IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received 30 June 2024, accepted 15 July 2024, date of publication 30 July 2024, date of current version 16 August 2024.

Digital Object Identifier 10.1109/ACCESS.2024.3435845

RESEARCH ARTICLE

A Review of Security Issues When Integrating IoT With Cloud Computing and Blockchain

LATIFA ALBSHAIER, ALANOUD BUDOKHI, AND AHMED ALJUGHAIMAN
Department of Computer Networks and Communications, College of Computer Sciences and Information Technology, King Faisal University, Al-Ahsa 31982, Saudi Arabia

Corresponding author: Latifa Albshaier (223000803@student.kfu.edu.sa)

This work was supported by the Deanship of Scientific Research, Vice Presidency for Graduate Studies and Scientific Research, King Faisal University, Saudi Arabia, under Grant KFU241426.

ABSTRACT The integration of the Internet of Things (IoT) and cloud computing, which play essential roles in our everyday routines, is expected to emerge as a fundamental element of the forthcoming internet, realizing increased usage and acceptance. This fusion is anticipated to revolutionize various applications, offering The integration of IoT and cloud may pose challenges. Cloud computing's capacity to distribute resources and data across diverse locations, facilitating access from different industrial settings, has significantly enhanced IoT functionality. However, rapid migration to the cloud has raised security concerns, as conventional security measures for computers are not always applied effectively to cloud-based systems. Overcoming these obstacles can be achieved by integrating cloud and IoT technologies, as the vast resources available on the cloud can greatly benefit IoT, helping the cloud transcend current limitations related to physical objects in a more dynamic, distributed manner. Several discoveries from the research were made by exploring the facilitation of a smooth shift of IoT initiatives to the cloud by studying IoT and cloud computing, investigating various cloud-related challenges and resolutions derived from recent scholarly works, and analyzing the most recent advancements in attacks targeting cloud-based IoT systems. Identifying gaps in the research on IoT-based cloud infrastructure and addressing cybersecurity in cloud computing is important for future research directions, necessitating a review of the technological challenges mentioned in the literature. As such, this research explores how blockchain technology effectively addresses security concerns within this combination, emphasizing its capacity to improve data integrity and privacy and to ensure secure transactions. The exploration delves into the multifaceted implications and potential applications of blockchain, elucidating its role in reinforcing the overall security of these interconnected systems.

INDEX TERMS IoT, cloud computing, security issues, blockchain.

I. INTRODUCTION

Combining Internet the of Things (IoT) and cloud computing offers a fast method of managing, storing, and understanding data collected from IoT devices. It allows devices to send their data to the cloud, where it can be easily stored and analyzed [1]. Using cloud computing makes it easier and cheaper for people and businesses to set up and use many connected devices. Thus, bringing together IoT and cloud computing has enabled the creation of systems that turn data from sensors and devices into things we can do or decisions we can make. This combination also helps with predictions and quick decision-making by watching things happen in real-time. It also helps identify problems throughout the whole system. Moreover, in cloud-based applications, it is simple to adjust the size of what you are using at will because hardware and software tasks are handled separately [2]. Ensuring data is safe and private when sent between IoT devices and the cloud is achieved by using end-to-end encryption protocols. In addition, cloud computing allows

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

the offloading of computer tasks, speeding up processes and reducing the time it takes to process information [3].

Bringing these technologies together offers many benefits, such as better performance, the ability to grow easily, predict what might happen, saving money, greater security, and more convenience [4]. First and foremost, putting these things together really boosts how well everything works by simplifying device connection and data sharing without issue. The significant computing power and storage space in the cloud handle much data from IoT devices very efficiently, ensuring everything is processed and viewed smoothly. Being able to easily adjust to different needs easily is a significant advantage in this combination, thanks to the cloud's ability to change its resources as needed. This ability to adjust easily is especially good for IoT applications because the number of connected devices can increase or decrease often. In addition, the power of prediction is improved. By using the information, we obtain from IoT devices and using smart math in the cloud, organizations can figure out important things, offer predictions, and make smart decisions. This helps with caring for things before they break, improving processes, working better, and even anticipating customer and market actions. It also saves much money. The cloud's policy of paying only for what you use allows companies to avoid spending significant money upfront on necessities to get started. As well, IoT devices do not need much storage and computer power on their own because the cloud accounts for a significant part of the work, cutting down the costs for each device. Combining technologies work together like this also strengthens security much, as the cloud usually has solid safety features, such as keeping information safe with codes, controlling who has access, and updating things regularly to remain safe, improving the security of IoT systems significantly. The cloud can watch over and control many connected devices all in one place, simplifying the search and destruction of any security problems that might occur. The user experience is also simplified, as they can reach and control their IoT devices and the information they collect from anywhere using applications or platforms in the cloud. These remote capabilities make it easy to watch, control, and understand IoT systems, allowing everything to work better and to become more adaptable. Thus, bringing together IoT and cloud computing is a significant change that brings many benefits to different areas.

The IoT, which is akin to a significant web of connected devices and sensors, holds much data that requires ample computer power to store, process, and understand. As such, cloud computing enables the obtainment of the right amount of computer power easily when we need it, making it efficient to deal with all this data. This combination makes it easy to combine everything together, enabling quick movement, storage, and understanding of real-time data. This also contributes to better decision-making and improved predictions, as the cloud's centralized system makes it easier to obtain, secure, and control the data the IoT creates. Combining IoT and cloud computing thus allows us to create new and creative applications and services, pushing forward such areas as healthcare, smart cities, and industrial automation. Through this combination, not only does everything work more efficiently, but it also encourages new ideas, and growth in many different areas is encouraged [4]. However, combining IoT and cloud computing has also brought many security concerns. For instance, data breaches and privacy problems can occur because of all the connections and shared information between devices and cloud networks. Dealing with these tricky security problems therefore necessitates creative solutions, one powerful example of which is using blockchain technology, which can help strengthen security in this connected system. Recognized for being decentralized, resistant to tampering, and transparent, blockchain becomes a hopeful solution to fix security problems brought by combining IoT and cloud computing. In response, this paper looks at how blockchain technology could play a crucial role in improving security in this integration. It assesses how blockchain can ensure data stays true, maintains privacy, and makes transactions secure, rendering the whole security system stronger for these connected systems.

Companies using connected devices can gain much from combining IoT and cloud computing, the latter of which allows for quick and safe storage, processing, and access to data from IoT, meaning we can implement automation, analyze information, and make better decisions by collecting and studying real-time data on a larger scale [5].

This research paper investigates the collaboration of IoT, cloud computing, and blockchain, first by detailing how IoT and the cloud work together to simplify the management of data from various devices. This partnership facilitates speedy data processing, storage, and analysis, making it a significant tool because it enhances decision-making and enables accurate predictions. However, in combining these technologies, combined, there are security concerns that have been expressed. To address them, the paper examines blockchain technology, recognized for its decentralized, transparent, and secure nature. This study seeks to explore its potential to enhance the security of IoT and cloud computing. It also aims to determine whether blockchain can contribute to strengthening data security, safeguarding privacy, and ensuring secure transactions within these systems. Finally, the research endeavors to ensure the safety and security of IoT and Cloud Computing when combined. The study's objectives can be summarized as follows:

- To explore how IoT, cloud computing, and blockchain technologies can be combined and work together.
- To highlight the benefits of combining IoT and cloud computing for data processing, scalability, making predictions, and cost savings.
- To identify the growing security issues within interconnected networks of IoT and cloud systems.
- To investigate how blockchain technology can strengthen security within this integrated ecosystem.

- To examine how blockchain improves data integrity, privacy measures, and transaction security through the integration of IoT and cloud computing.

This study makes significant contributions to the literature on integrating IoT, cloud computing, and blockchain. By thoroughly examining the combination of these technologies, the research will clarify the complex dynamics and implications, providing a roadmap to improve the collaboration between IoT and the Cloud while incorporating Blockchain for enhanced security. Such insights are invaluable, benefiting the field by deepening our understanding of how these technologies intersect and offering strategies to tackle the emerging security concerns linked to their integration. Furthermore, this study will be of great value to future investigations, providing a strong foundation for subsequent researchers entering this domain. Future researchers can also use the findings of this study to delve deeper into security aspects, exploring various applications of blockchain technology and innovative methods to strengthen the security of integrated IoT and cloud computing systems. The significance of this study lies in its potential to lead the revolution toward the more secure, efficient, and optimized utilization of these technologies in various domains. Finally, conducting this research is crucial to ensuring that the integration of IoT, cloud computing, and blockchain progresses in a secure, reliable, and transformative manner, driving innovation and progress across various sectors.

This paper uniquely explores the combination of IoT, cloud computing, and blockchain technologies, highlighting its innovative approach in comparison to existing studies. Unlike other research that might examine these technologies separately, this paper focuses on how they can work together effectively, with a special emphasis on improving security. In addition, it thoroughly investigates how the core features of blockchain, such as decentralization, transparency, and strong security, can enhance the integration of IoT and cloud computing. This study is extensive, covering not just technical details but also such benefits as scalability, cost savings, and improved predictive analytics, which are crucial to applying these technologies in real-world scenarios. Further, it provides recommendations to address new security risks that arise from connecting these systems. This forward-looking approach distinguishes the paper, making it a critical resource for future research and offering a roadmap for navigating the complexities of integrating these technologies safely and efficiently.

This study thoroughly assesses how IoT, cloud computing, and blockchain can work together, as divided into different parts to help in understanding it better. Section II clarifies how we select and analyze the papers and studies that are relevant to ours using the PRISMA 2020 flow diagram. In Section III, we begin by exploring the fundamentals of IoT and cloud computing. We will discuss IoT technologies, protocols, architectures, limitations, and suggested security practices. Thereafter, we moved on to cloud computing, where we explained service and deployment models. After that, we delve into how IoT can be integrated with cloud computing. The Discussion section (Section IV) represents the core of this paper, where we dive into the complex challenges related to security in IoT and the cloud. We also discussed important topics, including service quality, identity management, data security, support protocols, resource allocation, big data handling, energy consumption, and computational performance. In this section, we will focus on how blockchain can strengthen the integration of IoT and cloud computing, especially in dealing with security issues. The Related Studies (Section V), Open Challenges and Limitations (Section VI), and Future Directions (Section VII), these sections are like a road map for future research, shedding light on what has already been studied, areas seldom explored, much, and potential paths toward progress. Finally, in the Conclusion (Section VIII) we summarize the important findings, highlighting how blockchain plays a crucial role in securing the integration of IoT and the cloud and we suggest future research directions to make security even stronger in this combined area.

II. SELECTION OF RESEARCH PAPERS FOR REVIEW

A systematic literature review (SLR) is a crucial research method used to thoroughly explore revolution previous research and studies on a particular topic. Its primary goal is to gather a complete collection of relevant papers in said field. This serves as an effective way of bringing together past findings and filling any gaps in our knowledge. With the increasing amount of research and scientific papers, there is a rising need for a dependable and strong study that summarizes previous work and combines these findings to address any identified gaps.

In our research paper, we used the PRISMA 2020 Flow Diagram designed for new systematic reviews (shown in Figure 1) to demonstrate visually how many records were included or excluded when selecting studies. We started by searching for relevant research papers on Google Scholar, using a specific search string related to ''Security OR security and privacy AND issues OR obstacles OR problems AND Integration AND IoT AND Blockchain OR Internet of Things AND Cloud OR Cloud Computing OR computing architecture.'' This initial search resulted in an initial count of 525 papers. After refining the search, removing duplicates, and using automation tools to exclude irrelevant entries, the total was reduced to 267. Following these steps, we were left with 258 records. Further screening helped us identify and exclude 179 reports that were either irrelevant to the main topic, not written in English, or not presented in a journal or conference format. This brought the final countdown to 72 remaining reports.

III. BACKGROUND

In recent times, both cloud computing and IoT have become prominent as leading technologies, a fact supported by research findings [6]. The current trend suggests rapid growth in digital technology, and the coming together of

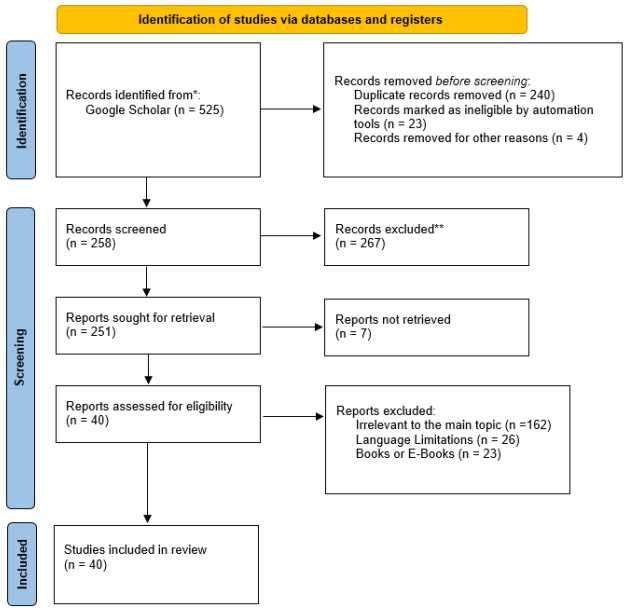

FIGURE 1. Selection of papers for literature review using PRISMA.

cloud computing and IoT holds the potential for efficient resource management. In this section, we first review the various types, architectures, and deployment models of cloud computing. Furthermore, we delve into security concerns and challenges linked to these models. The collaboration between IoT and cloud computing acts as a powerful team in today's technology landscape. IoT devices, ranging from sensors to smart gadgets, generate substantial data, but handling and interpreting all these data can be challenging. Hence, by integrating IoT with cloud computing, we solve this challenge [7]. Cloud computing involves using large, distant computers to store and process data. Thus, when we link IoT to these remote servers, it helps us manage data more effectively. Cloud servers can handle a substantial amount of data generated by IoT devices, store them, process them, and enable quick analysis. This connection is extremely beneficial for businesses, allowing them to make faster decision-making based on real-time information. It also ensures data accessibility from anywhere, benefiting industries, such as healthcare, manufacturing, transport, and smart cities. The collaboration between IoT and cloud computing therefore enhances technology, making it smarter and more efficient and transforming how we solve problems and innovate [8].

Blockchain technology could play a crucial role in improving the integration of IoT and cloud computing, functioning as a digital ledger that securely stores information across a network of computers, making it extremely difficult to alter or hack [9]. When integrated with IoT and cloud computing, blockchain can provide an additional layer of security and trust in the data generated by IoT devices.

For example, IoT devices continuously gather sensitive data, such as personal information or critical operational data. By using blockchain, these data can be securely recorded and verified. The decentralized nature of blockchain ensures that the data are not stored in a single location, reducing vulnerability to cyber-attacks [10]. In addition, it guarantees data integrity and authenticity of the data. Each piece of information stored on the blockchain is timestamped and linked to previous records, forming a transparent and unalterable history of the data's journey.

Furthermore, blockchain technology allows the implementation of smart contracts, which are self-executing contracts with terms directly written into code. These contracts can automate processes between IoT devices and cloud services without requiring a central authority, diminishing the need for intermediaries, and boosting efficiency in transactions or interactions.

In simple terms, incorporating blockchain into IoT and cloud computing offers an extra layer of security, transparency, and efficiency to the system [11]. As well, it assists in securing sensitive data, ensuring their authenticity, and automating processes, thereby enhancing the overall trustworthiness and reliability of the entire system.

A. IOT

Anything located on the Earth's surface, whether it is an interactive device or a non-interactive object, falls under the category of a "thing" in the IoT, which represents a revolutionary concept where forming an extensive network of interconnected devices and objects capable of communicating and sharing data without human intervention. This includes a wide range of everyday items, from smart thermostats and wearable fitness trackers to industrial sensors and autonomous vehicles, all linked through the internet. Thus, the significance of the IoT lies in its transformative ability to connect the physical and digital worlds, facilitating seamless communication and empowering these devices to collect, exchange, and act on data [12]. This interconnected ability will bring convenience and efficiency to our lives and industries, and by integrating sensors, actuators, and communication capabilities into various objects and systems, IoT facilitates automation, real-time monitoring, and intelligent decision-making [13], as well as streamlines processes, optimizes resource utilization, enhances productivity, and creates new opportunities across various sectors such as manufacturing, transportation, agriculture, and smart cities. As IoT continues to evolve, its capacity to connect devices and provide data-driven insights holds the potential to unlock innovative solutions and shape a more connected and efficient world [12].

1) TECHNOLOGIES EMBEDDED IN IOT DEVICES

- **Sensors:**
  They are like the eyes and ears of smart devices in the IoT. They work on collecting real-world data. For example, to detect room temperature, regardless of whether it is getting hotter or colder, to keep an eye on movement; or to check the humidity, sensors gather all

details. This helps devices determine what is happening in their surroundings. In terms of security, sensors can read unusual activities or sudden changes. For example, they might alert you if someone is trying to access a device without permission or if there is a shift in the environment that could affect how the device works [14], [15].

- **Actuators:**
  Actuators are like the actors in smart devices. They do things based on what the sensors tell them. Whether it is turning something on or off or making things move, actuators follow the instructions they are given. In terms of security, actuators can keep things safe by acting when a sensor raises an alarm. For example, they could lock a door or stop a system if there is a security problem [16].
- **Network:**
  The network provides connectivity which is how smart devices communicate with each other or with a main system. For example, they use Wi-Fi, Bluetooth, or cell networks to send and receive data [17], [18]. From a security perspective, it is crucial to use strong encryption methods to secure communication between devices and servers. This helps stop unauthorized access and keeps important information safe while it is moving around [19].
- **Processors:**
  Processors are like the brains of smart devices. They look at the data from sensors, make decisions, and initiate actions [18]. In terms of security, processors follow security rules and use authentication methods. This means they ensure only the correct people or devices can access the data, and they ensure the data remains as it should, without any changes [14].

2) IOT PROTOCOLS

- **Message queuing telemetry transport (MQTT):**
  MQTT is a simple way for devices to communicate with each other, making it a great option for IoT, as it does not need much internet space, which is good for devices with less power [15]. It works as follows: devices send their messages to a mediator, called a ''broker,'' and other devices can sign up to receive the messages they care about. However, one problem is that MQTT is highly insecure, so we need extra steps to keep the information safe when it is being shared [17].
- **Constrained application protocol (CoAP):**
  CoAP is made for small and simple devices in IoT, such as those that have little power or processing ability. It is a basic method for these devices to communicate with each other over the internet. CoAP works like hypertext transfer protocol (HTTP), which is used for regular internet communication, but it is designed specifically for IoT devices. However, there can be problems that can arise because CoAP uses the user datagram protocol (UDP), which lacks some of the reliability features that TCP (Transmission Control Protocol) has. This might cause some issues in ensuring data gets delivered properly [14], [16].
- **Hypertext Transfer Protocol (HTTP):**
  HTTP is a common method of communication on the internet. In IoT, it is used to send data between IoT devices and servers [18], [19]. Even though HTTP is well-known and can handle different data types, it might not be the best choice for IoT devices having few resources. This is because it has extra features that can use up additional power, which is a problem for devices that run on batteries. Therefore, using HTTP can be a challenge for devices with limited power [16].

There are shared difficulties in these communication protocols, such as security problems, possible issues with data reliability, and poor efficiency for devices with limited resources. Finding the right balance between making communication efficient and keeping data secure and dependable is a significant challenge in developing protocols for IoT.

3) IOT ARCHITECTURE

Through data communication methods, particularly via radio frequency identification (RFID) tags, these objects transition into communicative nodes capable of exchanging information across the internet. The traditional IoT architecture consists of three core layers: the perception layer, the network layer, and the application layer. However, some sources [20], [21] have introduced the middleware and the business layers as additional components supplementing the existing three layers, resulting in the formation of a comprehensive five-layer architecture, as illustrated in Fig. 2: The architecture of IoT architecture consists of five

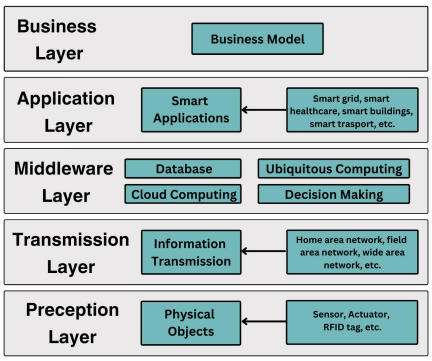

FIGURE 2. Five layers of the IoT architecture.

interconnected layers, each playing a crucial role in the functionality and operation of IoT systems. The first layer, known as the Perception Layer, involves sensors, actuators, and devices that gather data from the physical world. Security concerns arise here due to the vulnerability of these endpoints to physical tampering, data spoofing, or unauthorized access. Moving to the network layer, where data from various devices are transmitted and collected, security challenges revolve around securing communication protocols, preventing data interception, and avoiding network-based attacks

like Man-in-the-Middle (MitM) or denial-of-service (DoS) attacks [22]. The third layer, called the middleware layer, handles such tasks as processing data, storing information, and managing devices. In terms of security, it is important to ensure that the data remains intact, are encryption is utilized when sending and storing, and prevent unauthorized access to stored information is prevented. Moving on to the application layer, here, user applications and services connect with IoT systems. Security concerns here include ensuring that authentication (verifying identity) is secure, authorization (controlling access) is reliable, and application programming interface (API) interactions are secure to avoid any exploitation of application vulnerabilities [23]. Finally, the business layer manages business applications, analytics, and decision-making processes, and its security is centered on safeguarding sensitive business data, ensuring the operations comply with regulations, and setting up secure access controls for critical business functions [12]. It is important to tackle security issues at every layer to create a strong and secure IoT architecture, which guarantees that data, devices, and systems are protected from potential threats and vulnerabilities.

Table 1 outlines the different layers within the IoT framework, providing a clear explanation of the various types of attacks that represent significant security threats at each level. The foundational layer of the IoT architecture is the perception layer, responsible for capturing environmental data. This layer [24] serves as the hub for all data collection and sensing activities, housing sensors, barcode labels, RFID tags, Global Positioning System (GPS), and cameras. Its fundamental purpose is to recognize objects and gather data. Meanwhile, the network layer collects and transmits the data perceived by the Perception layer. It accumulates data from the lowest layer and sends it to the internet. Typically, this layer may encompass a gateway, serving as an interface between the sensor network and the internet. Handling data storage and service management characterizes the middleware layer, which involves processing information and autonomously making decisions based on the resulting outcomes [20].

4) IOT LIMITATIONS AND CHALLENGES

Security in IoT encounters various challenges that require careful consideration. For instance, a significant issue is the large number of devices connected to the internet. With numerous devices collecting and exchanging data, each one becomes a potential vulnerability for cyber-attacks. In addition, many IoT devices lack appropriate security measures or have default passwords, making them vulnerable and easy targets for hackers [16]. Another challenge lies in device diversity, each with its own operating system and security protocols. This variety makes it challenging to establish universal security standards that can effectively cover all devices. Furthermore, as these devices collect sensitive data, there are concerns regarding data privacy and how this information is stored, accessed, and shared. As IoT rapidly expands into various industries such as healthcare and smart homes, ensuring the protection of personal information becomes crucial [19]. Staying current with security updates and patches for IoT devices is thus challenging, as some devices may not receive regular updates or support, leaving them exposed to known security issues. Securing the extensive network of interconnected IoT devices, while also considering usability, privacy, and standardized security measures, remains a significant challenge across the IoT landscape.

The challenges faced by IoT devices in terms of security are becoming more complex and varied, involving different vulnerabilities that pose significant risks to both the security and functionality of these devices. A prominent threat to IoT devices is the widespread presence of malware, which includes viruses, worms, and botnets. This type of malicious software can exploit vulnerabilities in device software or firmware, posing a serious risk to their operation and security. Malicious programs can harm your device by threatening its safety, removing important information, or blocking its use. Ransomware is especially dangerous because it locks up your data, asks for money to unlock it, and might harm important device functionalities [13]. Another significant threat is something called distributed denial-of-service (DDoS) attacks, wherein a number of infected devices flood a system with way too much traffic, causing problems or even rendering the service completely useless [18]. In addition, when people interfere with IoT devices physically without permission, it is a real threat Someone accessing these devices without permission could change the data, damage the device on purpose, or install harmful software or hardware [17]. These dangers show how important it is to implement security measures for IoT devices, including regularly updating software, using encryption, having strong proof of identity, (authentication), dividing the network into smaller parts (network segmentation), and following good security rules for the physical aspects. All these help to reduce the growing risks facing IoT devices in today's connected world [14].

5) BEST PRACTICES TO SECURE IOT

In our connected world, rendering IoT devices more secure requires both the people who make them and the people who use them to work together. This way, they can effectively reduce the possible risks [16]. Makers of these devices are important in that they must ensure strong security right from the start, using secure design principles, checking for security regularly, and using encryption. It is also important for them to be clear about the security features and to make it easy for users to update the device's software quickly to fix any problems. Users are just as crucial as they must be careful and follow proper security rules. This means keeping up with information about security problems and updates for their IoT devices and quickly adding any fixes or updates provided by the makers. In addition, ensuring strong, different passwords and using extra security steps (multi-factor authentication,

TABLE 1. Attacks in IoT Layers.

IoT Layer	Attack	Security Challenges	Solutions Through Cloud Computing and Blockchain Integration
Perception Layer	• Physical Tampering • Spoofing Attacks	• Physical altering incorporates unauthorized get to IoT gadgets to change their equipment, firmware, or embedding pernicious code, compromising the device's capability, permitting data robbery, or enabling unauthorized oversight. • Spoofing ambushes IoT device sensors by infusing incorrect records, deceiving the framework into making inaccurate determinations or identifying misleading developments, surely disturbing operations, or allowing unauthorized passage based completely on misrepresented records.	• Cloud computing: Enhanced encryption and access control; centralized device management. • Blockchain: Decentralized security protocols; immutable data records to prevent tampering.
Network Layer	• MitM Attacks • DoS Attacks	• MitM attacks captured and controlled IoT communications, permitting assailants to modify actualities, view records, or infuse pernicious substances, compromising data astuteness, taking unstable actualities, or sending unauthorized information. • DoS attacks flood IoT systems or devices with unwanted guests, sometimes blocking access to network users or altering data, causing gadget breakdowns due to asset exhaustion, and ruining typical operations or insights gathered.	• Cloud computing: DDoS protection; traffic encryption. • Blockchain: Decentralized data transmission; enhanced privacy and security through smart contracts.
Middleware Layer	• Data Integrity Breaches • Unauthorized Access	• Information astuteness breaches include unauthorized modification or debasement of data stored or created in middleware structures, without a doubt skewing analytics, or driving poor decision-making based on altered or adulterated data. • Unauthorized access involves exploiting vulnerabilities in middleware systems to gain entry, potentially compromising the confidentiality of sensitive data, or allowing attackers to manipulate critical systems through illegitimate access.	• Cloud computing: Scalable cloud infrastructure; robust authentication mechanisms. • Blockchain: Transparency and data integrity checks; restricted access through consensus mechanisms.
Application Layer	• Injection Attacks • Authentication Bypass	• Injection attacks, such as SQL injection or code injection, take advantage of weaknesses in IoT applications to gain access. This can result in compromised databases, gaining unauthorized access, and often leading to data breaches or attackers gaining control of the system. • Authentication bypass occurs when attackers exploit weaknesses in authentication methods to gain unauthorized access to IoT applications or systems. They bypass the usual authentication processes, posing a threat to the overall security of the system.	• Cloud computing: Secure cloud storage; comprehensive user rights management. • Blockchain: Encrypted data storage on the blockchain; user control over data sharing.
Business Layer	• Data Breaches • Insider Threats	• Data breaches occur when unauthorized individuals gain access to sensitive information within the business layer. This can result in the exposure of proprietary data, theft of intellectual property, or violation of privacy regulations. Such incidents have the potential to cause extensive damage to the overall ecosystem. • Insider threats refer to situations where trusted individuals within an organization misuse their privileges, whether intentionally or unintentionally, to compromise IoT systems. This can sometimes lead to significant harm to data integrity, confidentiality, or system stability.	• Cloud computing: Cloud analytics for real-time threat detection; compliance as a service. • Blockchain: Immutable audit trails; automated compliance and verification via smart contracts.

which proves your identity helps make the device more secure [19]. Users should also regularly check and control their privacy settings, turn off things they do not need, and separate their IoT devices from important systems. It is also necessary to monitor what your devices are doing and watch out for anything strange or someone gaining access without permission. If everyone follows these good rules, learns more about security, and actively works to keep things safe, it creates a strong defense against possible problems with IoT security can be created, helping make the whole system safer for everyone involved [14].

B. CLOUD COMPUTING

Cloud computing presents a significant change in how we perform tasks using technology. It has completely changed how we get and use computing services like servers, storage, databases, networking, software, and more. Instead of having everything on our own computers or servers, we can now access and use these services over the internet, which means we can get what we need whenever we need it from a shared group of resources that can be easily adjusted. Cloud computing works in different ways, and there are three main types: Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS) [25]. IaaS allows people to rent virtualized computing things, such as servers and storage, meaning they can have a flexible and scalable setup without having to worry about taking care of physical hardware. PaaS gives developers a platform and tools to create, deploy, and handle applications. It makes things easier by hiding the complicated details of the infrastructure. Meanwhile, SaaS delivers fully ready-to-use software applications over the internet. You do not have to install anything; you can access them directly through web browsers or application interfaces. The importance of cloud computing is that it gives you the power to easily adjust the size, flexibility, cost, and access to computing resources. This helps businesses, developers, and users incorporate computing power efficiently, be creative quickly, and handle changing needs without the need to deal with physical infrastructure [25]. This technology is still changing industries, encouraging new ideas, and shaping how we do modern computing. It is all about being quick, scalable, and using resources efficiently on a global level [25].

1) CLOUD COMPUTING SERVICE MODELS

Cloud computing provides different ways to help with various needs, and each way has its own job and features. Infrastructure as a Service (IaaS) is one of them. With IaaS, people can get virtualized computing things over the internet. They can rent servers, storage, and networking parts without having to own or manage the physical equipment themselves. Users using Infrastructure as a Service (IaaS) have control over the operating systems, applications, and development frameworks on this virtualized infrastructure. This gives them the power to easily adjust and manage hardware setups, making it scalable and flexible. Platform as a Service (PaaS) makes things even simpler. It hides the complex infrastructure details and gives users a platform where they can create, launch, and handle applications without worrying about hardware complexity. PaaS includes tools, development environments, and middleware, letting developers concentrate entirely on creating and deploying applications. Software as a Service (SaaS) is like having fully prepared software applications available online. Users can employ these applications without having to worry about the underlying infrastructure, platform, or software updates. SaaS includes applications for different purposes, including email services, Customer Relationship Management (CRM), and office productivity tools. Each service model, whether IaaS, PaaS, or SaaS, offers different levels of user control and

responsibility, so organizations can choose the one that suits their needs, including how they like to work.

- **IaaS:** This model provides virtualized computing resources through the internet. With IaaS, users can rent such services as virtual machines, storage, and networking, giving them greater control over their security measures, including handling network and access controls, keeping the operating system up to date, and enables security system configuration.
- **PaaS:** This model gives developers a platform and tools to create, launch, and handle applications without having to worry about the complicated details of the infrastructure. When it comes to security, this means making sure the development environment is secure, keeping Application Programming Interfaces (APIs) safe, and controlling access to data to prevent unauthorized changes.
- **SaaS:** This model brings software applications directly to users over the Internet, removing the need for users to install, maintain, or handle the software. Instead, they can use the software through a web browser or application interface. Security concerns in SaaS focus on encrypting data when it is sent and stored, using secure ways to confirm who is using the software, and making sure everything follows the rules and regulations to keep user data safe.

Figure 3 illustrates the differences between IaaS, PaaS, and SaaS infrastructure, platform, and software management in cloud computing.

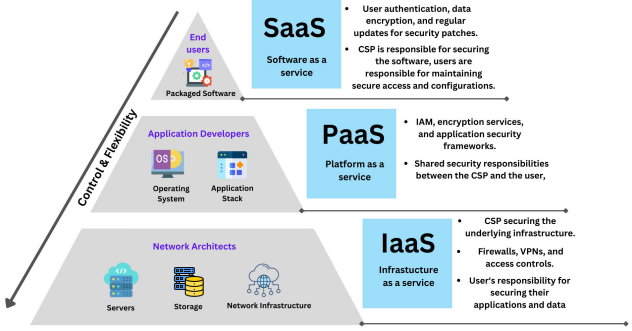

FIGURE 3. Cloud Computing Service Models.

2) CLOUD COMPUTING DEVELOPMENT MODELS

Cloud computing has different architectures: public, private, hybrid, and community clouds. These represent various ways of owning, accessing, and using the cloud, each with its own features. Keeping these different cloud models safe needs different strategies because they have different structures and levels of control. In a public cloud setup, where outside companies offer services used by many people, the main security concerns are protecting data, controlling access, and following rules. In this case, the company providing the cloud service accounts for securing the basic setup, while users are in responsible for keeping their applications and data safe. Keeping sensitive information safe and reducing risks related to shared resources is crucial. Encryption, identity management, and secure access controls play a key role in achieving this. On the other hand, a private cloud provides resources exclusively to one organization, giving more control and the ability to customize security measures [25]. When it comes to security in a private cloud, the focus is on defending the perimeter, having strict access controls, and using strong authentication methods. This is to prevent threats from people within the organization and unauthorized access. In a hybrid cloud, which mixes features of both public and private clouds, a full security plan is needed. It should handle challenges in making different systems work together, moving data between them, and keeping security rules consistent. In this hybrid setup, it is important to use strong encryption, identity association, and standardized security methods to ensure data is kept safe and private throughout the entire system [25]. In summary, when we talk about public clouds, we trust the company providing cloud services to keep our information safe. On the other hand, private clouds give us more control over our data. Hybrid clouds combine both public and private approaches to ensure everything is secure. However, as more people use cloud technology, worries about safety come up. Things like data breaches, managing who can access what, following rules, and making sure data is transmitted safely are significant challenges that need attention [26]. Ensuring that information in cloud systems is kept private, accurate, and available is important. This means we need strong security measures and strict rules to protect us against various cyber threats. Dealing with these challenges leads to ongoing improvements and new ideas in cloud security. This is crucial to keep people trusting and relying on cloud services. In Table 4, we provide a simple comparison of public, private, and hybrid cloud models. It clarifies different aspects such as control, access control, responsibility, data confidentiality, compliance, scalability, and flexibility from a security perspective. Additionally, Figure 4 illustrates differences between public, private, hybrid, and community in terms of ownership, accessibility, and functionalities.

3) CLOUD COMPUTING LIMITATIONS AND CHALLENGES

Keeping things safe in cloud computing is tricky because there are many different and complicated challenges. We need smart plans to handle them well. One significant worry is people accessing the system without permission. This could lead to breaches, where important data or resources might be accessed or messed with [27]. When there are weaknesses or gaps in how data is protected in the cloud, it can lead to data breaches. This is when private information is exposed and can be a result of vulnerabilities or problems with how the data is encrypted. Sometimes, people from within a system, whether on purpose or by mistake, can pose a threat. This is called insider threats. To deal with this risk, it is important

TABLE 2. Cloud Computing Deployment Models.

Aspect	Public Cloud	Private Cloud	Hybrid Cloud
Control	Limited control over infrastructure; CSP manages security of underlying infrastructure shared among multiple users.	Higher degree of control; dedicated resources for a single organization allowing for customization of security measures.	Intermediate level of control; a combination of public and private clouds, requiring a cohesive security approach.
Access Control	Emphasis on user authentication, access control, and encryption to protect data from unauthorized access.	Strict access controls at the organization level; additional layers of security for internal networks and data.	Requires consistent access controls across both public and private environments; may involve federated identity management.
Responsibility	CSP is responsible for securing underlying infrastructure; users are responsible for securing their applications and data.	Both CSP and the organization share security responsibilities; the organization has more control over security measures.	Shared security responsibilities between CSP and organization; requires coordination and agreement on security policies.
Data Confidentiality and Compliance	Concerns about shared environment security and data privacy; encryption and compliance measures essential.	Enhanced data confidentiality due to dedicated resources; strict adherence to compliance requirements.	Challenges in maintaining data confidentiality and compliance across hybrid environments; encryption and compliance measures needed for both environments.
Scalability and Flexibility	High scalability; flexibility in resource allocation but may impact security due to shared environment.	Scalable with tailored security measures; more flexibility in customization.	Offers scalability with a balance between control and flexibility; requires adaptable security solutions.

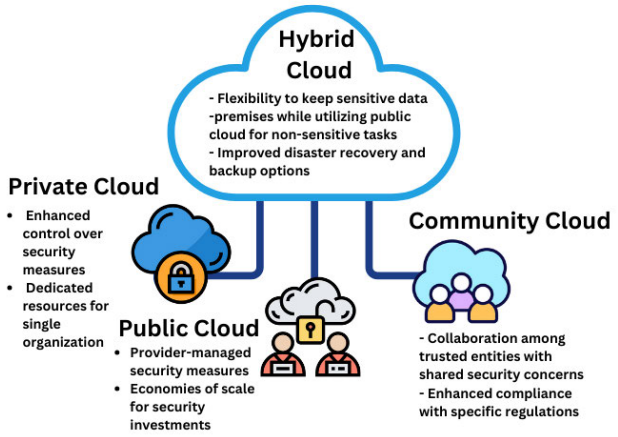

FIGURE 4. Cloud Computing Deployment Models.

to have strong rules about who can access what and keep a close watch to stop any misuse by people inside the system. Account hijacking is a significant problem when attackers get hold of user credentials. This is a serious threat. Also, weaknesses in shared resources can affect many users, so it is important to have strong measures to keep things separate and secure. To deal with these problems, it is crucial to use a strong approach, including encryption, regular audits, teaching users, and having strict rules about who can access what. This helps make cloud systems more secure against changing risks. Security frameworks can have limitations because cloud systems are always changing, making it hard to set up strong defenses. There are different types of threats like malware, phishing attacks, and DDoS attacks that make things even more complicated. Malware is a threat because it can sneak into cloud networks and mess up how data is kept safe or how the system works. Phishing attacks are another threat; they trick users into sharing sensitive information, which could lead to data breaches. DDoS attacks occur when a large volume of internet traffic is directed at cloud systems simultaneously, overwhelming them and leading to service disruptions or shutdowns [28]. Figuring out and making sure who is responsible for what is in the cloud, between the providers and users, can be tricky. To handle this, it is important to keep making security plans better. This includes having strict rules about access controls, using encryption, updating things regularly, and regular monitoring. This helps make cloud systems stronger against changing threats and challenges.

4) BEST PRACTICES TO SECURE CLOUD COMPUTING

Keeping cloud computing secure involves important steps to protect data and systems. First, using encryption is important. It makes sure that data is safe, whether it is in reset or transit so that even if someone tries to intercept it, they will not be able to understand it [28]. Using strong access controls and authentication methods is important to stop unauthorized people from accessing cloud systems. It is like having solid locks and keys to keep unwanted visitors out [28]. Making sure to regularly update software and systems with security patches and fixes is crucial. This helps protect against known weaknesses and keeps everything as safe as possible. It is like giving your computer or system a shield to defend against potential problems. Having strong rules for passwords and using multi-factor authentication gives an extra layer of security. It is like having a double lock on your door to ensure only the right people get in. Also, doing regular security checks helps find and fix any possible problems or risks, making everything more secure. Teaching and guiding users on how to follow security rules and do things safely is important. It is like making sure everyone knows the right way to keep things secure. Also, it is crucial to clearly define who does what between the cloud providers and the users, as per the shared responsibility model. Keeping an eye on

cloud systems all the time helps catch anything suspicious quickly, so we can respond fast to potential threats. Following the rules and standards set by the industry makes sure we are doing things in the right way. Finally, the best way to make cloud computing secure is to use a careful and active approach that includes all these good practices. There are several important aspects to focus on to ensure everything is protected well which are summarized as follows:

- Data Encryption: ensure to encrypt data in transit and data in rest, which helps prevent unauthorized access if someone tries to intercept it.
- Access Controls: Applying strong access controls and authentication methods to restrict access only to authorized users, enhancing security by preventing unauthorized entry.
- Regular Updates: ensure to regularly update software, apply patches, and install security fixes to address any known vulnerabilities and keep the system secure.
- Strong Authentication: Enforcing strict rules for passwords and using multi-factor authentication to add extra layers of security.
- Security Audits: Regularly perform security audits to find and fix any potential weaknesses or risks in the system.
- User Training: Teach clients about security conventions and first-class practices to cultivate a safety-conscious way of life.
- Clear Responsibilities: Characterize clean parts among cloud carriers and clients beneath the shared commitment form.
- Continuous Monitoring: Screen cloud situations as often as possible for suspicious exercises or peculiarities, permitting provoke reactions to capacity dangers.
- Compliance Adherence: Guarantee adherence to venture compliance necessities and rules for strong security hones.
- Comprehensive Approach: Utilize a proactive and comprehensive strategy, combining these components, to make strides in cloud computing security viably.

C. IOT AND CLOUD COMPUTING INTEGRATION

Various sectors engaged in IoT, including genomics data processing, education, small and medium business services, augmented reality, manufacturing, emergency recovery, smart cities, remote forensics, hospitality, e-government, human resources, and the Internet of Cars, make use of cloud computing services [14], [29]. There are unique challenges inherent in cloud computing, IoT, and their application environments [30]. Cloud computing and the IoT present distinct challenges in their application environments. Cloud computing's main challenge lies in security. Storing vast amounts of data on remote servers makes it susceptible to cyber threats, requiring robust encryption and authentication measures to safeguard sensitive information. Additionally, ensuring constant availability and reliability of services in the cloud is vital, demanding efficient infrastructure and redundancy planning to prevent downtime [30]. IoT, on the other hand, grapples with interoperability issues among devices from different manufacturers. Connecting diverse devices and systems involves varying protocols and standards, leading to compatibility hurdles that hinder seamless communication. Furthermore, IoT devices often operate on low power, making energy efficiency a critical concern to prolong battery life and maintain consistent functionality. Balancing these challenges in cloud computing and IoT environments necessitates ongoing innovation in security protocols, standardization efforts, and energy-efficient designs to maximize their potential while addressing these inherent complexities. Research aiming to integrate IoT and Cloud Computing has encountered significant hurdles, resulting in inconclusive outcomes. The recent rapid global adoption of cloud computing and IoT holds substantial promise as they complement and influence each other significantly [31], [32]. Scholars have envisioned diverse cloud and IoT-related applications to gather and process data utilizing cloud storage and computational capabilities. This section intends to clarify the Cloud-IoT architecture, referencing a preceding (Figure 5) to explain the knowledge layers, interlinking the application, network, and sensing layers. IoT visualization protocols enable the representation of data-collecting objects through various IoT systems, facilitating their processing in the cloud for improved efficiency [33]. The application layer not only detects the environment but also concurrently sends requests to the cloud for processing data and obtaining results from sensor data [21]. Moreover, essential tasks include handling data from the sensor layer, conducting data analysis, and sharing information with IoT devices and related objects [34]. When connecting IoT systems with cloud technology, choosing the right type of cloud is a careful decision. A hybrid cloud setup seems like the best option because it can handle different challenges and make the most of both public and private cloud features. It is like finding the middle base to get the best of both [35]. When you connect IoT devices to a hybrid cloud system, it gives you a flexible and balanced way of doing things. The private part of the hybrid cloud makes sure that security is a top priority, especially for handling sensitive IoT data and following the rules. This way, the organization keeps control over important tasks and data, reducing the chances of problems like breaches. It is like having the best of both in which we can gain flexibility and strong security [35]. At the same time, the public part of the hybrid cloud gives us the ability to grow, reach, and handle the flow of data from IoT devices in a way that is efficient and does not cost a lot. It makes processing and analyzing data from IoT devices smooth. The hybrid cloud can adjust resources as needed, making sure data analysis is done well, even when the workload from IoT devices changes. This keeps things responsive and reduces delays. Connecting IoT with a hybrid cloud can be tricky because it involves dealing with different environments, making sure everything works together, and effectively handling the complexity of the

hybrid infrastructure. Furthermore, dealing with how data is managed, following the rules, and keeping a unified security plan for both the public and private parts is a significant challenge. Even though the hybrid cloud's ability to be flexible and find a balance between security and growth makes it a strong choice for connecting IoT with cloud technology. It fits well with the various demands and details of IoT applications and how their data is handled.

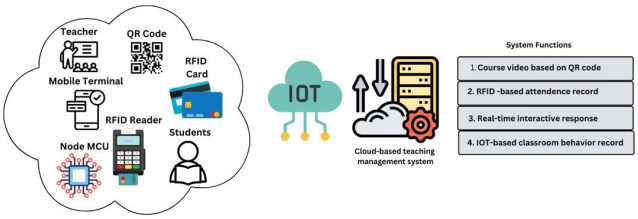

FIGURE 5. Cloud-IoT Environment.

In an IoT-Cloud environment, the combining of IoT devices with cloud computing makes it easier to handle data such as processing, storing, and analyzing. This integration lets the smart devices gather much information from different places and send it to the cloud for processing and storage. The cloud has strong and flexible computing abilities, so it can quickly analyze the data in real-time, find important details, and give us useful information to do actions. Also, the cloud provides a central hub to efficiently handle and control various smart devices. This collaboration allows businesses to use both smart devices and cloud computing together to make better decisions, improve how well things run, and create new and creative services for users. In education, combining smart devices with the cloud brings new solutions to make learning better, simplify administrative work, and overall, make things work more smoothly.

A real-life example is a smart classroom that has different smart IoT devices such as interactive whiteboards, smart projectors, and sensors. These devices will work to collect real-time data in the class like temperature, humidity, and lighting [36]. These smart devices gather information about what is happening, like what students are doing, how they are talking to each other, and what the environment is like. The information collected by these devices is sent to a special cloud platform made for schools. This cloud platform will process and analyze that data. For example, the information that is collected from the interactive whiteboards can clarify how interested students are or figure out which teaching materials work the best for them. Teachers and administration can log in to this cloud platform to get a better understanding of what is happening in the classroom. They can see how students are behaving, what is going on in lessons, and how well students are doing in their studies [36]. They could use special tools or dashboards on the cloud platform to check how students are learning. This helps them to understand where things can be better, and they can adjust their teaching methods right away based on what they see happening at the moment. Additionally, the online platform in the cloud makes it easy for students to work together on projects, even if they are not in the same place. Students can get their educational materials stored online from anywhere, allowing them to learn from a distance, collaborate on assignments remotely, and share learning materials. The integration of IoT and cloud in education is not just about making teaching modern it is also helping teachers make decisions based on data. It creates a more engaging and personalized way of learning, making things easier for teachers and improving the quality of education.

Another real-world example that shows how IoT devices and cloud computing work together in a smart city. In smart cities, sensors will be in things like traffic lights, garbage systems, and buses. These sensors are always collecting information in the city [37]. These smart devices will gather data such as how traffic flows, the amount of waste, the air quality, and how much energy is being used. After collecting this information, it is sent to the cloud which has strong tools for storing and analyzing data. The cloud's powerful resources handle and analyze the data right away. For example, data about traffic gathered by the smart sensors can be looked at in the cloud to make traffic move better, find where there are traffic jams, and change traffic lights to make things work more efficiently. Also, the cloud's ability to expand and store a large amount of data means that cities can keep records of past information for a long time. This lets city planners and administrators thoroughly study the data and make decisions based on what they learn [37]. These findings could include things like noticing how much energy people use, understanding how waste is generated, or identifying places where there might be a risk of environmental pollution. Integrating IoT devices and cloud computing will help cities run better. This means they can use resources smarter, make better decisions, and improve life for people who live there. This integration will allow cities to use data in decision-making and development.

When devices communicate over the Internet, they use two main protocols: the Simple Object Access Protocol (SOAP) and the Representational State Transfer (RESTful) architecture used by web servers. The most common protocol is the Hypertext Transfer Protocol (HTTP), which is especially important for systems and resources with limited energy. SOAP web services share information using extensible Markup Language (XML), while HTTP is widely used in most Web Services Security (WSS) standards [33]. The Constrained Application Protocol (CoAP) mandates the use of RESTful services for computers with limited resources, facilitating wireless communication among devices with constrained access. CoAP operates using the Hypertext Transfer Protocol (HTTP) protocol instead of the more common Transmission Control Protocol (TCP) protocol employed by UDP [21].

Cloud computing has evolved into a platform for data storage and processing applications, commonly utilized by IoT sensors for this purpose [38]. It not only offers innovative

commercial models but also opportunities to enhance existing information systems. Nevertheless, the integration of IoT and cloud computing raises significant concerns regarding privacy and security [22]. The objective is to convert conventional resources like sensors and machines into intelligent entities, providing users with dependable decision-making tools. Scholars have introduced frameworks, such as integrating the Health Level 7 protocol with IoT, for real-time healthcare monitoring utilizing cloud computing [39]. CoAP has emerged as an advanced architecture that fulfills real-time requirements when combining IoT and cloud computing [24]. Architectural diagrams that encompass the cloud, network, gateway, and devices serve to illustrate the infrastructure of the IoT [22]. Cloud computing offers a valuable solution for the management of IoT services and the composition of applications [7]. The recent increase in surveys and resulting product developments highlight the peak achieved in the convergence of cloud computing and IoT [40], [41].

The integration of cloud computing and IoT presents significant opportunities across various domains. IoT's capacity to interconnect diverse objects can be harnessed by the cloud to reach physical entities. With its limitless capabilities and resources, cloud computing aids IoT in overcoming technological constraints related to energy, processing, and storage. Additionally, it manages applications that utilize IoT data. Meanwhile, the cloud benefits from IoT's expansive reach, employing dynamic and distributed methods to engage with physical sensors, delivering new services across real-world scenarios. Many researchers are exploring the combined potential of cloud computing and IoT, seeking tailored advantages in specific applications [42]. Figure 6 illustrates an architecture that integrates cloud and IoT technologies. The integration of IoT sensors, cloud servers, and client devices operates within a sophisticated interconnected system, revolutionizing the way data is gathered, processed, and utilized. IoT sensors, implanted in different contraptions, obtain actual-time data from the encompassing environment, beginning from temperature and stickiness to development and region. These sensors transmit the collected measurements to a cloud server through wi-fi or wired systems. The cloud server, which has significant storage and processing capabilities will store and analyze this large amount of data [26]. Leveraging powerful algorithms and machine learning, the server interprets the information, extracting valuable insights and patterns. People use devices like smartphones, tablets, or computers to get information that has been processed. They can do this through apps or interfaces, which lets them check, control, and make decisions remotely. This integration is made possible by using standardized means of communication like MQTT or HTTP. These ensure that the different parts can connect smoothly. Creating this linked system requires careful planning of where to put sensors, how the network is set up, and making sure data is transmitted securely. This ensures that the different parts of the IoT system can communicate effectively and safely. This setup allows for various applications in different industries, like making homes smarter, automating industry processes, and improving healthcare.

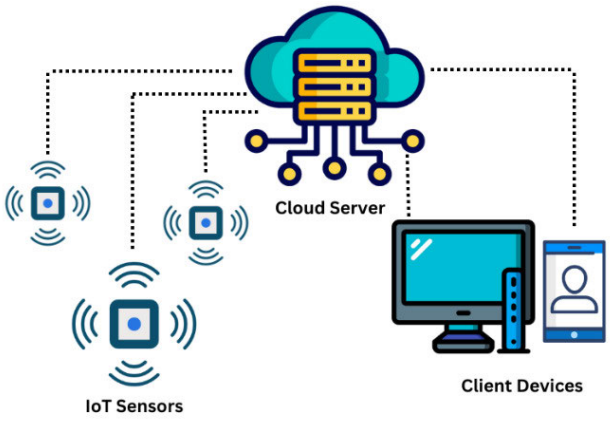

FIGURE 6. IoT and Cloud Computing Integration.

D. BLOCKCHAIN

1) BLOCKCHAIN OVERVIEW

As new technologies like cloud computing, edge computing, IoT, and significant data become more common, we need new ways to handle systems that are spread out and not centrally controlled. Because all these technologies operate online, there is an increasing number of malevolent users and attackers, which leads to security problems [43]. Furthermore, because the volume of data and susceptible devices is growing, it is critical to enforce verified and trustworthy services these days.

One of the various digital technologies accessible today that aids organizations in achieving their objectives by resolving the previously mentioned problems is blockchain technology. It is a distributed ledger of transactions that is immutable [44]. The trades are arranged chronologically here to assist users in tracking transactions without the need for a central authority or record keeper. Different sophisticated consensus algorithms are used to protect an operation or marketing in a non-trusted decentralized environment (i.e., blockchain network). A blockchain-distributed database's primary characteristics include improved security, immutability, decentralized systems, and quicker settlement. Peer-to-peer (P2P) networks, in which every computer is connected to every other computer without a central authority, are used to store the distributed database's details across different computer networks or systems [44].

Every computer is referred to as a node in a blockchain network, and every node is linked to its predecessor node. Blockchain uses public-key cryptography using private and public keys to sign transactions digitally. There is a mathematical correlation between the two keys. A message or piece of data is signed and encrypted by the sender using their public key. The receiver is the one who uses their private key to decode the data or message.

The main idea of blockchain was first presented in 1991. To prevent hackers and other malevolent users from tampering with the records, an automated ledger that signed the papers at that time was a chain or block of data with a digital signature. The Bitcoin blockchain was originally conceived by Satoshi Nakamoto in 2008 [45]. Its foundation is Distributed Ledger Technology (DLT), with blockchain being introduced for the first time in 2009. The idea of blockchain was utilized to create Bitcoin, a decentralized cryptocurrency. Blockchain facilitates the verification and authentication of Bitcoin transactions as well. Consequently, an overload of digital currencies, like Ethereum, Ripple, and Litecoin, has surfaced through the utilization of blockchain technology [45]. Blockchain mostly stores transaction data between entities in supply chain management systems. Diverse blockchain implementations inside the public blockchain exhibit distinct design schemas concerning aspects like decentralization, variability, consensus methods, and design architecture emphasis.

Blockchains exist in a variety of shapes and sizes, but they usually serve the same four tasks. Distributed data storage (public ledger of transaction records), encryption, immutability, and consensus procedures are all examples of distributed data storage. Blockchain, a type of DLT, maintains encrypted data across a peer-to-peer network (P2P), connecting contiguous ''blocks'' of information into ''chains.'' All the information exchanged on the blockchain is visible to all network members. The consensus process ensures that data remains unchangeable in the network and stops the users from adding information to the ledger without proper authorization. Moreover, the structure of the blockchain prevents any alteration or tampering with previously recorded data in the chain. Making edits compromises the integrity of the distributed ledger.

2) BLOCKCHAIN TYPES

One of the commonly used methods to classify blockchains is based on membership or accessibility. In a publicly accessible ledger, a public blockchain operates in a fully decentralized manner. Users might require authorization to make changes or updates to the blockchain. Many cryptocurrencies are built using public blockchains [46]. Private blockchains are accessible only to specific host enterprises and are primarily utilized for internal audits and maintaining records. The consortium blockchain, also known as a hybrid blockchain, is semi-private and accessible to different organizational groups such as banks, energy suppliers, and hospitals. It enables more efficient transactions or shared information among these parties. The purpose of the blockchain determines its type, which could be a unique design structure. Private and consortium blockchains have lower levels of decentralization and serve a smaller number of users compared to public blockchains. As a result, they have the potential to be more sustainable and cost-effective than public blockchain [46].

3) CRYPTOCURRENCY

The term ''cryptocurrency'' is now widely used by businesses and academics. Transactions in the Bitcoin network may occur without the involvement of a third party with a specifically created data storage structure. The blockchain, introduced in 2008 and used in 2009, is the fundamental technology behind Bitcoin [43]. A list of blocks contains all committed transactions, and blockchain may be considered a public ledger. As fresh blocks are consistently added to it, this chain gets longer. Asymmetric cryptography and distributed consensus techniques are used for user security and ledger consistency.

The primary focus of any cryptosystem is to ensure the CIA triad confidentiality, integrity, and availability to offer a comprehensive security strategy that protects all sensitive and important data [43]. These main cybersecurity objectives face a major threat known as data theft. Over time, various solutions have been suggested to overcome this issue, and blockchain is one of the most recent technologies aimed at addressing this issue. Data is vulnerable to multiple cases of plagiarism and theft while being transported and stored, which makes it difficult how to distinguish between the original and fraudulent data. Blockchain can eliminate these situations. A blockchain is a decentralized database that records and shares each event or transaction among the parties.

4) CRYPTOGRAPHY IN BLOCKCHAIN

- **Encryption algorithms:**
  The core concept of cryptography is to encrypt data in a way to ensures confidentiality, preventing unauthorized users from understanding or decrypting it. Cryptography is used for two main purposes: to securely transmit data over unsecured channels such as the Internet and to prevent unauthorized individuals from accessing the information they see. The term ''plaintext'' in cryptography refers to the information hidden, while ''encryption'' is hiding the plaintext. The encrypted plaintext is referred to as ''ciphertext. Encryption algorithms are a collection of rules that help carry out this process. An ''encryption key,'' which is subsequently supplied to the encryption algorithm as input along with the data, is typically used in the encryption process. The receiving side can obtain the data by employing the relevant ''decryption key'' in conjunction with a decryption algorithm.
- **Hash functions:**
  Hash functions in cryptography one of the cryptographic primitives that may be used to guarantee data integrity is the hash, which typically neither encrypts nor decrypts communications. Hash functions may map inputs of any size to a fixed-size output, and the output produced is known as a hash or digest. The Trapdoor One-Way (TOWF) principle is used to construct hash functions, and the hash function is unidirectional. When a message of any length is transformed into a collection of n bits

TABLE 3. Characteristics of Blockchain's.

Qualities	Public Blockchain	Private Blockchain	Hybrid blockchain
Gain access	Anybody	Only one company	Several organizations
Read / Write Authorization	Not authorized	Authorized	Authorized
Security	Could be malicious	Trusted	Trusted
Type of network	Decentralized	A little bit decentralized	Decentralized
Data in Blockchain	No finality	Facilitated finality	Facilitated finality
Immutability	Infeasible to tamper	Controlled and could be tampered	Could be manipulated
Scalability	High	High	Low

by a hash function, the number of potential hashes is less than that of distinct input messages. A significant component of blockchain security is hash functions. An attacker must utilize all 2256 possible critical combinations to crack a 256-bit private key. If a standard supercomputer capable of processing 1018 keys per second is employed to break into such a system, it will take 3*1051 years to locate the key.

- **Digital signature:**
  A standard digital signature is a mathematical system based on public-key cryptography that uses a private key to generate shortcodes known as digital message signatures, which can then be verified using the matching public key. Digital signatures prevent digital messages from being altered or forged in this situation. Blockchain technology employs a signature technique to sign the transaction, verifying the sender's identity and ensuring transaction integrity and sender non-repudiation. Many signature techniques use blockchain's integrity and anonymity. One of the most crucial cryptographic building blocks that enables blockchain to have attainable consensus and be publicly verifiable is the digital signature [47].
  In addition to hash functions, another fundamental cryptographic building element of blockchains is the digital signature. An electronic signature serves as an authentication tool that enables a message originator to affix a secret code to their message, acting as a signature and ensuring the communication's integrity and origin. Furthermore, disagreements between several parties may arise if a digital signature is missing. Today, digital signatures are used extensively in a variety of contexts to guarantee authenticity, integrity, and non-repudiation. Digital Signature Algorithms (DSA) and Hash Function Algorithms are the two types of algorithms used to create a digital signature.
  Almost all blockchains use signature mechanisms to sign transactions. They work by confirming the sender's identity, guaranteeing the integrity of the transaction, and preventing the sender from taking back their actions. A standard digital signature is a mathematical technique based on public-key cryptography that creates digital message signatures, or short codes, with a private key and a corresponding public key for verification. In this case, advanced marks prevent virtual messages from being adjusted or manufactured. Blockchain time employs a signature procedure to sign the exchange and confirm the sender's recognizable proof to form certain exchange judgments and sender non-repudiation. It is well known that the bounty of signature methods makes utilization of the namelessness and judgment of blockchain period. The virtual signature is one of the foremost vital cryptographic developing components that grants blockchain to be freely unquestionable and include the potential agreement.
  The advanced signature is another basic cryptographic component that shapes the motivation of blockchains and hash highlights. A mystery code that serves as a signature and ensures the verbal exchange's keenness and beginning can be added to a message by way of the sender utilizing an electronic signature. Besides, the nonattendance of a digital signature caused a debate between one or two parties. These days, numerous circumstances utilize advanced marks to create certain non-repudiation, judgment, and legitimacy.
  Moreover, blockchain nodes, or verifiers, verify the legitimacy of a signature on a transaction or block using the signer's public key. Blockchain offers additional features like unlikability, privacy, and anonymity by utilizing a variety of signature mechanisms. A signature technique can also be used to generate signatures of uniform size by utilizing signature aggregation. Blockchain technology makes use of several signature schemes, including [47]:
  - **Multi-Signature:** In a multi-signature system, multiple users sign the same communication. Using a multi-signature technique could be helpful when a blockchain transaction requires the signatures of various participants.
  - **Blind Signature:** In privacy-related protocols, this system employs signatures, but the parties who sign the message (or transaction, in the case of a blockchain) are different from the signer. Blind signatures are used to guarantee unlikability and transaction secrecy.

5) DISTRIBUTED LEDGER TECHNOLOGY (DLT)

DLT has gained popularity in recent years. Emerged as a means of capturing the advancements of blockchain technology and variations that broaden its core concepts [45]. In the context of modern blockchain technology, the phrase typically describes decentralized ecosystems managed by

consensus procedures in which most participants ultimately reach the same decision. All the data (such as., exchanges of digital assets) in such decentralized ecosystems are arranged as a chain of blocks and replicated among all network maintainers (miners), much like the Bitcoin blockchain [43]. Distributed ledger technology, or DLT, is any shared ledger, regardless of the underlying data type. The identical copies of information are duplicated across a decentralized network, ensuring their maintenance. The data is collected across several nodes in various geographical locations. To establish a shared truth that allows the data in the shared ledger to be verified and aware of tampering, the network's nodes reconcile their versions of the data concurrently through consensus. The success of DLT depends on the consensus process, which helps with the deterministic ordering of all valid transactions. The fundamental technology that underpins DLTs today, traditionally distributed systems, employs two types of mainstream consensus methods: non-byzantine and byzantine. An overview of these mechanisms is given in this section.

- **An overview of consensus mechanisms:**
  Consensus is a distributed computing technology that helps a dispersed network decide how much-shared data is worth. It primarily relies on two technologies: consensus procedures and information security protocols [48]. Proof of Work (PoW) serves as a consensus technique to ensure that the data stored in the ledger is accepted by the entire Distributed Ledger Technology (DLT) network. Information security measures like hashing and encryption safeguard data integrity and prevent unauthorized access. Public blockchains used in cryptocurrencies such as Ethereum and Bitcoin are considered the most recognized examples of Distributed Ledger Technology (DLT), which requires stronger consensus mechanisms across the network. Also, the PoW model used by Bitcoin is incredibly energy inefficient. The Raft algorithm creates three roles: Leader, Follower, and Candidate. The Raft creates uniformity by designating a Leader and giving him total control over the replication log. Because they maintain log replication, reply to written requests, and regularly send out heartbeat signals, a Leader with superior machine performance and stability can boost the consensus's efficiency. The Raft algorithm's election of the Leader could not guarantee that the Leader's performance was the best throughout the network since each node had an equal chance of becoming the Leader [48].
  The majority of consensus methods employed in consortium blockchains today are vote-based ones, and the performance of the leader node determines how effective they are. This is because, in these consensus algorithms, the leader node bears the primary responsibility for initiating the consensus process. When the leader node performs badly or becomes a malicious Byzantine node, the consortium blockchain performs poorly or creates an unsafe consensus. The information security technologies and consensus techniques employed in DLT are examined in this section.
  - **The Byzantine Consensus Mechanisms:**
    The first mention of the Byzantine general's problem was in Lamport's 1982 work [48]. This subject describes how to get honest generals to agree when there are a certain number of evil generals. Lamport proposed two approaches to deal with this problem. There are two kinds of solutions: one is signed, and the other involves an oral message. These two algorithms are complex because of their high communication complexity, but they made Practical Byzantine Fault Tolerance (PBFT) viable.
    Based on the Byzantine Generals problem, two types of faults in a distributed network can be distinguished: crash and Byzantine. Crash faults are sometimes known as non-Byzantine faults. They result from errors like loss and delay rather than malicious deeds. This is the distributed systems' most essential and frequent flaw. Known as Crash Fault Tolerance (CFT) consensus systems, these consensus mechanisms are specifically made to manage the failure that causes byzantine faults, which can lead to nasty behaviors like deliberately delaying messages and misleading other nodes [48]. This type of mistake requires a more complex fix. Byzantine Fault Tolerance (BFT) consensus techniques are the aggregate term for these consensus processes.
  - **Non-Byzantine Consensus Mechanisms:**
    It can be challenging to ensure convergence on agreement on a declared value or a sequence of operations in non-malicious (i.e., non-Byzantine) failure scenarios where some nodes fail. Whether the failures are fail-stop or fail-stuck, each participant reliably provides the same state and shares that the node has failed with the appropriate stop or stuck semantics [49]. On the other hand, in a malicious (that is., Byzantine) instance, a failing node could lead the other agents to observe things differently. The failed node may send a specific message to some nodes and a different one to other nodes.
- **Consensus techniques in blockchain:**
  There are different kinds of consensus mechanism algorithms, each of which works on different principles. In this systematic literature review paper, we will focus on two consensus mechanism algorithms PoW and PoS mechanisms. Below we will define the types of consensus mechanisms:
  - **PoW:**
    The first well-known blockchain mining method utilized by the Bitcoin network and documented in the literature was PoW. To avoid double spending, PoW mandates that each node (commonly called a ''miner'') that keeps a copy of the ledger

balance outgoing and incoming digital assets with previously verified transactions to validate a set of recently accessible, unconfirmed transactions [50]. The miner then adds confirmed transactions to a draft block. Subsequently, all miners compete with one another to solve a computationally demanding ''puzzle'' that verifies their block's authenticity and is inserted after the prior block in the chain. The only person who can answer the question correctly and upload their block of transactions to the shared ledger wins a mining reward in cryptocurrency, such as Bitcoins. Using this technique, tokens for native cryptocurrencies are also produced. The computationally costly problem at the center of the Proof-of-Work mechanism must be sufficiently challenging to solve to discourage attackers from trying to undermine the blockchain by making it unfeasible to find a solution. Similarly, for other nodes to accept the proposed solution and for the network to ascertain its accuracy, it must be easy to validate, irrespective of any node's processing capacity. The task for Bitcoin is to determine whether a ''nonce'' is necessary. This nonce is generated by combining the contents of the challenge block to create a new hash output that falls inside a target range, like a target hash prefixed with many 0s [50]. The only method available for computing the intended output of a nonce due to the nature of hashing algorithms is brute force, which entails attempting to guess each nonce one at a time until a solution is found. Therefore, which node will mine the next block and stop interfering with the validated transactions is unknown. It is regularly modified to maintain the problem at the same level multiple times. For instance, the Bitcoin puzzle takes 10 minutes on average to produce a block. PoW has proven crucial to preserving and protecting the functionality of Ethereum and Bitcoin, two of the most popular public blockchains. This is because potential attackers are discouraged by its high processing power needs and transparent information. Moreover, Bitcoin's motivation for competing to find a solution makes it harder for many rogue individuals to dominate and subjugate most network nodes. However, because of its excessive energy loss and consumption, the computational power required for PoW is highly controversial. Another primary concern is PoW's security vulnerability to a ''51 attack'' on public blockchain networks where several nodes compete for mining power [50]. An attacker may reverse transactions and obtain most of the web's computing power more quickly with such networks.

– **PoS:** Another consensus method frequently contrasting with PoW is PoS. PoS algorithms select the next eligible block to be added to the chain by considering the total amount of native cryptocurrency tokens each account currently holds. This helps to mitigate the energy consumption issue brought about by PoW algorithms, which require miners to solve a computationally expensive puzzle. Locking stakes for the term of service is often required of the stakeholders selected to oversee the PoW network [51]. Because PoS requires nodes to maintain the network with their token shares, it encourages nodes to construct and validate blocks appropriately. They risk losing their investment and future capacity to generate blocks if they commit fraud. Excellent and equitable stakeholders may be able to get access to their frozen claims. A certain transaction fee is also given to the block validator in exchange for correctly adding the block to the blockchain. Tokens for cryptocurrencies are frequently only issued during the platform's debut and the initial stages of the PoW mining process. PoS mining is utilized when a new block of transactions is uploaded to the blockchain. Even though the overall number of blocks each node can produce is weighted based on the percentage of stakes they possess across the network, nodes with more enormous stakes are frequently permitted to have more blocks than others in proof-of-stake networks. To prevent permanently favoring those with more tokens and centralizing the network, Proof of Stake, or PoS, takes a more sophisticated technique to choose the next block than simply relying on the validator's cash balance.
Instead, several strategies have been implemented to select the following Proof of Stake block. One such technique, created by Nxt and BlackCoin [51], selects the next block depending on the stake of the validator of a partnership and the hash generated by its validation by using randomness in the block selection process. Since all account balances in the shared ledger are visible to the whole network and are compensated with transaction fees, it is feasible to forecast the next block [51]. In the early stages of the PoW mining process and the platform's launch, tokens for cryptocurrencies are frequently the only ones created. Whenever a new block of transactions is uploaded to the blockchain, PoS mining is employed. Another method by which Peercoin generates the next block is based on how many and how old the tokens are in user accounts. The term ''coin age'' refers to this idea. When an arrangement creates a block, its currency age is reset to 0, and the counting process continues until the specified minimum age restriction is once more attained. Because of the high stakes, this eliminates the possibility that a single user or a small number

of users might profit from the system. PoS benefits energy efficiency since it does not require block generators to perform computationally intensive tasks. Similarly, PoS allows users to participate in block-building even with less capable computer hardware. However, with cryptocurrencies, stakes must be created beforehand by some other method, as Proof of Stake determines the block sequence according to the wealth of network maintainers. These stakes can be bought from other users who have previously acquired stakes or produced in a PoW-based system before transitioning to a PoS system.

- **Consensus processes are used in public blockchains**: Public blockchains provide the foundation for most cryptocurrency-based systems, such as Litecoin, Ethereum, and Bitcoin. Anyone with an Internet connection can update these public, decentralized, permissionless computer systems known as blockchains [43]. Anyone with such access can trade digital assets on these platforms. Users are urged to contribute to the networks by verifying transactions to earn digital tokens that can be used for trading commodities or in a shared market. Because public blockchains are "trustless," users can remain anonymous on the chain to protect their identity and feel safe knowing that their transactions are carried out honestly without having to build a relationship of trust with any parties or middlemen [44]. This is why users find public blockchains appealing. The most popular public blockchains are made to be append-only logs of transactions that are continuously confirmed and reconciled. After being verified by most network maintainers, a sequence of transactions is collected into a structured block and successfully mined. Because of this, the most recent block that has been mined is connected to the previous block in the series to preserve a coherent and consistent transaction history. Public blockchains must ensure that the shared ledger of transactions constantly provides the same image to whoever sees the chain at a given moment to prevent large quantities of trades in digital assets. Therefore, public blockchains typically use the most effective ways to reach consensus in highly decentralized worldwide networks. As a result, transactions entered public ledgers are transparent and unchangeable.

6) SMART CONTRACT

A smart contract is a program stored on the blockchain with ordinary transactions and executes its terms automatically if trustworthy intermediaries are not present. This has ushered in a new era for blockchain technology and profoundly altered the blockchain landscape. Smart contracts, the cornerstone of the blockchain, open a world of possibilities for supply chains, healthcare, digital identity, the IoT, and business process management [52]. The ultimate objectives of smart contracts are to do away with trusted intermediaries, minimize human interaction, lower the cost of enforcement, and guard against security threats and purposeful or accidental fraud.

Self-executing "smart contracts" kept up to date on a hosted blockchain allow agreements and connections to be codified and trusted [53]. Smart contracts facilitate automated transactions, eliminating the need for external financial institutions like banks, courts, or notaries to oversee them. This can contribute to the maintenance of dependable and secure company operations. These transactions are observable, traceable, and irreversible.

Formal verification is necessary to show that a contract code is correct for each input in its state space and that the contract functions as intended. The application of proof and verification in other conventional sectors has been limited due to the significant cost and labor involved. Therefore, traditional methods are essential for smart contract verification. On open blockchains, smart contracts are accessible from anywhere in the world [54]. Moreover, many smart contracts are immutable, which means that although they can be updated on some platforms, they are not easily fixable if a flaw or vulnerability later surfaced. Lastly, many smart contracts require expensive resources to run and store data [55]. This makes them very desirable targets for malicious individuals to attack. Therefore, formal verification is a helpful tactic that can reduce the likelihood of mistakes and defects in a contract and help ward off future hostile attacks.

7) NETWORK SECURITY AND ATTACKS

Blockchain maintains a decentralized distributed ledger that does away with the requirement for trustworthy intermediaries in transactional processes. A blockchain ledger consists of a series of blocks (see Figure 7), each linked to the one before it by a cryptographic hash [56]. Every block in a blockchain consists of two parts: the body and the genesis block. Blockchain maintains the ledger's immutability and state through a decentralized consensus process. Blockchain technology provides an immutable,

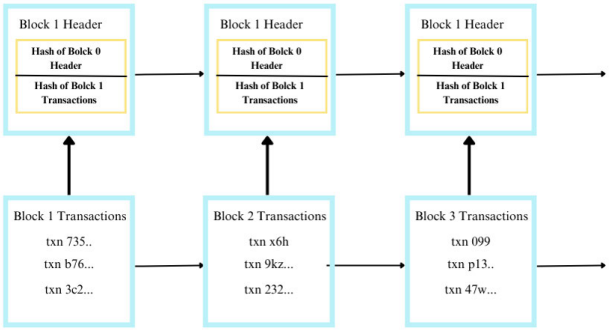

FIGURE 7. A blockchain ledger series of blocks.

distributed, and decentralized ledger. Every time a new block or transaction is generated on a peer-to-peer (P2P)

TABLE 4. Comparison of consensus mechanisms used in public blockchain.

Consensus mechanisms	Degree of decentralization	Scalability	Randomness in miner selection
PoW Byzantine consensus	High	Low	High
PoS Byzantine consensus	Medium	High	Medium

network, blockchain technology spreads the ledger around the web. Each transaction has a distinct, verifiable record in a ledger [57]. The popularity of Bitcoin has increased interest in blockchain research. Turing's full implementation of language-based smart contracts was essential to advancing blockchain technology.

Blockchain technology is gaining attraction in several industries. When financial assets are involved, security issues arise from the possibility of asset theft or hacker compromise of the system. Blockchain technology should improve data integrity, address security vulnerabilities, and make transactions decentralized, transparent, and irreversible. Thus, security is crucial to ensuring blockchain adoption. Blockchain systems are thought to be less susceptible due to their immutable records, decentralized consensus, and encryption.

- **Security Risks**:
  Technology is much sought after because it makes life simpler, but it is crucial to be aware of the security risks that the internet poses. The four most serious security flaws in blockchain systems: double-spending, Sybil, 51 percent attack, and DDoS attack are succinctly outlined in this section.
  1) **Sybil attack** : When an attacker takes on many identities at once, it is referred to as a Sybil attack. One of the primary issues with P2P network connections is this. It manipulates and influences the whole network by using several false identities. When seen in isolation, these several personas seem like ordinary individuals, but in the background, an individual identified only as the ''unknown attacker'' is in command of all these made-up companies simultaneously. The Sybil attacked the whole network. In this way, one might try to prevent data from being delivered or received by the network. Increasing the cost of obtaining an identity is the only way to decrease Sybil's attacks [58]. To keep new users from joining the network and creating legitimate identities, this spending needs to be balanced. It should also be high enough to suffer expenses in the process of creating many identities. For example, the miner nodes handle the validation and verification process of PoW blockchains, which need much computing power. The Sybil attack is challenging due to the associated computing power cost.
  2) **Double spending**: Double-spending is a type of data consistency attack when the same digital money (or digital asset) is spent twice. Double-spending is a strategy used to trick someone about the status of a transaction. The 51 percent attack is primarily cited as the reason for double-spending [59].
  3) **51 percent of attacks**: A 51 percent attack is an effort by a group of miners who control more than 50 percent of the network's mining hash rate or processing power to threaten a blockchain, which is presently not possible [58]. The attackers may prevent data transfer between users and IoT devices by preventing new transactions from getting confirmations. If the attackers led the network, they could also undo completed transactions.
  4) **DDoS**: When an attacker overwhelms the network with numerous requests in a single effort, it is known as a DDoS attack, which prevents users from accessing the network's resources. A denial-of-service attack occurs when these requests originate from the same source. A denial-of-service attack, on the other hand, originates from several sources of requests. In this case, it is difficult to defend against these attacks since we must first distinguish between legitimate and malicious requests.

IV. DISCUSSION

A. IOT AND CLOUD SECURITY CHALLENGES

There is a strong interconnection between the IoT and cloud computing, as each technology is considered supportive and complementary to the other technology. The IoT provides the ability to collect data from multiple devices and thus the ability to analyze significant data, while cloud computing provides huge resources to store, process, manage data, and improve the security of this data. Recently, these technologies have been depended upon within the technological landscape to develop decision-making processes, improve operations, and enable competition in various institutions [60].

For successful integration of cloud and IoT, various issues must be addressed to ensure benefits for the wider population. While the fusion of Cloud and IoT opens up numerous opportunities and possibilities, it also presents an expanded target for potential attackers. The integration involves diverse data types and services supported by multiple networks that require a flexible network structure capable of supporting a wide array of data and fulfilling quality of service requirements [32]. Addressing protection concerns is most important to prevent unauthorized admission of user information. The integration of IoT with cloud computing introduces a multitude of complicated protection challenges. Most

concern revolves around the full-size quantity of statistics generated by IoT tools, mainly vulnerabilities in information privacy and safety [32].

Securing and correctly dealing with sensitive facts face difficult situations due to the sheer volume and diversity of statistics transmitted from numerous IoT endpoints. This situation often leads to worries about protecting data, confirming identities, and controlling who can access it. Furthermore, as more IoT devices and the cloud are connected, there is a greater chance of cyber-attacks like hacking into personal information. Communication protocols and network infrastructure have weaknesses that can be used by bad people to intercept, change, or hack information being sent, creating significant security risks. Furthermore, as more IoT devices and the cloud are connected, there is a greater chance of cyber-attacks like hacking into personal information. Communication protocols and network infrastructure have weaknesses that can be used by bad people to intercept, change, or hack information being sent, creating significant security risks. Additionally, the limited resources in IoT devices make it difficult to have strong security features because there is not enough computing power and memory available. As more devices and systems connect to the Internet, it's important to ensure that they can work together and that their security measures can all work together too. To tackle those protection-demanding situations, complete techniques are wanted, which encompass implementing statistics encryption, robust authentication techniques, steady communication protocols, and frequently updating security features. These actions are intended to reinforce the integrity and confidentiality of information transmitted between IoT gadgets and the cloud. In this section, we can explore the problems related to the combination of cloud computing and IoT, drawing insights from current literature critiques.

1) QUALITY OF SERVICE

Managing QoS becomes a substantial situation when coping with increasing record volumes and evolving information characteristics. As specific kinds and quantities of records are reached theses record a set of them can be activated. Metrics including bandwidth, postpone, and packet loss ratio play pivotal roles in assessing the best carrier, highlighting the crucial need for QoS guide.

2) IDENTITY MANAGEMENT

Each node communicating over the Internet necessitates a unique identifier. As objects integrate into the IoT, they also require distinctive identification numbers. Moreover, mobile devices like sensor nodes on vehicles and various objects must possess the ability to self-identify within the emerging network. A practical approach to achieving this objective involves assigning IPv6 addresses. This is a viable solution as IPv6 addresses are considered adequate even for extensive ubiquitous networking scenarios.

3) DATA SECURITY

Data security stands out as a prominent among the top ten security challenges projected for 2020. Information held by government agencies, users, companies, banks, and other institutions often contains customers' details. Thus, to handle, collect, and use this information, organizations must comply with regional general information protection and security laws. Data security focuses on limiting access and permitting authenticated users to access, modify, and contribute to the data. Some papers we reviewed presumed that US authorities could potentially access and monitor user information. Therefore, to ensure the security of sensitive or private data, the virtual storage server must ideally be located within the user's country or a trusted geographical area.

4) SUPPORTED PROTOCOL

Various protocols can be utilized to connect diverse devices to the internet, but the gateway device supports certain protocols but cannot accommodate all. In a scenario in which various devices are being interconnected to the internet, the use of diverse protocols is expected to enable these devices to communicate effectively within the network. Multiple protocols indicate the need for a central hub or gateway device, that can as an intermediary between the devices and the broader internet infrastructure [4]. This gateway tool, although multipurpose, might not guide each protocol due to technological boundaries or strategic design alternatives. Therefore, it will be configured to deal with a specific set of protocols, ensuring compatibility and seamless verbal exchange among a variety of tools, even as brushing off these protocols does not assist. This technique might necessitate compatibility tests and modifications at some point in the network setup to accommodate the gateway's protocol limitations, ensuring gadgets communicate successfully within the network and benefit get admission to the internet, even via a subset of supported protocols.

The selection of which protocols the gateway supports might be encouraged by way of such elements as protection, efficiency, and compatibility with the intended devices, forming the primary component in permitting coherent connectivity at the same time and balancing the constraints of protocol diversity. Everything relies on the gateway including the sensor that is being used, so it is all up to the gateway. Users must decide whether to choose a cheaper or simpler sensor, as a result of which there is no guarantee that the added sensor will be configured properly. To overcome this issue, one solution is to integrate standardized protocols into the gateway, some of which are commonly viewed as essential for gateway support as follows [13]:

- **MQTT:** MQTT is a lightweight messaging protocol, great for devices with limited resources. It is an efficient protocol for transmitting data between devices, making it suitable for various IoT applications.
- **HTTP/HTTPS:** These protocols play a crucial role in communication and data transfer. HTTP enables communication between devices and servers, while HTTPS

enhances security by encrypting data, guaranteeing integrity and confidentiality.

- **CoAP:** This protocol is designed for devices with limitations in power and bandwidth, typically used in IoT networks for machine-machine communication. It is similar to HTTP but is better suited for devices with limited resources due to its efficiency in such environments.
- **TCP/IP:** Serves as the foundation of the internet, allowing devices to communicate and share data across networks. Moreover, to have effective communication with different devices and systems linked to the Internet, the gateway must support this kind of protocol.
- **UDP:** It is commonly used for real-time communication, and provides faster data transmission than TCP but lacks in error mechanisms. It might be essential for certain applications or devices within the IoT system that prioritize speed over error detection and correction.

Applying these protocols to the gateway device will improve the capability of communicating with various sensors and devices. Furthermore, this will ensure a better chance of successfully configuring and integrating any newly added sensors into the network [13]. Using these protocols in the gateway will solve the issue of the devices that utilize various communication protocols, leaving a flexible IoT environment.

5) RESOURCE ALLOCATION

Managing resources in a cloud environment becomes complicated when unexpected devices from the IoT ask for resources. The difficulty lies in predicting the specific resource requirements of an entity or IoT. Resource allocation should consider such factors as the type, quantity, and frequency of data generated by the sensor, as well as its intended usage. Furthermore, disparate resource locations can complicate the monitoring and correction of technical faults.

6) SIGNIFICANT DATA

In the upcoming years, the substantial stream of data will pose a significant challenge for cloud service providers. Managing this extensive amount of data will hamper the ability to offer rapid and secure access, subsequently leading to increased latency in data transmission.

7) ENERGY CONSUMPTION

As sensor networks proliferate globally and cloud connectivity expands, the escalated communication of data will result in a substantial power consumption increase. Envisioning a world in which billions of sensors and low-power devices operate collectively raises challenges. A requisite for such an environment involves an efficient energy utilization system and a consistent energy supply. Furthermore, sensors would need to harness power from the environment to generate their required energy, establishing a need for self-sustaining power generation systems.

8) COMPUTATIONAL PERFORMANCE

Addressing these challenges has led to a critical dependence on cloud service providers. However, the scalability of the cloud to handle workloads also renders it vulnerable to attacks that deplete resources once operations commence. Instances of such attacks include exploiting vulnerabilities in application communication and overwhelming protocols through excessive volume, as detailed in [4]. In these attacks, traffic nodes are produced by exploiting a compromised node within the system. By attempting to deactivate the network, the energy of this node is drained, confining the attack to the transport protocol layer.

B. IOT SECURITY CHALLENGES

- **Device Vulnerabilities:**
  IoT devices contain many weaknesses, the most notable of which is weak authentication as a result of devices relying on default or weak passwords, thus allowing unauthorized persons to access user data. Therefore, it is necessary to provide strong authentication mechanisms. IoT devices also suffer from a lack of encryption, which can expose them to many security threats as a result of their communication and transfer of data across networks. Finally, IoT devices suffer from firmware vulnerabilities because IoT resources impose restrictions to prevent updating the firmware; thus, this firmware could expose several security vulnerabilities that an attacker can exploit [61].
- **Data Privacy Concerns:**
  There are concerns related to data privacy, as IoT devices collect data from several sources, thus allowing attackers to listen to conversations that contain user identification data or sensitive data. In addition, IoT devices can contain sensitive data while being transferred or stored within a network; thus, the network can be exposed to a hack, causing sensitive data to be leaked and easily accessed [62].
- **Lack of Standardization:**
  Lack of standardization can cause problems with limited compatibility and interoperability between IoT devices and thus the inability to implement all functions. If IoT platforms and devices do not use the same protocols, it becomes impossible for them to work together, thus leading to security risks, reduced efficiency, and increased costs.
- **Physical Security:**
  IoT devices can be exposed to actual physical access, including unauthorized access to data and attempts to manipulate them. Therefore, it is necessary to address these risks by implementing security measures that include locking devices and applying tamper-evident

mechanisms, and device hardware must be designed to be tamper-resistant [63].

C. CLOUD SECURITY CHALLENGES

- **Data Breaches:**
  Data breaches, which happen when sensitive information is accessed without permission, are a significant problem in cloud computing. They occur mostly due to weak passwords, malicious software, and threats from inside the system, allowing unauthorized people access to important data and compromising security. Cloud computing faces various security threats, such as unauthorized access to accounts, which can lead to alterations or loss of data [64].
- **Identity and Access Management (IAM):**
  The problem is the server can be vulnerable to attackers who use security weaknesses to make fake requests and gain control over access management. In addition, mistakes in setting up cloud systems (misconfiguration) can lead to unauthorized access to these systems. The lack of authentication rules in systems will also lead to risks in clarifying the identity of the authorized user to access the cloud [65].
- **Compliance and Regulations:**
  Cloud services that operate across various hybrid networks might struggle to meet all data protection standards. To overcome this issue, integrating a specialized cloud security management solution can help meet these standards more effectively. However, managing multiple cloud services creates challenges in meeting information security standards. This is because responsibilities are divided among many individuals, leading to numerous decisions and changes. As well, the large amount of stored data creates opportunities for various attacks. Therefore, the compliance standards should be updated regularly based on the specific needs and size of each company.
- **Shared Responsibility Model:**
  The shared responsibility model aims to define the limits of responsibility between cloud service providers and users, as there are some gaps and misconceptions, the most notable of which are as follows:
  - Cloud provider certifications do not include compliance to protect all sensitive information data but are only responsible for some of the lower layers in the architecture.
  - Customers believe that their sensitive data, once stored on a major cloud provider, will be secure, but the service provider offers a set of tools and services that help secure the data (encryption, authentication, etc.), and the user must specify the security elements they wish to implement.

D. INTEGRATION CHALLENGES

- **IoT–Cloud Integration Security:**
  Security challenges include the possibility of unauthorized access to sensitive user data during its transfer from IoT devices to cloud computing, in addition to the possibility of data leakage due to the inability to implement encryption for all system layers. Finally, weak authentication can cause systems to be exposed to many security violations and can allow access to and the manipulation of user data [20].
- **Issues of integrating IoT and the cloud:**
  When integrating IoT devices with cloud computing, several security issues can arise. One significant concern is data privacy, as IoT devices collect vast amounts of sensitive information that is transmitted to cloud servers for storage and processing. However, ensuring data encryption and access control mechanisms are in place is crucial to protecting the confidentiality of these data and preventing unauthorized access.
  In addition, authentication and authorization mechanisms must be strong enough to verify the identities of devices and users accessing the IoT system through the cloud, as weak authentication can lead to security breaches and data leaks.
  Another critical security challenge is that without proper validation and integrity checks, the data transmitted between devices and the cloud may be at risk of tampering or manipulation, which will compromise its accuracy and reliability. Network security is also a key concern, as securing the communication channels between IoT devices and cloud servers is essential to preventing snoop, MitM attacks, and unauthorized data interception. Potentially, implementing encryption protocols and secure communication channels can help mitigate these network security risks [66].
  Furthermore, the security of IoT devices themselves poses a significant challenge, as these devices often have limited processing power and memory, making them susceptible to security threats, such as malware and unauthorized access. Regularly updating devices with security patches and implementing strong security measures is thus essential to protecting against potential vulnerabilities [66]. Addressing these security issues requires a comprehensive approach that includes powerful security measures, regular examinations, incident response plans, and awareness of emerging threats in IoT and cloud environments.
- **The role of cloud computing in enhancing security when integrating IoT and blockchain:**
  The integration of IoT and blockchain technology presents a unique opportunity to enhance security and trust in different applications. However, this integration also introduces new cybersecurity challenges that must be addressed. Cloud computing plays a critical role in addressing these cybersecurity issues by providing scalable resources and advanced security mechanisms.
  One of the key cybersecurity challenges in integrating IoT and blockchain is the secure storage and management of huge amounts of data generated by IoT devices. Cloud storage solutions can offer a secure and

scalable environment for storing these data, ensuring their integrity and confidentiality.

Moreover, cloud computing principles can enhance the security of blockchain networks by providing a strong infrastructure for hosting blockchain nodes [16]. Cloud-based blockchain solutions can improve the flexibility and availability of the network, which will reduce the risk of single points of failure and enhance overall security.

In addition, cloud platforms can offer advanced security features, such as encryption, access control, and monitoring, to protect blockchain transactions and data.

Furthermore, cloud services can facilitate secure communication between IoT devices and blockchain networks, through which cloud-based IoT gateways can act as intermediaries that will secure data transmission and authentication between IoT devices and blockchain nodes [16].

- **Blockchain's role in addressing security issues when integrating IoT and cloud:**

  Integrating the IoT and cloud computing presents numerous security challenges, such as data breaches, unauthorized access, and tampering. However, blockchain technology offers promising solutions to these issues due to its decentralized, transparent, and immutable nature [9].

  First, blockchain can enhance data integrity in IoT and cloud computing environments. Because blockchain records are immutable and distributed across multiple nodes, data alterations and tampering become nearly impossible without consent from the network. This ensures that data transmitted from IoT devices to the cloud remains unchanged and authentic. For instance, in a smart home system, the temperature data recorded by sensors can be securely transmitted to the cloud without the risk of manipulation, ensuring reliable data for automated climate control systems.

  Second, blockchain can improve authentication and access control in IoT ecosystems. Traditional centralized authentication systems are vulnerable to attacks, but blockchain enables decentralized authentication using cryptographic keys. Each IoT device can have a unique blockchain identity, and access can be controlled through smart contracts, which are self-executing contracts with the terms of the agreement directly written into code. This ensures that only authorized devices and users can access sensitive data and services, reducing the risk of unauthorized access.

  Third, blockchain enhances the transparency and traceability of transactions in IoT networks. Every transaction or data exchange is recorded on the blockchain, providing a clear and auditable trail of activities. This transparency helps with monitoring and identifying any suspicious activities or anomalies in real-time. For example, in a supply chain management system, blockchain can track the journey of goods from production to delivery, ensuring that each step is verified and recorded, thereby preventing counterfeiting and fraud.

  Finally, blockchain supports secure and decentralized data storage. Instead of relying on a central cloud server, data can be stored across a distributed network of nodes. This decentralization mitigates the risks associated with central points of failure, making the system more resilient against cyberattacks. In healthcare IoT, patient data can be securely stored and accessed only by authorized personnel, ensuring privacy and compliance with regulations, such as the Health Insurance Portability and Accountability Act (HIPAA).

  Table 5 below summarizes the key security challenges associated with integrating IoT and cloud computing and outlines how blockchain technology addresses each issue. By leveraging blockchain's decentralized, transparent, and immutable nature, these solutions enhance the overall security and integrity of IoT and cloud environments.

- **Possible security issues when integrating the IoT, cloud, and blockchain:**

  Integrating IoT, cloud computing, and blockchain technologies promises significant advancements in data management, security, and operational efficiency. However, this integration also introduces new security challenges that must be addressed to ensure the integrity and confidentiality of data and systems.

  One potential security issue is the complexity of managing a hybrid system involving IoT, cloud, and blockchain technologies, each of which has unique security requirements and vulnerabilities. IoT devices are often constrained in terms of computational power and security features, making them susceptible to attacks like device spoofing or firmware manipulation. Meanwhile, cloud environments, while scalable and efficient, can be vulnerable to data breaches and unauthorized access if not properly secured. Integrating blockchain adds another layer of complexity, requiring robust consensus mechanisms and secure smart contract implementations. Thus, ensuring cohesive security across all three layers is challenging and demands a comprehensive approach to managing and monitoring each component's security posture effectively.

  Another critical security issue is the potential for data privacy concerns. While blockchain provides transparency and immutability, these can conflict with privacy requirements. Sensitive data from IoT devices, when stored on the blockchain, become accessible to all members of the network. This could lead to the unintended exposure of private information, especially in such sectors as healthcare and finance. As such, techniques like zero-knowledge proofs or secure multi-party computation are necessary to balance transparency and privacy, but these add complexity and require careful implementation.

TABLE 5. Blockchain role in addressing security issues when integrating IoT and cloud.

Security Issue	Blockchain Solution	Benefits
Data integrity	Immutable and distributed records	Ensures data authenticity and prevents tampering
Authentication and access control	Decentralized authentication and smart contracts	Reduces unauthorized access and improves security
Transparency and traceability	Auditable trail of activities on the blockchain	Real-time monitoring and anomaly detection
Data storage	Decentralized storage across network nodes	Enhances resilience and mitigates central point of failure risks

Scalability and performance are also significant concerns when integrating these technologies. Blockchain networks, especially public ones, can experience latency and throughput issues due to the consensus mechanisms required for security. As well, IoT systems often generate vast amounts of data that must be processed and stored efficiently. Integrating blockchain may exacerbate these issues, as each transaction must be verified and recorded across the network, which can lead to performance bottlenecks and ineffective scaling for large IoT deployments without advanced solutions, like sharding or off-chain processing.

In addition, securing smart contracts used in blockchain to automate interactions between IoT devices and cloud services presents another challenge. Smart contracts, once deployed, cannot be easily altered. Therefore, any vulnerabilities or bugs in the code can be exploited, leading to potential financial losses or unauthorized actions. Ensuring the security and correctness of smart contracts through thorough testing, auditing, and formal verification is essential, but it can be resource-intensive. Table 6 below highlights the primary security issues that arise when integrating IoT, cloud computing, and blockchain technologies. Each issue is described in detail, along with the specific challenges and considerations that must be addressed to ensure a secure and effective integration of these advanced technologies. These security issues highlight the need for a multi-faceted approach to ensure the secure integration of IoT, cloud, and blockchain technologies. Balancing the strengths of each technology while addressing their inherent vulnerabilities is crucial to building robust and secure systems.

- **Interoperability:**
  The difference between IoT devices and computing systems in terms of using different protocols leads to incompatibility between them and thus difficulty communicating smoothly. As a result, limited services can be implemented, and there is a decrease in work efficiency in addition to increased costs.

E. SECURITY BEST PRACTICES AND SOLUTIONS

- **Encryption and Authentication:**
  Strong authentication methods help secure IoT devices and cloud services, as it is necessary to use biometrics and certificates to verify the identities of devices and users and thus prevent unauthorized access. However, encryption methods should be applied for data access when it transfers between devices and the cloud to ensure secure data transfer, which cannot be done [67].
- **Securing Patches and Updates:**
  Implementing organized updates and managing patches helps with processing security vulnerabilities in IoT platforms and cloud computing services. Cloud computing can share secure updates on all applications so no attacker can exploit security vulnerabilities to attack the network [67].
- **Observing and Incident Response:**
  Monitoring IoT systems helps in discovering any irregular status or likely security breach, so behavioral analysis tools are needed to analyze network data to notify users of any interrupting or malevolent situations so they can be reported. However, security threats must be addressed quickly by preparing communication strategies and implementing securing protocols to decrease any possible threats [67].

F. FUTURE TRENDS AND MITIGATION STRATEGIES

- **Emerging Technologies:** Blockchain technology is one improvement technology that helps to enhance IoT and cloud computing, as well as help with monitoring integrated data from different sources and sharing them in a secure and trusted way because of data encryption. These techniques depend on distributed records technology, which works to store all encrypted data, in addition to easily transforming data without the need for a third party, which helps enhance IoT and cloud computing.
- **Regulatory Developments:** Regulatory developments facing the IoT include hardware and mobility requirements, in addition to technical standardization, network numbering, and addressing mechanisms. These developments can impact data security, hence the need to develop security standards for IoT and cloud environments.

G. BLOCKCHAIN ADOPTION TO SECURE IOT AND CLOUD INTEGRATION

By adopting blockchain, the study aims to improve the security of integrating both technologies. This involves a network of blockchain, transaction, and mining nodes strategically positioned across user premises and within the cloud [9].

TABLE 6. Summary of security issues in integrating IoT, cloud, and blockchain.

Security Issue	Description	Challenges and Considerations
The complexity of a hybrid system	Managing unique security requirements and vulnerabilities of IoT, cloud, and blockchain	Ensuring cohesive security across all layers requires comprehensive monitoring and management
Data privacy concerns	Transparency of blockchain conflicts with privacy requirements	Balancing transparency and privacy with techniques like zero-knowledge proofs
Scalability and performance	Latency and throughput issues due to blockchain consensus mechanisms	Finding solutions to handle large amounts of IoT data efficiently and avoid performance bottlenecks
Smart contract security	Vulnerabilities and bugs in smart contracts leading to exploitation	Ensuring security and correctness through testing, auditing, and formal verification

These nodes encompass various systems, including enterprise servers, standalone PCs, and smart devices, acting as integral components. The blockchain clients, which represent IoT devices with limited resources, communicate with cloud-based blockchain transaction nodes using Representational State Transfer (REST) or HTTP APIs. These smart devices collect data and relay them to the transaction nodes, which, in turn, process this information.

To ensure security, smart devices are furnished with private keys for data signing. The signed data are subsequently sent to the transaction nodes for processing upstream. To ensure secure data communication, a mutual trust agreement is established between the IoT device and the transaction node. Such techniques as whitelisting and two-way authentication might be employed for secure one-to-one interaction between these devices [9].

The illustrated (Figure 8) portrays a secure data communication architecture tailored for IoT devices interacting with transaction nodes within a blockchain framework. It delineates the intricate process by which IoT devices equipped with private keys sign data before transmitting them securely to designated transaction nodes for upstream processing. The figure emphasizes the establishment of a mutual trust agreement between these devices and transaction nodes, highlighting the incorporation of advanced security techniques such as whitelisting and two-way authentication. By visually representing this architecture, the figure elucidates how blockchain technology serves as the underlying foundation, ensuring robust security measures for one-to-one interactions between IoT devices and transaction nodes, and safeguarding the integrity of data exchanges within the network.

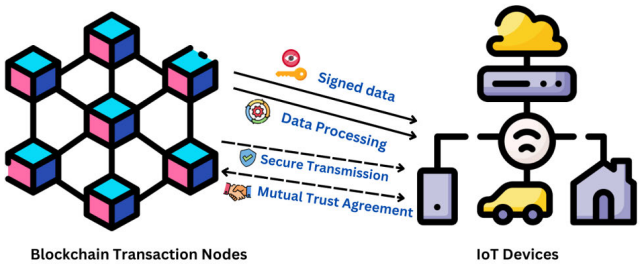

FIGURE 8. Secure data communication of IoT devices.

Furthermore, it is recommended to conduct device processing for the secure storage of personal signing keys. The amalgamation of blockchain technology today is an inclusive solution to unlimited security challenges, making it essential and inseparable in combining IoT and cloud computing systems [10]. The basic principles of blockchain play a fundamental role in solving problems, including decentralization, cryptographic security, and immutability. First, the primary role of decentralization is to eliminate centralized control, as well as reduce exposure to a single point of failure, which is a concern in the cloud environment [11]. The decentralized structure stores data in more than one place, helping to reduce the risk of data breaches and unauthorized access, which are often common concerns in traditional centralized cloud systems. Moreover, blockchain technology uses encryption algorithms and ensures data are transferred and stored securely and are not subject to tampering. In the encryption process, data are encrypted, time-stamped, and then added to a series of blocks, which creates an immutable record and, as a result, ensures data integrity and authenticity.

In addition, the methods used in blockchain help ensure consensus among network participants, facilitating the process of trust and verifying data accuracy without relying on central structures. Consensus mechanisms enhance security in data exchange between cloud computing devices and the IoT. In addition, smart contracts in blockchain technology automatically implement terms and conditions in advance, aiding in building safe and transparent transactions between devices without a third party or intermediaries. Smart contracts provide specific protocols for various procedures by regulating access, use, and implementation methods, enhancing security, and reducing the possibility of human errors or malicious activities. Blockchain technology works to add another layer of security and trust to cloud computing systems and the IoT through the transparent manner in which blockchain technology works, which enables the possibility of tracking data and their source to verify the legitimacy and history of the information [11]. Therefore, using the features provided by blockchain technology aids in building a strong, secure, and tamper-proof foundation that reduces the complex security concerns resulting from the integration of the IoT and cloud computing. Through these features, it is possible to create a secure and reliable framework for processing, transferring, and storing data within integrated systems.

Blockchain technology can enhance the security of integrating IoT devices with cloud services through two separate features: The transaction, is carried out by the participant,

and the Block is the dataset responsible for recording all data and details of the transaction. In addition, two blockchain technologies (public and private) are responsible for the control process within the IoT devices. Public blockchain technology means that permissions related to writing and reading are available to everyone, just like the cryptocurrency Bitcoin.

Private blockchain technology means user details are unavailable and can only be seen by trusted participants, thus helping to enhance security. Meanwhile, to improve security further, the technology relies on verifying each new participant before adding it to the blockchain by applying a set of rules. Several transactions are then collected to be added to a new block and then sent to all nodes within the network so each block contains a unique digital fingerprint [36].

The benefits of leveraging blockchain are as follows [36]:

- Blockchain technology is one of the first technologies to achieve security and transparency for IoT devices.
- This technology achieves transparency by giving each node a private copy of the blockchain and thus the data remains unchanged due to the existence of all transaction records.
- Data are encrypted in block records using a private key that is not publicly auditable, thus enhancing security.
- This technology provides the advantage of decentralization, meaning transactions and blocks are not stored within a device but are distributed among nodes across the blockchain network.
- This technology provides the advantage of impartiality by relying on specific rules before approving transactions.

Interactions between devices in the IoT present security problems; therefore, it is difficult to build trust through exchanging data between multiple IoT devices. In addition, the IoT depends on Wireless Sensor Network (WSN) technologies, exposing it to many security threats DDoS, and privacy breaches. Blockchain technology helps enhance trust and solve security issues by tracking all IoT devices and then enabling transaction processing and eliminating all points of failure. Blockchain technology relies on implementing cryptographic algorithms, such as hashing, to achieve security. In addition, this technology relies on consensus mechanisms to cultivate trust.

The technology is based on the decentralization feature, which helps reduce failures through interconnected nodes, thus eliminating data processing risks. The technology also relies on the cryptographic hashing feature to achieve data integrity, as each block has a unique hash for the previous block, thus maintaining the sequence of blocks without interruption. Finally, this technology relies on consensus mechanisms for PoW and PoS, thus ensuring the state of the ledger is correct [68]. This is because decentralized blockchain technology relies on immutable ledgers that work to enhance and ensure data integrity by creating historical data records, which protect them from manipulation or change.

1) MAINTAINING THE INTEGRITY OF IOT DATA THROUGH BLOCKCHAIN TECHNOLOGY

- **How blockchain maintains the integrity and privacy of data generated by IoT devices when transmitted to and stored in cloud environments:**
  Blockchain technology uses encryption algorithms that maintain the privacy and integrity of data once they enter distributed blocks, preventing modification. The distributed blocks are linked sequentially to each other, and therefore, any change to the details of one block requires changes to all blocks, complicating the process and proving that blockchain technology is resistant to tampering. Blockchain technology works to provide copies of each node within the network, and this helps the network to confront attacks protecting data privacy.
- **Using encryption technology and smart contracts to guarantee secure data processing and access control:**
  Smart contracts aim to implement and create contracts independently to automate agreements and write them in code. This helps in conducting all procedures automatically when conditions are met, thus controlling access to data. Furthermore, to secure the data, encryption techniques are used by giving each participant two public and private encryption keys. A public key is used to identify the participant and the private key before providing access to the data. Moreover, encryption techniques help protect data from changes by verifying and recording transactions using such mechanisms as PoW.

2) ENHANCING CLOUD SECURITY USING BLOCKCHAIN

- **How integrating blockchain technology with cloud services can bolster security measures, particularly in securing data storage, access management, and authentication protocols:**
  Blockchain technology helps create a secure cloud environment, by relying on attribute-based encryption to control access to data. Decentralized ledger technology is also necessary to maintain data security, which involves creating keys, defining access policies, and activating authentication protocols to determine identity. Specific users are allowed to access the data based on smart contract technology that ensures a reliable connection with the user who has the right to access the data [69].
- **The potential of decentralized identity management systems and permissioned blockchains for cloud security:** Decentralized identity management systems help provide security for the cloud by relying on distributed ledger technology. Self-Sovereign Identity (SSI) is one decentralized identity management system that helps users control their identities and thus prevent counterfeiting, as well as confirm identities in performing secure transactions. In these systems, permissioned blockchains are crucial using nodes to achieve global consensus and thus the ability to manage user credentials to maintain privacy in the cloud [70].

3) SPECIFIC INDUSTRIES/APPLICATIONS IN WHICH BLOCKCHAIN HAS DEMONSTRATED SIGNIFICANT SECURITY IMPROVEMENTS

Blockchain has shown significant improvements in safety in the autonomous vehicle industry by preventing accidents and developing the ability to determine maneuvers between parties to avoid accidents using smart contracts, as this technology has helped ensure the safety of all entities and prevent collisions on the road.

Blockchain technology has also been successfully implemented in the swarm robotics industry, as the features of this technology have helped ensure secure control between devices, in addition to security and scalability standards. Further, the technology necessitates the use of the Proof-of-Authority algorithm, which helps reduce resources, make correct decisions, and smooth communication between secret parties without any collisions [71].

Smart cities are also created based on the IoT, where smart contracts within blockchain technology are used to implement various operations with high efficiency and accuracy (parking control, waste management, energy, etc.). Here, conditions stored in smart contracts are followed to execute transactions and negotiate between devices to achieve the energy-trading scenario [72].

Further, a smart parking system has been implemented based on integrating IoT and blockchain technologies to activate an automated payment service based on the tokenization of IoT interactions. This technology can simplify the payment process easily by providing parking and requesting it in real-time, thus reducing transaction costs [72].

4) CHALLENGES AND CONSIDERATIONS

The following are some challenges or limitations associated with adopting blockchain to secure IoT and cloud integration.

- **Scalability**:
  Scalability becomes challenging because blockchain produces a large number of transactions, and to process them, blockchain scalability is necessary. Simultaneously, blockchains such as Bitcoin are unable to handle the large number of transactions generated by IoT devices. As a result, the blockchain must provide solutions that meet the requirements of IoT devices in terms of producing a huge number of transactions while processing them in a short time.
- **Interoperability**:
  Challenges facing interoperability arise because of contrasts between standards and protocols adopted in blockchain and IoT device production due to differences between manufacturers. To meet the challenges of interoperability, it is thus necessary to rely on communication protocols and standardize data formats and interfaces.
- **Regulatory challenges**:
  Regulatory challenges are encountered when designing blockchain-based IoT systems related to intellectual property rights and data privacy. Different laws and regulations between blockchain technology and the IoT must be followed when designing legal and regulatory frameworks that adhere to and can work securely [72].
- **Assumptions for successful implementation**:
  For the implementation of blockchain protocols and interfaces, as well as IoT device systems, compatibility must exist between them so they can achieve proper interaction and integration. In addition, successful decentralized networks can be built by addressing all costly problems and making improvements at a low cost, thus maintaining quality, safety, and scalability. In the end, ease of use is one of the standards for successful implementation, achieved through implementing several tests and assessing the user experience [73].

5) FUTURE EXPECTATIONS AND EMERGING DIRECTIONS

Future trends related to scalability solutions include the development of a methodology that helps blockchain technology track IoT sensors and then monitor all the information these devices collect. Thereafter, the mission of blockchain technology is to avoid duplicating any incorrect data and thus ensure scalability. In addition, this technology can achieve scalability by eliminating the need for a trusted third party, and the sensors then rely on this technology to transmit data.

V. RELATED STUDY

The forthcoming section aims to explore and analyze recent studies and developments pertaining to the integration of IoT and cloud computing, with a specific focus on the role of blockchain technology within this amalgamation. This segment dives into insightful works, investigative papers, and observational pieces to uncover the complexities and progressions in consolidating IoT and cloud computing standards. It scrutinizes the advancing environment of this integration, highlighting challenges, opportunities, and suggestions for various businesses and spaces. In addition, it covers the progressive utilization of blockchain, as a significant enabler of advancing the security, versatility, and decentralization components of IoT and cloud integration. By synthesizing findings from recent studies, this section endeavors to offer a comprehensive understanding of the synergies among IoT, cloud computing, and blockchain, shedding light on their collaborative potential to revolutionize diverse sectors and pave the way for more secure and efficient interconnected ecosystems.

This section thoroughly examines various important aspects related to the integration of IoT and cloud computing, particularly focusing on security issues. It covers such topics as technology, deployment, service, and sector/application, as well as the problems that have been discussed in this field. It also considers future opportunities and any limitations we might encounter. Moreover, the section explores how mobility plays a role within this context, the goal of which is to provide a clear understanding of the challenges and complexities involved in merging IoT and cloud computing while maintaining security, as shown in Table 7.

In [74] the authors concentrated on the integration of cloud computing and IoT, terming it as CLOUDIoT. They also mentioned a detailed analysis of the CLODIoT model and analyzed the specific difficulties of its applications. The applications that were considered in this paper: are healthcare, smart cities, smart homes, video surveillance, automotive and smart mobility, smart energy and smart grid, smart logistics, and environmental monitoring.

The authors also outline current research directions and analyze combination challenges. Despite a comprehensive analysis, open issues remain unresolved. The challenges within CloudIoT revolve around standardization and power efficiency, and currently, most connections to the cloud using web-based interfaces, causing complexities in machine–machine communication due to an increased network load, delays, and data processing. This lack of standardized interfaces hampers interoperability between the cloud and devices, requiring standardized protocols, architectures, and APIs to link diverse smart objects for enhanced services. In addition, power efficiency remains a critical concern, with frequent data transmission draining devices and gateway batteries within 24 hours. Energy efficiency in data processing and transmission in cloud technology and the IoT thus remains an unsolved problem.

significant data management is considered a sensitive topic in CLOUDIoT, as it requires managing and dealing with huge amounts of records from many different sources, necessitating complex processes to be activated in real-time. Synchronization is thus essential to manage interactive media records in real-time to provide offers and customer assistance. Another critical issue in the cloud and the IoT is security and privacy, one example of which is the Endeavors company, which works to manage privacy and security issues. Consideration in developing robust authorization elements is essential to ensure data governance and mitigate all risks, including altered sensor data, weak doors, vulnerabilities in communication channels, and burglary logs. Insights can be chosen through CLOUDIoT, allowing improved decision-making by way of centralizing real-time facts from one-of-a-kind assets. This centralized method enables superior actualities to be chosen and aggregate additives to be connected.

Estimating and charging complexities continue within CLOUDIoT due to different substances taking care of client connections, offerings, installments, and the increasing cost of maintaining associations among contraptions and the Cloud. Deciding coordinates benefit costs, distributing costs among partners, and managing charge strategies are uncertain issues in this situation.

Network communications present challenges to CLOUDIoT due to diverse technologies and the need for continuous data transmission, leading to exponential bandwidth. consumption. In effect, efficient access management and bandwidth optimization are open issues, especially at large scales. Fault-tolerant data transfer is thus crucial, especially in scenarios prone to connection failures, including healthcare applications where continuous and reliable data transmission is vital for patient monitoring.

The mechanisms by which papers are determined are also unclear. In addition, a large-scale implementation of multi-networking was not carried out.

In [21], the authors discuss each layer and the four categories of cloud services. The authors aim to consider the needs of the user and to be able to supply them with useful services and the effective use of resources. While there is not enough research on such important aspects as the type of IoT they are discussing and the services involved, they do not explain how they researched or collected the papers they used.

Amairah et al. [75] explain cloud computing and IoT in general and analyze the reference architecture. Also, as a result of reviewing some of the most common research, they offer specific directions for future studies, according to which there remains much work to be done to close security gaps, as well as on research directions concerning the integration of security systems. Further research is strongly recommended to explore and rectify the security vulnerabilities present within the integration system, a task that encompasses new avenues of investigation within this domain to address and bridge existing security gaps effectively.

In [20], the authors provide an overview of the integration of IoT and the cloud, as well as present a platform for IoT implementation with the cloud. Moreover, they conducted a comparison between IoT and cloud computing, highlighting numerous advantages of integrating IoT with the cloud. As well, they showcased various applications that have been enhanced by the cloud-based IoT paradigm. However, one of the shortcomings in this paper is that the authors attempt to compare cloud-based IoT with some new technologies, introducing gaps in this paradigm.

Díaz et al. [24] research the integration of cloud computing components and IoT-based cloud platforms, focusing on cloud infrastructure and IoT middleware, terming it ‘‘cloud of things’’ due to the merging of cloud computing and IoT capabilities. This paradigm resolved certain IoT issues, such as data accessibility and computing. In addition, they introduce new opportunities, such as ‘‘thing as a service’’ and smart things, but the paper lacks a detailed discussion of the methodology used for paper selection.

Cavalcante et al. [76] provides an overview of the progress and exploration of combining the cloud and IoT, identifying key research problems and paving the way for future studies in this area. Challenges highlighted by the authors include: 1) establishing standards and creating a framework for cloud-based IoT services and solutions; 2) analyzing ways to adapt IoT devices for better integration with cloud-based applications; 3) inadequate security assurance measures; and 4) managing huge volumes of real-time information successfully.

In [77], the authors addressed integration challenges in Intelligent Transportation Systems (ITS) to tackle transportation-related issues like traffic congestion, rising

fuel costs, and the necessity to enhance road safety. They showcased how cloud computing can improve the creation of mechanisms focused on traffic management and road safety by offering information to drivers. Moreover, they expressed the belief that combining cloud computing, IoT, and ITS could pave the way for developing more sustainable transportation solutions in the future.

Bae et al. [77] centered on the automated deployment and continuous integration of IoT-cloud services using docker containers. This process involves conducting a static check of the source code, building docker images, and deploying the output to a test environment for evaluation. They also provided a flowchart and developed a Python script for creating and running service containers without interrupting the service. Furthermore, they introduced application performance monitoring as an approach to evaluate the service's performance levels consistently.

Plathong and Surakratanasakul [39] introduced a real-time health tracking system by proposing a framework that merges the Health Level 7 protocol with IoT through cloud computing. This framework aims to enable the elderly and individuals to monitor their health remotely using IoT devices at any time and place. They suggested that this framework could potentially decrease mortality rates by averting misdiagnosis and incorrect treatments. However, the paper did not account for tracking other diseases like diabetes, heart conditions, or high blood pressure.

Karnouskos et al. [78] the study showcased the effectiveness of employing Open-Source Software (OSS) alongside various IoT devices as an educational tool for training developers and enhancing their IoT skills. They conducted a thorough analysis of technologies and concepts, resulting in a rapid development process. In addition, they provided training for developers to utilize the new technology and offered a variety of Open Source Software options and development approaches from which to choose.

Ahmed et al. [79] explained IoT devices in the healthcare sector and how it is possible to use these devices as a web service for future technologies. As witnessed during the COVID-19 pandemic, there was a significant surge in the number of patients requiring hospitalization. As such, to solve this problem, they combined several technologies including cloud computing, IoT, and Wireless Body Area Network (WBAN) to deal with this type of issue. They introduced an efficient workflow aimed at minimizing high energy consumption, high bandwidth usage, and extensive storage requirements, and they showed how the cloud provides an early diagnosis by analyzing patient health data.

Gooch and Chandrasekar [80] explains how CHORDS portals can be used to combine ground sensors and real-time weather radar data. With this system, weather radar data can be considered easily, quickly, and automatically by considering other sensors. However, the research does not investigate more about sensing networks.

Stradolini et al. [81] performed online anesthesia monitoring, an application that enables anesthesiologists to communicate concurrently with all sedated patients using Android apps. It connects via Wi-Fi to transmit data from the therapeutic drug monitoring platform, which continuously sends the measured data to the Android applications.

Alhussein et al. [82] introduce a framework that utilizes smart EEG sensors to record and transmit EEG signals from epileptic patients. This setup allows the framework to make real-time decisions regarding subsequent activities, and to determine whether to forward the data to the deep learning module. Moreover, various health sensors are employed in the proposed A structure to record, including psychological signals, gestures, and movement, and then transfer them to the cloud. The best options for developers in terms of communication protocols are thus MQTT and RESTful HTTP, according to [83]. It has been proven that the MQTT protocol is an excellent solution for the IoT layer due to its ability to handle limited objects and its ease of configuration. The paper should explore the issues in their field. IoT systems involve multiple disciplines, such as hardware, software, networking, and user experience. Focusing only on communication protocols might neglect other critical interdisciplinary factors affecting IoT integration.

Stergiou et al. [22] investigated IoT and cloud integration to discover their benefits, and their results show that the IoT performance is enhanced by cloud computing. As these technologies develop rapidly, security issues must be solved and open issues managed.

The three-level safety approach proposed in [84] elucidates a safety-based approach at three levels. To recognize different actions and cyberattacks, they determined that the random forest classification algorithm detects 93.9% of attacks in these complex environments.

Sie et al. [85] implemented a platform named Long-term care-based Smart Home Platform (LAESO), comprising a blend of sensor networks designed to log and monitor the activities of the elderly to handle emergency situations effectively. LAESO incorporates location-based video monitoring services and emergency notification systems by combining GPS positioning with crowd-sensing technology.

El-Sayed et al. [86] validated the effectiveness of edge computing by analyzing various network characteristics. They also present an evaluation of cloud computing systems and highlight a clear distinction in performance between edge computing and cloud computing systems.

Fog computing, a relatively recent discovery, serves as a decentralized processing technology that forms an alternative and supplement to cloud computing. Its primary advantages include low latency and rapid response rates, achieved by relying on nearby physical nodes for data processing and storage, consequently resulting in heightened security levels. In [87], the authors detailed the fog architecture, its defining characteristics, and its necessity across various sectors. They also outline various challenges and prospects

for fog computing. However, certain security concerns were not addressed comprehensively, such as interaction security, data transmission security, IDS, and task scheduling security.

Ali et al. [88] proposed a secure method for maintaining data authenticity in a cloud-based IoT network by merging blockchain's unchangeable smart contracts with conventional cloud infrastructure. In this system, cryptographic hashes of device metadata are stored on the blockchain, while the actual data remains off-chain in the cloud, ensuring scalability for extensive IoT device deployments. Multiple smart contracts on the blockchain authenticate and secure the cloud-stored data. Initial assessments demonstrate the framework's effectiveness in guaranteeing data authenticity within large-scale cloud-based IoT networks. By utilizing smart contracts and blockchain capabilities to store device metadata on the blockchain and actual data in the cloud, the framework ensures scalability and offers reliable evidence of data origin and integrity. The preliminary experimental findings affirm the framework's scalability in preserving data authenticity within cloud-centric IoT networks.

Zhang et al. [89] proposed architecture introduces a user-controlled data-sharing system with privacy preservation and granular access control. Named the Blockchain-based Architecture for Data Sharing (BaDS), this novel system employs a blockchain model and attribute-based cryptosystem, utilizing a Byzantine fault tolerance mechanism as the consensus algorithm instead of Proof of Work. BaDS primarily emphasizes achieving privacy, user autonomy in data sharing, and decentralization. By utilizing blockchain and attribute-based cryptosystems like Attribute-Based Signature (ABS) and Ciphertext-Policy Attribute-Based Encryption (CP-ABE), it enables detailed access control. The paper delineates BaDS's security requirements and illustrates how these criteria are fulfilled within the architecture. Furthermore, the authors implement and analyze the computational the cost associated with the BaDS architecture.

Ma et al. [90] introduced a new Blockchain-based Distributed Key Management Architecture (BDKMA) intended to fulfill the requirements of decentralization, detailed auditability, scalability, and privacy in hierarchical access control for IoT. By integrating blockchain with cloud and fog computing, this architecture introduces a unique approach to address these requirements. It divides the network into separate side blockchains based on deployment domains to expedite verification and conserve storage space for IoT devices. Each domain's Security Access Modules (SAMs) maintain the side blockchains, while a collection of multi-blockchains is stored in the cloud to facilitate interactions across domains. The simulation findings suggest that the multi-blockchain structure notably improves system performance and scalability as the network grows. Moreover, dynamically adjusting transaction collection time enhances performance and system capacity, catering to various environments more optimally.

Hossain et al. [91] introduced FIF-IoT, a forensic investigation framework specifically designed for IoT-based systems using a public digital ledger. FIF-IoT records various interactions within IoT systems, such as device-to-device, device-to-user, and device-to-cloud, storing this information as evidence in a public digital ledger similar to Bitcoin's. This framework guarantees confidentiality, anonymity, and non-repudiation of the evidence available publicly. FIF-IoT includes interfaces for evidence acquisition and a method to verify evidence integrity during criminal investigations. The authors demonstrated FIFIoT's resilience in an adversarial scenario, displaying its ability to resist tampering, even in collusion scenarios. Additionally, they developed a prototype of FIF-IoT and evaluated its performance.

Ahmad et al. [92] The proposal defined in this study aims to improve decentralized Identity Management (IDM) within IoT-cloud applications by integrating face recognition data into a blockchain-based transaction ledger. This concept of blockchain IDM is showcased through a campus-wide printing service as a practical illustration. The decentralized IDM is intended for implementation utilizing Cloudlet, which provides effective connectivity for IoT devices on a large scale with low latency and high bandwidth. Face identity data obtained through facial recognition is verified using an immutable blockchain mechanism. This verification process grants access to printing services based on user identity validation. The blockchain also facilitates a smart contract that tracks the user's printing transactions. Through blockchain integration, the IDM system is decentralized, service processes are automated, and the overall service remains cost-effective and transparent.

Zhao et al. [93] demonstrated the particular necessities for securely storing Virtual Machine (VM) measurements within IaaS cloud environments. While recognizing blockchain technology as a promising solution for these requirements, it acknowledges challenges in controllability and performance. To address these concerns, the paper introduces the Mchain approach, aiming to balance integrity and controllability while optimizing performance. This approach involves a two-layer blockchain-based network. The first layer verifies data packages against specific correspondences and utilizes a consensus achievement algorithm to construct semi-finished blocks, ensuring integrity across all nodes. The second layer generates tamper-resistant metadata through PoW tasks, enhancing robust integrity. For controllability, the approach proposes a user-defined policy using Key Policy Attribute-Based Encryption (KP-ABE) encryption, allowing flexible limitation of verifiers' scope. The authors conducted experiments across six scenarios with simulated datasets to evaluate the approach, demonstrating its effectiveness in integrity, controllability, and the time overhead of data storage.

Qiu et al. [94] investigated blockchain-integrated IoT systems and introduced solutions for deploying blockchain in IoT by highlighting agent mining and cloud mining

approaches. They assessed the system's performance by considering users' service demands, computing capabilities, and networking capabilities. They formulated access selection for users, computing resource allocation, and networking resource allocation as a joint optimization problem. To address this challenge, the authors utilized a dueling deep reinforcement learning approach, demonstrating the effectiveness of their proposed scheme through simulation results. They emphasize the crucial influence of cloud server reliability on system performance. If these servers are untrustworthy, they suggest either not using them or limiting their usage. Additionally, they underscore the significance of robustness in learning outcomes, suggesting that increasing training samples and expanding the state space can mitigate this issue.

Yang et al. [95] presented a blockchain-based method that empowers data owners to oversee the anonymization process and boosts service security. This approach utilizes blockchain to validate the use of privacy budgets and dynamically adjust their allocation via smart contracts, aligning with the data owners' privacy needs. They substantiated their proposal through a prototype implementation using the Hyperledger permissioned blockchain, confirming its efficacy in ensuring privacy and practical application.

Liang et al. [96] introduced ProvChain, a blockchain-based system for data provenance designed specifically for cloud auditing. Its main focus is on preserving user privacy and ensuring enhanced availability. Using blockchain technology, ProvChain records data with unchangeable timestamps and generates blockchain receipts for each data entry, ensuring its validation. The system is adaptable to various use cases requiring globally verified proof, allowing for different data granularities, such as segments of data within cloud storage rather than entire files. Their evaluation demonstrates that enabling provenance in ownCloud results in minimal overhead. Regarding incentives for blockchain miners, users can pay a fee to cloud service providers for data provenance services. These fees can be used by the service provider to compensate the blockchain network, ensuring that miners are rewarded for ongoing block mining and validation. The fee structure can be tailored based on individual user data usage levels.

Wu et al. [97] provided a thorough survey of blockchain research, categorizing it into four layers: data, consensus, network, and application. The data layer covers foundational blockchain elements, such as cryptographic aspects, data structures, and mining processes. The network layer focuses on Peer-to-Peer (P2P) network concerns, scalability, transaction processes, and data privacy. While efforts have been made to enhance scalability, few solutions are both practical and secure for real-world deployment, and traditional P2P network vulnerabilities remain a concern for blockchain networks. In the consensus layer, classical consensus mechanisms like PoW, PoS, and Delegated Proof of Stake (DPoS) are discussed, highlighting their pros and cons, along with attacks and countermeasures against PoW. The application layer examines blockchain extensions (e.g., smart contracts, sidechains) and their general applications across various fields.

Ali et al. [98] presented an extensive survey of recent endeavors to advance blockchain technology, focusing particularly on efforts in creating blockchain-based platforms, applications, and services tailored for the evolving landscape of the IoT. It outlines the fundamental attributes of blockchain, emphasizing its distributed ledger functionality, immutability, and verifiable transaction records through distributed consensus algorithms. The paper underscores that blockchains create a trustless environment, reducing reliance on centralized entities. With the decentralized nature of blockchain technology demonstrated in cryptocurrency networks, it is seen as a potential solution for decentralizing the IoT. Currently, the IoT heavily depends on centralized entities for authentication, authorization, and data management. Blockchain is envisioned as a means to create a decentralized framework for the IoT, eliminating the need for centralized intermediaries. The survey emphasizes several areas within the IoT landscape where blockchain-based decentralization shows potential benefits. These include enhancing privacy, securing communications, managing identities and data, and exploring opportunities for monetizing IoT data and resources.

Fernández-Caramés and Fraga-Lamas [99] evaluated the current status of blockchain technologies and explored potential applications in the Blockchain-based IoT (BIoT) across sectors, such as healthcare, logistics, smart cities, and energy management. These BIoT applications come with distinct technical requirements, differing from cryptocurrency-focused implementations. These entail concerns such as energy efficiency in devices with limited resources and the need for specialized architectures. The primary aim of this review was to assess practical limitations and identify areas for future research in BIoT. It provided a comprehensive examination of essential aspects in designing an optimized BIoT, covering architecture, necessary cryptographic algorithms, and consensus mechanisms. Additionally, the review offered recommendations to guide future BIoT researchers and developers in addressing critical challenges before deploying the next generation of BIoT applications.

Makhdoom et al. [100] outlined the threat landscape in the realm of IoT, highlighting the resultant security needs and performance requirements for IoT systems. It introduces fundamental blockchain concepts and explores the impact of blockchain technology on IoT, identifying obstacles that hinder its integration into IoT environments. Subsequently, it reviews various blockchain-based IoT applications, illustrating trends in IoT applications and demonstrating how these applications tackle issues related to blockchain. Finally, it conducts a gap analysis, highlighting major challenges that obstruct the adoption of blockchain in the IoT environment. The conclusion proposes a pathway to address and overcome

some of these challenges, aiming to facilitate the integration of blockchain technology into IoT systems.

Medhane et al. [101] introduced a distributed security framework that combines blockchain, edge-cloud, and Software-Defined Networking (SDN) technologies, proposed for implementation in the upcoming generation of the IoT ecosystem. This framework is highlighted as a substantial contribution aimed at securing future IoT systems. It employs blockchain technology and leverages edge-cloud mechanisms for rapid attack detection at the SDN edge, ensuring swift responses to security threats. The study demonstrates the framework's effectiveness in achieving data confidentiality and early attack detection, resulting in reduced storage, latency, and resource consumption in IoT networks. By utilizing blockchain, all devices within the IoT network share data, enhancing overall security. The authors suggest that this security framework can effectively preserve data confidentiality, detecting and mitigating potential security threats by real-time monitoring of IoT traffic. They proposed future enhancements concentrate on several aspects, including virtualization, the preservation of security attributes like confidentiality and integrity, and the facilitation of IoT service and application migration. These enhancements aim to further enhance the quality of service in the next generation of IoT systems.

Gai et al. [102] aim of their work was to establish a privacy-preserving method for deploying edge computing in IoT. Their proposed approach, known as the Blockchain-based Internet-of-Edge (BIoE) model, utilized blockchain techniques in task allocations. This model successfully achieved three main objectives: enabling functional task allocation in an edge-based IoT system, maintaining privacy, and resisting tampering. Through their evaluation, the authors demonstrated that their model effectively met the intended design goals. The authors of the paper introduced a novel integration called the BIoE model, encompassing IoT, edge computing, and blockchain. This model is designed to develop a scalable and manageable IoT system by capitalizing on the advantages of edge computing and blockchain. It aims to establish a privacy-preserving mechanism while considering energy cost constraints. They conduct experimental evaluations using Ethereum and observe that their model enhances privacy protection without compromising performance, all in an energy-efficient manner.

Yu et al. [103] introduced LayerChain, a hierarchical edge cloud blockchain system designed specifically for secure, large-scale, and low-delay applications in the Industrial Internet of Things (IIoT). This system manages long-term blockchain transaction data from IIoT devices using a three-layer hierarchical structure involving light and full-edge nodes, as well as multiple distributed clouds. To handle varying computing power and storage space across different edge nodes, they propose an edge node classification method. Additionally, they present a tree-based clustering algorithm to decrease blockchain block propagation time by organizing block propagation into multiple propagation trees, thus preventing redundant block propagation. Extensive experiments conducted demonstrate that LayerChain efficiently utilizes storage and computational resources while significantly reducing block propagation time, showcasing its suitability for large-scale low-delay IIoT applications.

Memon et al. [104] provided an assessment of the current state of Cloud-Based IoT (CB-IoT) and predicted a taxonomy of future challenges that could exacerbate current issues, potentially resulting in increased vulnerabilities to cyber threats and subsequent financial and data losses. In response to these challenges, the article explores the potential of Blockchain-Based IoT (BB-IoT) and anticipates emerging challenges in this domain. Instead of advocating for a complete migration, the article proposes a hybrid IoT approach aiming to capitalize on the strengths of both CB-IoT and BB-IoT while addressing their respective weaknesses. This proposed hybrid-IoT model operates through three distinct communication configurations tailored for various applications: a local area network with edge nodes, a metropolitan area network with fog nodes, and a multi-layered ecosystem suitable for industrial and business applications. The article highlights the importance of establishing new policies and standards to ensure a secure and distributed IoT system, enabling the effective implementation of this hybrid approach.

Habib et al. [57] provided insights into the potential collaboration between blockchain technology and cloud computing, to improve security and reliability within the cloud computing paradigm. It highlights the robust computational capabilities and extensive storage capacity of cloud platforms, aligning with the demands of blockchain technology. The review provides an in-depth exploration of recent studies and current literature, analyzing the advantages and challenges associated with integrating blockchain within cloud computing. The article categorized and explored various security services that blockchain can provide within a cloud environment. It primarily focuses on discussing how cloud computing can enhance and support blockchain operations. Furthermore, the article presents the current stances of major cloud service providers in adopting and merging blockchain within their systems. The collaborative potential of blockchain and cloud computing is emphasized as a solution to common obstacles, suggesting potential integration strategies for future study and development.

Tapas et al. [105] introduced an enhancement to the current IoT-cloud framework by suggesting a decentralized design aimed at managing resource access authorization and delegating responsibilities. This enhancement incorporates blockchain as a foundational element and utilizes smart contracts as a principal mechanism for decentralized, trustless operations and independent audit capabilities. The paper outlines the design and implementation specifics of these contracts and includes preliminary results obtained from this proposed setup.

Singh et al. [106] presented an innovative smart home architecture merging cloud computing and blockchain technology to establish a secure and efficient system. Cloud computing extends smart home capabilities by leveraging cloud services, managed by a broker selecting energy-efficient service providers for users. Blockchain facilitates a peer-to-peer network, enabling communication between untrusted nodes efficiently. Encryption and hashing in blockchain ensure data confidentiality and integrity in both local and overlay networks. Authorization is managed through policy headers and shared keys between devices and miners, ensuring availability via accepted transactions. Moreover, the article introduces a Multivariate Correlation Analysis (MCA) algorithm for traffic feature correlation detection in smart home networks, providing a network attack detection and response system. Evaluation results, including Receiver Operating Characteristic (ROC) curves, CPU utilization, throughput time overhead, and network overhead, indicate significant enhancements in smart home security and efficiency due to the proposed architecture.

VI. OPEN CHALLENGES AND LIMITATIONS

While the integration of IoT, cloud computing, and blockchain technology presents a promising approach to bolstering security, several limitations persist. One primary concern involves the computational overhead and energy consumption associated with blockchain implementation in large-scale IoT networks. The consensus mechanisms within blockchain systems often demand extensive computational power, potentially hindering the scalability and performance of IoT devices with limited resources. Moreover, the integration of these technologies introduces complexity, leading to interoperability challenges and potential vulnerabilities stemming from the complex interactions between diverse systems. Additionally, the regulatory landscape and compliance standards are evolving, raising uncertainties around legal and regulatory frameworks governing the use of blockchain in different sectors. Security concerns such as potential privacy breaches, data management, and identity verification in a decentralized environment remain open challenges that require extensive research and robust solutions. Furthermore, while blockchain offers immutable and transparent ledgers, it is not immune to all security threats, such as 51 percent attacks and novel cryptographic vulnerabilities, necessitating continuous evolution and adaptation of security measures in this integration. Addressing these limitations will be crucial in realizing the full potential of integrating IoT, cloud computing, and blockchain while ensuring robust security.

A. SCALABILITY AND PERFORMANCE LIMITATIONS

Scalability is a significant problem when connecting IoT devices with cloud computing and blockchain technologies. IoT devices generate much data, which must be processed quickly. However, blockchain struggles with handling large amounts of transactions quickly, which can cause delays. As the blockchain becomes larger, it requires more resources, including storage and power, which can render cloud computing less efficient.

B. INTEROPERABILITY AND STANDARDIZATION ISSUES

Interoperability is another significant challenge, as IoT devices, cloud services, and blockchain technology often work poorly together because they come from different manufacturers or use different platforms. There is also a lack of common standards to help these technologies communicate smoothly, which can prevent IoT systems from reaching their full potential.

C. PRIVACY CONCERNS

Despite blockchain's security features, privacy is a concern. Blockchain's transparency means that once data are on the blockchain, they are visible to everyone and cannot be changed or removed. This could include personal data from IoT devices that should not be publicly accessible. Integrating with cloud computing also introduces risks related to controlling and storing personal data.

D. SECURITY RISKS

Even though blockchain enhances security, combining it with IoT and cloud computing introduces security risks. IoT devices often have poor security, making them easy targets for hackers. If breached, these devices could compromise the entire network, including cloud services and blockchain systems. In addition, the interaction between different technologies can create new vulnerabilities, risking data exposure and attacks.

VII. FUTURE DIRECTIONS

Following an extensive examination of security concerns and solutions, a crucial issue identified is the absence of predictive measures for security breaches. In future research, attention could be directed towards the following areas within cloud computing and IoT systems: addressing security challenges in existing cloud systems by offering diverse logical control methodologies to enhance cloud security; analyzing the latest models in cloud security and IoT, presenting comprehensive evaluations; reviewing the current integration of cloud computing and IoT to scrutinize security issues and challenges, including aspects such as authentication, encryption, multitenancy, virtual machine security, and exploring methods to mitigate these issues. Emphasizing the need to bridge the existing gap, researchers are encouraged to focus on filling this void to effectively mitigate security concerns within this domain. Looking ahead, the evolution of security measures in the integration of IoT, cloud computing, and blockchain technology demands a proactive approach to address emerging threats and vulnerabilities.

Future directions in this realm should encompass multifaceted strategies. Primarily, focusing on developing standardized security protocols and frameworks that can uniformly govern interconnected systems is imperative. This includes fostering enhanced encryption techniques, robust

TABLE 7. Related study.

Ref.	Year	Technology	Deployment	Sector/Application	Open Issues	Limitations	Mobility
[69]	2015	CloudIoT Paradigm	Public	Health care, Smart cities	Power and energy efficiency	M2M communication,Data processing	✓
[15]	2014	Cloud of things (CoT)	Hybrid	Health Care Smart cities	Smart gateways Scalability	lack of the scalability and performanceN/A	✓
[21]	2018	Cloud computing and IoT	N/A	Health care, Smart cities	N/A	Lack of future trends analysis	✗
[9]	2018	Cloud–based IoT	N/A	Health care, Smart cities	significant data, Fog Computing	Lack of reliable osmotic computing solutions	✗
[36]	2016	Cloud computing and IoT	N/A	Smart city, Smart Logistics	Security ,Fog computing	Storage,Network	✓
[71]	2016	IoT and cloud computing	N/A	Smart city, Health care	Standardizing cloud-based IoT	Data extraction, Data synthesis	✗
[72]	2015	Cloud computing and IoT	N/A	Transportation	Develop transportation solutions	High costs, Scalability	✓
[35]	2017	IoT by cloud computing	N/A	Public health	Medical devices IoT	Medical devices to track patient condition	✗
[37]	2017	IoT by cloud computing	Public	Robots (EV3, Braccio)	Autonomous machines	Reinforcement learning	✓
[75]	2017	IoT and cloud computing	Public, Private	Health care	Large volume of storage	Sensors with low energy and storage	✗
[76]	2017	IoT and cloud computing	Private	Geosciences	System to generate CHORDS portals	Radar data fusion	✓
[77]	2018	IoT and cloud computing	N/A	Medical Application	N/A	Cloud-based system for hospital	✓
[77]	2018	IoT and cloud computing	N/A	Health care	Cognitive framework to handle significant data	complexity of data and signals	✓
[78]	2019	IoT and cloud computing	N/A	Communication	Protocols in IoT-fog-cloud	The IoT to fog layer communication	✓
[34]	2018	IoT and cloud computing	Private, Public, Hybrid	Business functionality	Security challenges	Storage, communication capabilities	✓
[79]	2015	IoT and cloud computing	N/A	significant Data Analytics	Higher accuracy level	Complexity of significant Data	✓
[80]	2016	IoT and cloud computing	Private,Public	Platforms, applications	Resource allocation,Security	Lack of identification of the future work analysis	✓
[81]	2017	IoT and cloud computing	Hybrid	Computing Environment	Significant processing models	Storage capacity	✓
[82]	2018	IoT and cloud computing	Hybrid	Healthcare, transport	Scalability,Complexity	Computation, storage	✓
[83]	2018	IoT and Blockchain	Hybrid	Health care, GPS	Throughput, latency,scalability	Computational, storage	✓
[84]	2018	IoT and Blockchain	Public	Business activities	N/A	Computational and storage resources	✓
[85]	2019	IoT and Blockchain	N/A	Business activities	Facilitate blockchain-based IoT	HKAS in privacy-oriented	✓
[86]	2018	IoT and Blockchain	Public	Health care, Smart Home	N/A	Storage of IoT devices	✓
[87]	2018	IoT and Blockchain	Public	Business activities	N/A	Bandwidth and high-latency network	✓
[88]	2018	Cloud computing and Blockchain	Private	Business activities	Improving approach for more data types	Poor access control	✗
[89]	2018	Cloud and Blockchain and IoT	N/A	Business activities	Cloud mining approaches	Nodes in IoT are resource-limited	✓
[90]	2018	Cloud computing and Blockchain	private	Business activities	Practical deployment issues in a cloud	Integrity and accountability guarantee	✓
[91]	2017	Blockchain and cloud computing	Private	Financial sector	ProvChain for federated cloud provider	Lack of ProvChain for a federated cloud provider	✓
[92]	2019	Blockchain and IoT	Private, Public, Hybrid	Financial sector	Pseudonym for user anonymity	Storage issues	✓
[93]	2018	Blockchain and IoT	Private, Public	Financial sector	Development of blockchains	Consensus algorithm	✓
[94]	2018	Blockchain and IoT	Private, Public	Public sectors	Interoperability and standardization	Transaction capacity in Blockchain	✓
[95]	2019	Blockchain and IoT	Private, Public, Hybrid	Financial sector	Develop a blockchain-based secure IoT	Scalability, large storage	✓
[96]	2020	Blockchain and IoT	N/A	Health care, Smart grid	Research in edge-cloud	Improve quality of service	✓
[97]	2019	Blockchain and IoT	N/A	Financial sector	Task allocations	Energy-saving efficiency	✓
[98]	2020	Blockchain and IoT	N/A	Manufacturing,Healthcare	N/A	Several critical limitations	✓
[99]	2020	Cloud and Blockchain and IoT	Public, Private, Hybrid	Financial sector	Hybrid IoT	security Services,network architecture	✓
[100]	2022	Blockchain and cloud computing	Private, Public	Financial sector	Data storage at every node,Security	Transaction consumes	✓
[101]	2018	Blockchain and Cloud and IoT	Public	Smart City	Deploy smart contracts	Maintaining the public auditing system	✓
[102]	2019	Blockchain and Cloud and IoT	Private,Public	Smart home	Efficient security solution	Lack of identification of the future work analysis	✗

Ref: Reference, HKAS: Hierarchical Key Assignment Scheme, N/A: Not Applicable

authentication methodologies, and access control mechanisms that align with the dynamic nature of these integrated technologies. Moreover, exploring artificial intelligence and machine learning applications to detect anomalies, predict potential threats, and automate real-time responses could fortify security measures. Collaboration between industry stakeholders, policymakers, and security experts will be crucial to establishing regulatory frameworks that prioritize data privacy and security without stifling innovation.

As advancements continue, research efforts should concentrate on adaptive security solutions capable of dynamically responding to evolving threats. Additionally, educating end-users and stakeholders about the risks and best practices for secure integration will be pivotal. Embracing a proactive, collaborative, and adaptive approach will be key in shaping the future of security in the integration of IoT, cloud computing, and blockchain technology.

VIII. CONCLUSION

IoT and cloud technologies have experienced remarkable growth in recent times. Moving forward, IoT and cloud systems are expected to generate vast volumes of data that necessitate efficient collection and processing. Security stands out as one of the most significant challenges confronting the realms of cloud computing and IoT. This paper delves into investigating the amalgamation of IoT and cloud computing, addressing issues compatible with cloud systems and computing methodologies to facilitate the smooth transition of IoT applications to the cloud. Moreover, the focus is placed on cloud architectures, deployments,and the architecture of cloud IoT. This review paper highlights several critical security issues, including QoS, identity management, data security, supported protocols, resource allocation, scalability, energy consumption, and computational resources. In conclusion, the integration of IoT with cloud computing and the adoption of blockchain technology presents a promising avenue for revolutionizing modern technological landscapes. However, this fusion also brings forth a host of intricate security challenges. The vast interconnectivity and data exchange in IoT devices poses vulnerabilities in terms of privacy breaches, data integrity, and security threats. Cloud computing amplifies these concerns with the aggregation of data in centralized locations, becoming potential targets for cyberattacks. While blockchain technology offers decentralized and immutable data structures, its adoption presents its own set of security complexities. The complexity of this integration demands comprehensive solutions that address issues, such as secure data transmission, authentication, access control, and resilience against evolving cyber threats. Establishing robust security measures within this amalgamation is crucial for leveraging the full potential of IoT, cloud computing, and blockchain while ensuring the safety and integrity of the interconnected systems. Therefore, a comprehensive approach that looks at both the security of individual technologies and the complex relationships between them is essential to strengthen this combination against new security threats.

ACKNOWLEDGMENT

The authors extend their appreciation to the Deanship of Scientific Research, Vice Presidency for Graduate Studies and Scientific Research, King Faisal University, Saudi Arabia [GRANT No. KFU241426]. The authors would like to thank the anonymous reviewers for their insightful scholastic comments, directions, and suggestions, which improved the quality of the paper.

REFERENCES

[1] A. Mohiyuddin, A. R. Javed, C. Chakraborty, M. Rizwan, M. Shabbir, and J. Nebhen, "Secure cloud storage for medical IoT data using adaptive neuro-fuzzy inference system," *Int. J. Fuzzy Syst.*, vol. 24, no. 2, pp. 1203–1215, Mar. 2022.

[2] Y. Karam, T. Baker, and A. Taleb-Bendiab, "Security support for intention driven elastic cloud computing," in *Proc. 6th UKSim/AMSS Eur. Symp. Comput. Modeling Simulation*, Nov. 2012, pp. 67–73.

[3] L. Golightly, V. Chang, Q. A. Xu, X. Gao, and B. S. Liu, "Adoption of cloud computing as innovation in the organization," *Int. J. Eng. Bus. Manage.*, vol. 14, Jan. 2022, Art. no. 184797902210939.

[4] W. Ahmad, A. Rasool, A. R. Javed, T. Baker, and Z. Jalil, "Cyber security in IoT-based cloud computing: A comprehensive survey," *Electronics*, vol. 11, no. 1, p. 16, Dec. 2021.

[5] D. CeArley, B. Burke, S. Searle, and M. J. Walker. (Oct. 3, 2017). *Gartner's top 10 Strategic Technology Trends for 2017*. Accessed: Feb. 5, 2020. [Online]. Available: https://www. gartner.com/smarterwithgartner/gartner-top-10-strategic-technology-trends-for-2018

[6] M. T. Khorshed, A. B. M. S. Ali, and S. A. Wasimi, "A survey on gaps, threat remediation challenges and some thoughts for proactive attack detection in cloud computing," *Future Gener. Comput. Syst.*, vol. 28, no. 6, pp. 833–851, Jun. 2012.

[7] A. R. Javed, R. Abid, B. Aslam, H. A. Khalid, M. Z. Khan, O. H. Alhazmi, and M. Rizwan, "Green5G: Enhancing capacity and coverage in device-to-device communication," *Comput., Mater. Continua*, vol. 67, no. 2, pp. 1933–1950, 2021.

[8] M. Anuradha, T. Jayasankar, N. B. Prakash, M. Y. Sikkandar, G. R. Hemalakshmi, C. Bharatiraja, and A. S. F. Britto, "IoT enabled cancer prediction system to enhance the authentication and security using cloud computing," *Microprocessors Microsyst.*, vol. 80, Feb. 2021, Art. no. 103301.

[9] S. Rasool, A. Saleem, M. Iqbal, T. Dagiuklas, A. K. Bashir, S. Mumtaz, and S. A. Otaibi, "Blockchain-enabled reliable osmotic computing for cloud of things: Applications and challenges," *IEEE Internet Things Mag.*, vol. 3, no. 2, pp. 63–67, Jun. 2020.

[10] R. B. Uriarte and R. DeNicola, "Blockchain-based decentralized cloud/fog solutions: Challenges, opportunities, and standards," *IEEE Commun. Standards Mag.*, vol. 2, no. 3, pp. 22–28, Sep. 2018.

[11] D. C. Nguyen, P. N. Pathirana, M. Ding, and A. Seneviratne, "Integration of blockchain and cloud of things: Architecture, applications and challenges," *IEEE Commun. Surveys Tuts.*, vol. 22, no. 4, pp. 2521–2549, 4th Quart., 2020.

[12] H. I. Ahmed, A. A. Nasr, S. Abdel-Mageid, and H. K. Aslan, "A survey of IoT security threats and defenses," *Int. J. Adv. Comput. Res.*, vol. 9, no. 45, pp. 325–350, Oct. 2019.

[13] S. Balaji, K. Nathani, and R. Santhakumar, "IoT technology, applications and challenges: A contemporary survey," *Wireless Pers. Commun.*, vol. 108, no. 1, pp. 363–388, Sep. 2019.

[14] M. M. Sadeeq, N. M. Abdulkareem, S. R. M. Zeebaree, D. M. Ahmed, A. S. Sami, and R. R. Zebari, "IoT and cloud computing issues, challenges and opportunities: A review," *Qubahan Academic J.*, vol. 1, no. 2, pp. 1–7, Mar. 2021.

[15] M. Mansour, A. Gamal, A. I. Ahmed, L. A. Said, A. Elbaz, N. Herencsar, and A. Soltan, "Internet of Things: A comprehensive overview on protocols, architectures, technologies, simulation tools, and future directions," *Energies*, vol. 16, no. 8, p. 3465, Apr. 2023.

[16] J. Park and J. Park, "Blockchain security in cloud computing: Use cases, challenges, and solutions," *Symmetry*, vol. 9, no. 8, p. 164, Aug. 2017. [Online]. Available: https://www.mdpi.com/2073-8994/9/8/164

[17] E. Schiller, A. Aidoo, J. Fuhrer, J. Stahl, M. Ziörjen, and B. Stiller, "Landscape of IoT security," *Comput. Sci. Rev.*, vol. 44, May 2022, Art. no. 100467.

[18] B. B. Gupta and M. Quamara, "An overview of Internet of Things (IoT): Architectural aspects, challenges, and protocols," *Concurrency Comput., Pract. Exper.*, vol. 32, no. 21, Nov. 2020, Art. no. e4946.

[19] A. Gerodimos, L. Maglaras, M. A. Ferrag, N. Ayres, and I. Kantzavelou, "IoT: Communication protocols and security threats," *Internet Things Cyber-Phys. Syst.*, vol. 3, pp. 1–13, Jan. 2023.

[20] H. F. Atlam, A. Alenezi, A. Alharthi, R. J. Walters, and G. B. Wills, "Integration of cloud computing with Internet of Things: Challenges and open issues," in *Proc. IEEE Int. Conf. Internet Things (iThings) IEEE Green Comput. Commun. (GreenCom) IEEE Cyber, Phys. Social Comput. (CPSCom) IEEE Smart Data (SmartData)*, Jun. 2017, pp. 670–675.

[21] M. Aazam, I. Khan, A. A. Alsaffar, and E.-N. Huh, "Cloud of things: Integrating Internet of Things and cloud computing and the issues involved," in *Proc. 11th Int. Bhurban Conf. Appl. Sci. Technol. (IBCAST)* Islamabad, Pakistan, Jan. 2014, pp. 414–419.

[22] C. Stergiou, K. E. Psannis, B.-G. Kim, and B. Gupta, "Secure integration of IoT and cloud computing," *Future Gener. Comput. Syst.*, vol. 78, pp. 964–975, Jan. 2018.

[23] L. Kakkar, D. Gupta, S. Saxena, and S. Tanwar, "IoT architectures and its security: A review," in *Proc. 2nd Int. Conf. Inf. Manag. Mach. Intell. (ICIMMI)*. Cham, Switzerland: Springer, 2021, pp. 87–94.

[24] M. Díaz, C. Martín, and B. Rubio, "State-of-the-art, challenges, and open issues in the integration of Internet of Things and cloud computing," *J. Netw. Comput. Appl.*, vol. 67, pp. 99–117, May 2016.

[25] M. P. Nath, R. Sridharan, A. Bhargava, and T. Mohammed, "Cloud computing: An overview, benefits, issues & research challenges," *Int. J. Res. Sci. Innov.*, vol. 6, no. 2, pp. 1–11, Feb. 2019.

[26] I. Ahmed, "A brief review: Security issues in cloud computing and their solutions," *TELKOMNIKA (Telecommun. Comput. Electron. Control)*, vol. 17, no. 6, p. 2812, Dec. 2019.

[27] M. K. Sasubilli and V. R, "Cloud computing security challenges, threats and vulnerabilities," in *Proc. 6th Int. Conf. Inventive Comput. Technol. (ICICT)*, Jan. 2021, pp. 476–480.

[28] H. Tabrizchi and M. K. Rafsanjani, "A survey on security challenges in cloud computing: Issues, threats, and solutions," *J. Supercomput.*, vol. 76, no. 12, pp. 9493–9532, Dec. 2020.

[29] A. Darwish, A. E. Hassanien, M. Elhoseny, A. K. Sangaiah, and K. Muhammad, "The impact of the hybrid platform of Internet of Things and cloud computing on healthcare systems: Opportunities, challenges, and open problems," *J. Ambient Intell. Humanized Comput.*, vol. 10, no. 10, pp. 4151–4166, Oct. 2019.

[30] H. Shukur, S. Zeebaree, R. Zebari, D. Zeebaree, O. Ahmed, and A. Salih, "Cloud computing virtualization of resources allocation for distributed systems," *J. Appl. Sci. Technol. Trends*, vol. 1, no. 2, pp. 98–105, Jun. 2020.

[31] L. M. Haji, S. Zeebaree, O. M. Ahmed, A. B. Sallow, K. Jacksi, and R. R. Zeabri, "Dynamic resource allocation for distributed systems and cloud computing," *TEST Eng. Manage.*, vol. 83, pp. 22417–22426, May 2020.

[32] M. Ishaq, M. H. Afzal, S. Tahir, and K. Ullah, "A compact study of recent trends of challenges and opportunities in integrating Internet of Things (IoT) and cloud computing," in *Proc. Int. Conf. Comput., Electron. Electr. Eng. (ICE Cube)*, Oct. 2021, pp. 1–4.

[33] J. Ren, H. Guo, C. Xu, and Y. Zhang, "Serving at the edge: A scalable IoT architecture based on transparent computing," *IEEE Netw.*, vol. 31, no. 5, pp. 96–105, Aug. 2017.

[34] R. Gravina, P. Alinia, H. Ghasemzadeh, and G. Fortino, "Multi-sensor fusion in body sensor networks: State-of-the-art and research challenges," *Inf. Fusion*, vol. 35, pp. 68–80, May 2017.

[35] J. Surbiryala and C. Rong, "Cloud computing: History and overview," in *Proc. IEEE Cloud Summit*, Aug. 2019, pp. 1–7.

[36] Z. Dai, Q. Zhang, L. Zhao, X. Zhu, and D. Zhou, "Cloud-edge computing technology-based Internet of Things system for smart classroom environment," *Int. J. Emerg. Technol. Learn. (iJET)*, vol. 18, no. 8, pp. 79–96, Apr. 2023.

[37] T. Alam, "Cloud-based IoT applications and their roles in smart cities," *Smart Cities*, vol. 4, no. 3, pp. 1196–1219, Sep. 2021.

[38] L. M. Haji, O. M. Ahmad, S. Zeebaree, H. I. Dino, R. R. Zebari, and H. M. Shukur, "Impact of cloud computing and Internet of Things on the future internet," *Technol. Rep. Kansai Univ.*, vol. 62, no. 5, pp. 2179–2190, 2020.

[39] K. Plathong and B. Surakratanasakul, "A study of integration Internet of Things with health level 7 protocol for real-time healthcare monitoring by using cloud computing," in *Proc. 10th Biomed. Eng. Int. Conf. (BMEiCON)*, Aug. 2017, pp. 1–5.
[40] H. Tianfield, "Security issues in cloud computing," in *Proc. IEEE Int. Conf. Syst., Man, Cybern. (SMC)*, Oct. 2012, pp. 1082–1089.
[41] M. Bahrami and M. Singhal, "The role of cloud computing architecture in big data," in *Information Granularity, Big Data, and Computational Intelligence*, 2015, pp. 275–295.
[42] A. Singh and K. Chatterjee, "Cloud security issues and challenges: A survey," *J. Netw. Comput. Appl.*, vol. 79, pp. 88–115, Feb. 2017.
[43] S. Namasudra and K. Akkaya, *Introduction to Blockchain Technology*, 2023, pp. 1–28.
[44] V. Ballamudi, "Blockchain as a type of distributed ledger technology," *Asian J. Humanity, Art Literature*, vol. 3, pp. 127–136, Dec. 2016.
[45] H. T. M. Gamage, H. D. Weerasinghe, and N. G. J. Dias, "A survey on blockchain technology concepts, applications, and issues," *Social Netw. Comput. Sci.*, vol. 1, no. 2, pp. 1–15, Mar. 2020. [Online]. Available: https://api.semanticscholar.org/CorpusID:216223922
[46] P. J. Taylor, T. Dargahi, A. Dehghantanha, R. M. Parizi, and K.-K.-R. Choo, "A systematic literature review of blockchain cyber security," *Digit. Commun. Netw.*, vol. 6, no. 2, pp. 147–156, May 2020. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S2352864818301536
[47] S. Dilhara, "A review on application of hash functions and digital signatures in the blockchain industry," Tech. Rep., Sep. 2021.
[48] Z. Zheng, S. Xie, H. Dai, X. Chen, and H. Wang, "An overview of blockchain technology: Architecture, consensus, and future trends," in *Proc. IEEE Int. Congr. Big Data (BigData Congr.)*, Jun. 2017, pp. 557–564.
[49] P. Zhang, D. Schmidt, J. White, and A. Dubey, "Consensus mechanisms and information security technologies," *Adv. Comput.*, vol. 115, pp. 181–209, Jan. 2019.
[50] S. Lu, X. Zhang, R. Zhao, L. Chen, J. Li, and G. Yang, "P-raft: An efficient and robust consensus mechanism for consortium blockchains," *Electronics*, vol. 12, no. 10, p. 2271, May 2023. [Online]. Available: https://www.mdpi.com/2079-9292/12/10/2271
[51] S. Zhou, K. Li, L. Xiao, J. Cai, W. Liang, and A. Castiglione, "A systematic review of consensus mechanisms in blockchain," *Mathematics*, vol. 11, no. 10, p. 2248, May 2023. [Online]. Available: https://api.semanticscholar.org/CorpusID:258654276
[52] A. Singh, R. M. Parizi, Q. Zhang, K.-K.-R. Choo, and A. Dehghantanha, "Blockchain smart contracts formalization: Approaches and challenges to address vulnerabilities," *Comput. Secur.*, vol. 88, Jan. 2020, Art. no. 101654. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0167404818310927
[53] S. Aggarwal and N. Kumar, *Attacks on Blockchain-Working Model*, 2021.
[54] S. Rouhani and R. Deters, "Security, performance, and applications of smart contracts: A systematic survey," *IEEE Access*, vol. 7, pp. 50759–50779, 2019. [Online]. Available: https://api.semanticscholar.org/CorpusID
[55] Y. Huang, Y. Bian, R. Li, J. L. Zhao, and P. Shi, "Smart contract security: A software lifecycle perspective," *IEEE Access*, vol. 7, pp. 150184–150202, 2019. [Online]. Available: https://api.semanticscholar.org/CorpusID
[56] A. Luntovskyy and D. Guetter, "Cryptographic technology blockchain and its applications," in *Proc. Int. Conf. Inf. Telecommun. Technol. Radio Electron.*, 2018, pp. 14–33. [Online]. Available: https://api.semanticscholar.org/CorpusID:131989690
[57] G. Habib, S. Sharma, S. Ibrahim, I. Ahmad, S. Qureshi, and M. Ishfaq, "Blockchain technology: Benefits, challenges, applications, and integration of blockchain technology with cloud computing," *Future Internet*, vol. 14, no. 11, p. 341, Nov. 2022. [Online]. Available: https://www.mdpi.com/1999-5903/14/11/341
[58] M. Iqbal and R. Matulevicius, "Exploring Sybil and double-spending risks in blockchain systems," *IEEE Access*, vol. 9, pp. 76153–76177, 2021.
[59] R. Alajlan, N. Alhumam, and M. Frikha, "Cybersecurity for blockchain-based IoT systems: A review," *Appl. Sci.*, vol. 13, no. 13, p. 7432, Jun. 2023.
[60] J. Pourqasem, "Cloud-based IoT: Integration cloud computing with Internet of Things," *Int. J. Res. Ind. Eng.*, vol. 7, p. 12, Dec. 2018.
[61] R. Ramadan, "Internet of Things (IoT) security vulnerabilities: A review," *PLOMS AI*, vol. 2, no. 1, pp. 1–7, Oct. 2021. [Online]. Available: https://plomscience.com/journals/index.php/PLOMSAI/article/view/14
[62] G. Gochev, S. Enkov, E. Doychev, and A. Terziyski, "Challenges in collecting and transmitting data from resource-constrained IoT devices," in *Proc. 17th Int. Conf. CONCENTRATOR PHOTOVOLTAIC Syst. (CPV-17)*, 2022, Art. no. 040003. [Online]. Available: https://api.semanticscholar.org/CorpusID:252144817
[63] B. Ali and A. Awad, "Cyber and physical security vulnerability assessment for IoT-based smart homes," *Sensors*, vol. 18, no. 3, p. 817, Mar. 2018.
[64] D. Chen and H. Zhao, "Data security and privacy protection issues in cloud computing," in *Proc. Int. Conf. Comput. Sci. Electron. Eng.*, vol. 1, Mar. 2012, pp. 647–651.
[65] I. Indu, P. M. R. Anand, and V. Bhaskar, "Identity and access management in cloud environment: Mechanisms and challenges," *Eng. Sci. Technol., Int. J.*, vol. 21, no. 4, pp. 574–588, Aug. 2018. [Online]. Available: https://api.semanticscholar.org/CorpusID:169375709
[66] J. Lee and J. Lee, "Current research trends in IoT security: A systematic mapping study," *Mobile Inf. Syst.*, vol. 2021, no. 1, 2021, Art. no. 8847099.
[67] S. Kumari, M. Karuppiah, A. K. Das, X. Li, F. Wu, and N. Kumar, "A secure authentication scheme based on elliptic curve cryptography for IoT and cloud servers," *J. Supercomput.*, vol. 74, no. 12, pp. 6428–6453, Dec. 2018. [Online]. Available: https://api.semanticscholar.org/CorpusID:16492515
[68] M. H. Miraz and M. Ali, "Integration of blockchain and IoT: An enhanced security perspective," *Ann. Emerg. Technol. Comput.*, vol. 4, no. 4, pp. 52–63, Oct. 2020, doi: 10.33166/aetic.2020.04.006.
[69] A. Ethan and D. Alexander, "Leveraging blockchain technology for data integrity in clinical trials," Tech. Rep., Feb. 2023.
[70] G. Habib, "Integration of blockchain technology with cloud computing," *Encyclopedia*, vol. 14, no. -31, p. 341, 2022.
[71] N. Khoshavi, G. Tristani, and A. Sargolzaei, "Blockchain applications to improve operation and security of transportation systems: A survey," *Electronics*, vol. 10, no. 5, p. 629, Mar. 2021. [Online]. Available: https://api.semanticscholar.org/CorpusID:233666873
[72] L. Stockburger, G. Kokosioulis, A. Mukkamala, R. R. Mukkamala, and M. Avital, "Blockchain-enabled decentralized identity management: The case of self-sovereign identity in public transportation," *Blockchain, Res. Appl.*, vol. 2, no. 2, Jun. 2021, Art. no. 100014. [Online]. Available: https://api.semanticscholar.org/CorpusID:263617573
[73] H. D. Zubaydi, P. Varga, and S. Molnár, "Leveraging blockchain technology for ensuring security and privacy aspects in Internet of Things: A systematic literature review," *Sensors*, vol. 23, no. 2, p. 788, Jan. 2023. [Online]. Available: https://api.semanticscholar.org/CorpusID:255883787
[74] A. Botta, W. de Donato, V. Persico, and A. Pescapé, "Integration of cloud computing and Internet of Things: A survey," *Future Gener. Comput. Syst.*, vol. 56, pp. 684–700, Mar. 2016.
[75] A. Amairah, B. N. Al-tamimi, M. Anbar, and K. Aloufi, "Cloud computing and Internet of Things integration systems: A review," in *Proc. Int. Conf. Reliable Inf. Commun. Technol.*, 2019, pp. 406–414.
[76] E. Cavalcante, J. Pereira, M. P. Alves, P. Maia, R. Moura, T. Batista, F. C. Delicato, and P. F. Pires, "On the interplay of Internet of Things and cloud computing: A systematic mapping study," *Comput. Commun.*, vols. 89–90, pp. 17–33, Sep. 2016.
[77] J. A. Guerrero-Ibanez, S. Zeadally, and J. Contreras-Castillo, "Integration challenges of intelligent transportation systems with connected vehicle, cloud computing, and Internet of Things technologies," *IEEE Wireless Commun.*, vol. 22, no. 6, pp. 122–128, Dec. 2015.
[78] S. Karnouskos, N. Gaertner, N. Verzano, F. Beck, A. Becker, S. Bianchino, D. Kuntze, M. Perez, R. Roy, S. Saelens, and M. Schmut, "Experiences in integrating Internet of Things and cloud services with the robot operating system," in *Proc. IEEE 15th Int. Conf. Ind. Informat. (INDIN)*, Jul. 2017, pp. 1084–1089.
[79] S. Ahmed, M. Saqib, M. Adil, T. Ali, and A. Ishtiaq, "Integration of cloud computing with Internet of Things and wireless body area network for effective healthcare," in *Proc. Int. Symp. Wireless Syst. Netw. (ISWSN)*, Nov. 2017, pp. 1–6.
[80] R. Gooch and V. Chandrasekar, "Integration of real-time weather radar data and Internet of Things with cloud-hosted real-time data services for the geosciences (CHORDS)," in *Proc. IEEE Int. Geosci. Remote Sens. Symp. (IGARSS)*, Jul. 2017, pp. 4519–4521.
[81] F. Stradolini, N. Tamburrano, T. Modoux, A. Tuoheti, D. Demarchi, and S. Carrara, "IoT for telemedicine practices enabled by an Android application with cloud system integration," in *Proc. IEEE Int. Symp. Circuits Syst. (ISCAS)*, 2018, pp. 1–5.

[82] M. Alhussein, G. Muhammad, M. S. Hossain, and S. U. Amin, "Cognitive IoT-cloud integration for smart healthcare: Case study for epileptic seizure detection and monitoring," *Mobile Netw. Appl.*, vol. 23, no. 6, pp. 1624–1635, Dec. 2018.
[83] J. Dizdarević, F. Carpio, A. Jukan, and X. Masip-Bruin, "A survey of communication protocols for Internet of Things and related challenges of fog and cloud computing integration," *ACM Comput. Surv.*, vol. 51, no. 6, pp. 1–29, Nov. 2019.
[84] M. T. Khorshed, N. A. Sharma, K. Kumar, M. Prasad, A. B. M. S. Ali, and Y. Xiang, "Integrating Internet-of-Things with the power of cloud computing and the intelligence of big data analytics—A three layered approach," in *Proc. 2nd Asia–Pacific World Congr. Comput. Sci. Eng. (APWC CSE)*, Dec. 2015, pp. 1–8.
[85] J.-J. Sie, S.-C. Yang, Z.-Y. Hong, C.-K. Liu, J.-J. Chen, and S. C. Li, "Integrating cloud computing, Internet-of-Things (IoT), and community to support long-term care and lost elderly searching," in *Proc. Int. Comput. Symp. (ICS)*, Dec. 2016, pp. 452–457.
[86] H. El-Sayed, S. Sankar, M. Prasad, D. Puthal, A. Gupta, M. Mohanty, and C.-T. Lin, "Edge of things: The big picture on the integration of edge, IoT and the cloud in a distributed computing environment," *IEEE Access*, vol. 6, pp. 1706–1717, 2018.
[87] V. Dahiya and S. Dalal, "Fog computing: A review on integration of cloud computing and Internet of Things," in *Proc. IEEE Int. Students' Conf. Electr., Electron. Comput. Sci. (SCEECS)*, Feb. 2018, pp. 1–6.
[88] S. Ali, G. Wang, M. Z. A. Bhuiyan, and H. Jiang, "Secure data provenance in cloud-centric Internet of Things via blockchain smart contracts," in *Proc. IEEE SmartWorld, Ubiquitous Intell. Comput., Adv. Trusted Comput., Scalable Comput. Commun., Cloud Big Data Comput., Internet People Smart City Innov. (SmartWorld/SCALCOM/UIC/ATC/CBDCom/IOP/SCI)*, Oct. 2018, pp. 991–998.
[89] Y. Zhang, D. He, and K.-K.-R. Choo, "BaDS: Blockchain-based architecture for data sharing with ABS and CP-ABE in IoT," *Wireless Commun. Mobile Comput.*, vol. 2018, pp. 1–9, Nov. 2018.
[90] M. Ma, G. Shi, and F. Li, "Privacy-oriented blockchain-based distributed key management architecture for hierarchical access control in the IoT scenario," *IEEE Access*, vol. 7, pp. 34045–34059, 2019.
[91] M. Hossain, Y. Karim, and R. Hasan, "FIF-IoT: A forensic investigation framework for IoT using a public digital ledger," in *Proc. IEEE Int. Congr. Internet Things (ICIOT)*, Jul. 2018, pp. 33–40.
[92] N. M. Ahmad, S. F. A. Razak, S. Kannan, I. Yusof, and A. H. M. Amin, "Improving identity management of cloud-based IoT applications using blockchain," in *Proc. Int. Conf. Intell. Adv. Syst. (ICIAS)*, Aug. 2018, pp. 1–6.
[93] B. Zhao, P. Fan, and M. Ni, "Mchain: A blockchain-based VM measurements secure storage approach in IaaS cloud with enhanced integrity and controllability," *IEEE Access*, vol. 6, pp. 43758–43769, 2018.
[94] C. Qiu, H. Yao, C. Jiang, S. Guo, and F. Xu, "Cloud computing assisted blockchain-enabled Internet of Things," *IEEE Trans. Cloud Comput.*, vol. 10, no. 1, pp. 247–257, Jan. 2022.
[95] M. Yang, A. Margheri, R. Hu, and V. Sassone, "Differentially private data sharing in a cloud federation with blockchain," *IEEE Cloud Comput.*, vol. 5, no. 6, pp. 69–79, Nov. 2018.
[96] X. Liang, S. Shetty, D. Tosh, C. Kamhoua, K. Kwiat, and L. Njilla, "ProvChain: A blockchain-based data provenance architecture in cloud environment with enhanced privacy and availability," in *Proc. 17th IEEE/ACM Int. Symp. Cluster, Cloud Grid Comput. (CCGRID)*, May 2017, pp. 468–477.
[97] M. Wu, K. Wang, X. Cai, S. Guo, M. Guo, and C. Rong, "A comprehensive survey of blockchain: From theory to IoT applications and beyond," *IEEE Internet Things J.*, vol. 6, no. 5, pp. 8114–8154, Oct. 2019.
[98] M. S. Ali, M. Vecchio, M. Pincheira, K. Dolui, F. Antonelli, and M. H. Rehmani, "Applications of blockchains in the Internet of Things: A comprehensive survey," *IEEE Commun. Surveys Tuts.*, vol. 21, no. 2, pp. 1676–1717, 2nd Quart., 2019.
[99] T. M. Fernández-Caramés and P. Fraga-Lamas, "A review on the use of blockchain for the Internet of Things," *IEEE Access*, vol. 6, pp. 32979–33001, 2018.
[100] I. Makhdoom, M. Abolhasan, H. Abbas, and W. Ni, "Blockchain's adoption in IoT: The challenges, and a way forward," *J. Netw. Comput. Appl.*, vol. 125, pp. 251–279, Jan. 2019.
[101] D. V. Medhane, A. K. Sangaiah, M. S. Hossain, G. Muhammad, and J. Wang, "Blockchain-enabled distributed security framework for next-generation IoT: An edge cloud and software-defined network-integrated approach," *IEEE Internet Things J.*, vol. 7, no. 7, pp. 6143–6149, Jul. 2020.
[102] K. Gai, Y. Wu, L. Zhu, Z. Zhang, and M. Qiu, "Differential privacy-based blockchain for industrial Internet-of-Things," *IEEE Trans. Ind. Informat.*, vol. 16, no. 6, pp. 4156–4165, Jun. 2020.
[103] Y. Yu, S. Liu, P. L. Yeoh, B. Vucetic, and Y. Li, "LayerChain: A hierarchical edge-cloud blockchain for large-scale low-delay industrial Internet of Things applications," *IEEE Trans. Ind. Informat.*, vol. 17, no. 7, pp. 5077–5086, Jul. 2021.
[104] R. A. Memon, J. P. Li, J. Ahmed, M. I. Nazeer, M. Ismail, and K. Ali, "Cloud-based vs. blockchain-based IoT: A comparative survey and way forward," *Frontiers Inf. Technol. Electron. Eng.*, vol. 21, no. 4, pp. 563–586, Apr. 2020.
[105] N. Tapas, G. Merlino, and F. Longo, "Blockchain-based IoT-cloud authorization and delegation," in *Proc. IEEE Int. Conf. Smart Comput. (SMARTCOMP)*, Jun. 2018, pp. 411–416.
[106] S. Singh, I.-H. Ra, W. Meng, M. Kaur, and G. H. Cho, "SH-BlockCC: A secure and efficient Internet of Things smart home architecture based on cloud computing and blockchain technology," *Int. J. Distrib. Sensor Netw.*, vol. 15, no. 4, Apr. 2019, Art. no. 155014771984415.

LATIFA ALBSHAIER received the B.S. degree in computer information systems from King Faisal University, Al-Ahsa, Saudi Arabia, in 2018, where she is currently pursuing the M.S. degree in sciences in cybersecurity with the Department of Computer Networks and Communications. Her research interests include artificial intelligence, cybersecurity, the Internet of Things, cloud computing, and blockchain.

ALANOUD BUDOKHI received the B.S. degree in computer science from King Faisal University, Al-Ahsa, Saudi Arabia, in 2022, where she is currently pursuing the M.S. degree in sciences in cybersecurity with the Department of Computer Networks and Communications. Her research interests include artificial intelligence, cybersecurity, the Internet of Things, cloud computing, and blockchain.

AHMED ALJUGHAIMAN received the B.S. degree in computer and information technology(computer networks and information security) from Indiana University—Purdue University Indianapolis, in 2011, the master's degree in network security from DePaul University, in 2013, and the master's degree in information assurance and the Ph.D. degree in security engineering from the University of Colorado Colorado Springs, in 2019 and 2021, respectively. He is currently an Assistant Professor with the College of Computer Sciences and Information Technology, King Faisal University, Saudi Arabia. His research interests include underwater wireless sensor networks, underwater communications, software-defined networks, cybersecurity, computer networks, terrestrial wireless sensor networks, network protocols, network security, the Internet of Things, blockchain, and unmanned aerial vehicles.