N. V. Ugwuoke, and B. Ramnani, "Crypto pharmacy—Digital medicine: A mobile application integrated with hybrid blockchain to tackle the issues in pharma supply chain," *IEEE Open J. Comput. Soc.*, vol. 2, pp. 26–37, 2021.

[101] L. Cocco, K. Mannaro, R. Tonelli, L. Mariani, M. B. Lodi, A. Melis, M. Simone, and A. Fanti, "A blockchain-based traceability system in agri-food SME: Case study of a traditional bakery," *IEEE Access*, vol. 9, pp. 62899–62915, 2021.

[102] Z. Lu, Q. Wang, G. Qu, and Z. Liu, "BARS: A blockchain-based anonymous reputation system for trust management in VANETs," in *Proc. 17th IEEE Int. Conf. Trust, Secur. Privacy Comput. Commun./12th IEEE Int. Conf. Big Data Sci. Eng. (TrustCom/BigDataSE)*, Aug. 2018, pp. 98–103.

[103] S. S. Arumugam, V. Umashankar, N. C. Narendra, R. Badrinath, A. P. Mujumdar, J. Holler, and A. Hernandez, "IoT enabled smart logistics using smart contracts," in *Proc. 8th Int. Conf. Logistics, Informat. Service Sci. (LISS)*, Aug. 2018, pp. 1–6.

[104] S. F. Wamba and M. M. Queiroz, "Industry 4.0 and the supply chain digitalisation: A blockchain diffusion perspective," *Prod. Planning Control*, vol. 33, nos. 2–3, pp. 193–210, Feb. 2022.

[105] P. K. Senyo, K. Liu, and J. Effah, "Digital business ecosystem: Literature review and a framework for future research," *Int. J. Inf. Manage.*, vol. 47, pp. 52–64, Aug. 2019.

MANO YADAV received the Ph.D. degree in computer science and information technology from MJP Rohilkhand University, Bareilly, India, in 2012. She is currently an Assistant Professor with the Department of Computer Science, Bareilly College, Bareilly, Uttar Pradesh. She has published more than 40 research papers in reputed journals/conferences. She has seven patents on her credit. Her research interests include wireless sensor networks, machine learning, and the IoT. She is a member of many technical societies, such as IACSIT, Singapore; and MIR Labs, USA. She served as a reviewer for many journals.

UDIT AGARWAL received the M.Sc. degree from MJP Rohilkhand University, Bareilly, India, in 2001, and the Master of Computer Application degree from Uttar Pradesh Technical University, Lucknow, India, in 2004. He is currently pursuing the Ph.D. degree with the Department of Computer Science and Information Technology, MJP Rohilkhand University. His research interests include blockchain, agricultural traceability, and ML.

VINAY RISHIWAL (Senior Member, IEEE) received the B.Tech. degree in computer science and engineering from SRMSCET, MJP Rohilkhand University, Bareilly, Uttar Pradesh, India, in 2000, and the Ph.D. degree in computer science and engineering from Gautam Buddha Technical University, Lucknow, India, in 2011. He is currently working as a Professor with the Department of Computer Science and Information Technology, Faculty of Engineering and Technology, MJP Rohilkhand University. He has 23 years of experience in academics. He has published more than 90 research papers in various journals and conferences of international repute. He has 20 patents on his credit. He visited many countries for academic purposes and worked on many projects of CST, UP Government, MHRD, and UGC. His current research interests include wireless sensor networks, the IoT, cloud computing, social networks, and blockchain technology. He is a Senior Member of ACM. He was a Convener of the Student Activities Committee, IEEE Uttar Pradesh Section, India. He received many awards as the best paper/researcher/orator at various platforms. He is the General/Conference Chair of the four international conferences, such as ICACCA, the IoT-SIU, MARC 2020, and ICAREMIT.

SUDEEP TANWAR (Senior Member, IEEE) received the B.Tech. degree from Kurukshetra University, India, in 2002, the M.Tech. degree (Hons.) from Guru Gobind Singh Indraprastha University, Delhi, India, in 2009, and the Ph.D. degree with specialization in wireless sensor network, in 2016. He is currently a Professor with the Computer Science and Engineering Department, Institute of Technology, Nirma University, India. He is also a Visiting Professor with Jan Wyzykowski University, Polkowice, Poland, and the University of Pitesti, Pitesti, Romania. He is leading the ST Research Laboratory, where group members are involved on the latest cutting-edge technologies. He has authored two books and edited 13 books, and more than 400 technical articles, including top journals and top conferences, such as IEEE TRANSACTIONS ON NETWORK SCIENCE AND ENGINEERING, IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY, IEEE TRANSACTIONS ON INDUSTRIAL INFORMATICS, IEEE WIRELESS COMMUNICATIONS, IEEE NETWORK, ICC, GLOBECOM, and INFOCOM. He initiated the research field of blockchain technology adoption in various verticals, in 2017. His H-index is 67. He actively serves his research communities in various roles. His research interests include blockchain technology, wireless sensor networks, fog computing, smart grids, and the IoT. He is a Final Voting Member of the IEEE ComSoc Tactile Internet Committee, in 2020. He is a member of CSI, IAENG, ISTE, CSTA, and the Technical Committee on Tactile Internet of IEEE Communication Society. He was awarded the Best Research Paper Awards from IEEE IWCMC-2021, IEEE GLOBECOM 2018, IEEE ICC 2019, and Springer ICRIC-2019. He has served many international conferences, as a member of the Organizing Committee, such as the Publication Chair for FTNCT-2020, ICCIC 2020, and WiMob2019; a member of the Advisory Board for ICACCT-2021 and ICACI 2020; the Workshop Co-Chair for CIS 2021; and the General Chair for IC4S 2019, 2020, and ICCSDF 2020. He is serving the Editorial Boards of *Computer Communications*, *International Journal of Communication System*, and *Security and Privacy*.

SUMAN KUMAR received the degree in electronics and communication engineering from the Indian Institute of Technology (IIT) BHU Varanasi, India, and the Ph.D. degree from Louisiana State University. He is currently an Associate Professor with the Computer Science Department, Troy University. He leads the Trojan Advanced Computer Knowledge and Networking Group (TrACKNet). Over the years, he has published numerous research papers on varied topics, such as opto-electronics devices, travelling wave tubes, high speed networks, data center networks, future internet architecture, health informatics, cloud computing, and intelligent transportation systems. His current research interests include all aspect of computer communications and networking, intelligent systems, and cyber security.

FAYEZ ALQAHTANI was appointed as the Director of the Computer Division, Deanship of Student Affairs. He is currently a Full Professor with the Software Engineering Department, College of Computer and Information Sciences, King Saud University (KSU). He is also a member of numerous academic and professional associations, such as the Association for Computing Machinery (ACM), the Australian Computer Society, and the Association for Information Systems. He has conducted research projects in several areas of information and communication technology, such as web 2.0, information security, enterprise architecture, software process improvement, the Internet of Things, and fog computing. He has participated in several academic events.

AMR TOLBA (Senior Member, IEEE) received the M.Sc. and Ph.D. degrees from the Mathematics and Computer Science Department, Faculty of Science, Menoufia University, Egypt, in 2002 and 2006, respectively. He is currently a Full Professor of computer science with King Saud University (KSU), Saudi Arabia. He has authored/coauthored over 160 scientific articles in top-ranked (ISI) international journals, such as IEEE INTERNET OF THINGS JOURNAL, *ACM Transactions on Internet Technology*, *IEEE Consumer Electronics Magazine*, IEEE ACCESS, IEEE SYSTEMS JOURNAL, *Future Generation Computer Systems*, *Journal of Network and Computer Applications*, *Neural Computing and Applications*, *Journal of Ambient Intelligence and Humanized Computing*, *Computer Networks*, *Computer Communications*, *Peer-to-Peer Networking and Applications*, *VCOM*, and *WWWJ*. He has translated four books into the Arabic language. His research interests include artificial intelligence (AI), the Internet of Things (IoT), data science, and cloud computing. He served as a Technical Program Committee (TPC) Member at several conferences, such as DSIT 2022, CICA2022, EAI MobiHealth 2021, DSS 2021, AEMCSE 2021, ICBDM 2021, ICISE 2021, DSS 2020, NCO 2020, ICISE2019, ICCSEA 2019, DSS 2019, FCES 19, ICISE 2018, ESG18, Smart Data17, NECO 2017, NC17, WEMNET17, NET17, and Smart Data16. He has been included in the list of the top 2% of influential researchers globally (prepared by scientists from Stanford University, USA), in 2020, 2021, and 2022. He served as an associate editor/a guest editor for several ISI journals.