Metaverse 2025, 6(2), 3367.
https://doi.org/10.54517/m3367

Article

Integration of IoT, fog, and cloud in a blockchain network for future smart cities

Yasaman Ghaderi[1], **Mohammad Reza Ghaderi**[2,*]

[1] Department of Urban Planning, Tarbiat Modares University, Tehran 1411713116, Iran
[2] Department of Electrical Engineering, Islamic Azad University, South Tehran Branch, Tehran 1584716911, Iran
*** Corresponding author:** Mohammad Reza Ghaderi, st_mr_ghaderi@azad.ac.ir

CITATION

Ghaderi Y, Ghaderi MR. Integration of IoT, fog, and cloud in a blockchain network for future smart cities. Metaverse. 2025; 6(2): 3367. https://doi.org/10.54517/m3367

ARTICLE INFO

Received: 3 March 2025
Accepted: 3 April 2025
Available online: 6 May 2025

Abstract: In recent times, the concept of smart cities has gained traction as a means to enhance the utilization of urban resources, delivering sustainable services across sectors like energy, transportation, healthcare, and education. Applications for smart cities leverage information and communication technologies (ICT), particularly the Internet of Things (IoT), cloud computing, and fog computing. By merging these technologies with platforms like the metaverse, cities can improve service delivery and create more engaging experiences for residents. The metaverse, in this context, serves as a virtual space for interactions between citizens and city authorities, contributing positively to urban planning and management. Nonetheless, data security and privacy remain significant challenges for smart cities implementing these technologies. To address this, blockchain-based security solutions can be effective in supporting sustainable smart city applications. By integrating IoT, fog computing, and cloud services into a blockchain framework, it's possible to establish a secure and advanced platform for the creation and deployment of applications aimed at sustainable urban development. This paper proposes a conceptual model that combines IoT, fog, and cloud technologies within a blockchain structure, enabling smart city applications to harness the strengths of each technology, thereby optimizing operations, improving service quality, and ensuring robust security.

Keywords: smart city; IoT; fog; cloud; blockchain; metaverse

1. Introduction

Urban centers are increasingly being reimagined as futuristic, intelligent hubs, often termed smart cities [1]. These cities are designed around core principles such as innovation, urbanization, enhanced quality of life (QoL), and sustainability. However, the rapid pace of population growth and urban expansion introduces significant social, economic, environmental, and technical challenges that threaten urban sustainability. Researchers suggest that smart cities can mitigate these issues by addressing problems like traffic congestion, healthcare access, air pollution, waste management, and resource scarcity. Consequently, governments are actively adopting intelligent frameworks to optimize resource utilization in urban areas [2].

The advancement of technologies such as the Internet of Things (IoT), cloud computing, fog computing, and software systems has been instrumental in driving smart city development. IoT enables seamless communication among physical devices, including sensors and actuators, forming interconnected networks that serve as the foundation of smart cities. To support these applications, robust cloud computing infrastructure is essential, providing scalable, on-demand computing power, data storage, and advanced software services. Fog computing further enhances these capabilities by offering real-time processing, improved location awareness, and better mobility and communication support for smart city applications [3]. Together, these technologies create a versatile platform for developing a wide range of applications aimed at optimizing urban services. By integrating IoT, fog, and cloud technologies into a unified system, a sophisticated framework emerges, enabling the creation and deployment of diverse smart city applications [4]. In this ecosystem, all urban components (vehicles, individuals, buildings, roads, hospitals, and utilities) are equipped with IoT, fog, and cloud technologies, along with intelligent programs, to enhance the efficiency of smart city operations.

Recent advancements in digital technologies, including IoT, fog computing, cloud computing, and cyber-physical systems, have transformed smart city applications [5]. These innovations are critical for managing urban information efficiently, fostering economic growth, and improving sectors like tourism and transportation [6].

In scenarios requiring immediate response, such as fire emergencies, patient monitoring, and real-time controls dependent on location, latency, and security, advanced computing paradigms like fog computing are indispensable. Fog computing complements cloud computing by operating closer to IoT devices, making it highly effective for smart city applications [7]. By embedding fog technology into cloud systems and IoT networks, data processing can occur near the source of data generation, reducing the need for extensive data transmission to the cloud. This approach minimizes network congestion, lowers bandwidth usage, and conserves energy [8].

The integration of fog, cloud, and IoT technologies creates a powerful platform for developing and deploying smart city applications. This platform leverages the strengths of IoT devices, fog nodes, and cloud services to enhance performance and functionality. However, trust in this platform is crucial for its success. Without reliability, the applications cannot provide the necessary support for smart cities [9].

As smart city technologies evolve, they generate and transmit vast amounts of data, raising concerns about data security and privacy. Blockchain technology has emerged as a foundational solution to these challenges [10]. It has the potential to transform smart city infrastructure, enabling secure and sustainable ecosystems for IoT applications. However, these advancements also introduce new challenges alongside opportunities [11].

Security remains a critical issue in smart cities due to the reliance on information technology (IT). Recent research has explored blockchain as a secure platform to address IT-related challenges in urban environments. Blockchain also enhances transparency and data traceability within decentralized networks. A unified system combining IoT, fog, cloud, and blockchain allows smart city applications to harness the strengths of each technology, improving operational efficiency, service quality (QoS), and security. This paper introduces an integrated platform that combines IoT, fog, and cloud technologies within a blockchain framework to enhance smart city applications. We demonstrate how blockchain can effectively resolve security challenges in this integrated platform.

This article examines the convergence of fog, cloud, IoT, and blockchain technologies in the context of sustainable smart city development. While exploring the benefits of integrating these technologies, we also address the persistent challenge of data security. We propose blockchain as a viable solution to the security issues inherent in the IoT-fog-cloud framework, paving the way for sustainable IoT applications in smart cities.

From this analysis, we propose a sustainable conceptual framework that leverages fog computing, cloud computing, and IoT devices to collect and process critical data. This framework incorporates blockchain technology to ensure cybersecurity, data integrity, and privacy in smart city applications. The platform enables the digital analysis of IoT-generated data, storing results in decentralized cloud repositories via fog computing, all secured by blockchain technology to support smart city initiatives.

Additionally, the proposed architecture adopts a layered approach, enabling the creation of a sustainable incentive model that could promote secure smart city applications. The article is structured as follows: Section 2 discusses the integration of IoT, fog, and cloud technologies, along with a review of relevant literature. Section 3 provides an in-depth exploration of blockchain technology. Section 4 introduces the proposed model, and the final section concludes with a summary and closing remarks.

2. Concepts and related works

2.1. Smart city

The primary aim of a smart city is to improve residents' quality of life (QoL), optimize urban resource utilization, foster sustainability, and reduce environmental impact. Achieving these objectives requires the implementation of cutting-edge optimization techniques and technological innovations. Numerous cities across the globe are striving to transition into smart cities, motivated by challenges such as rapid population expansion, underdeveloped land areas, energy limitations, resource scarcity, economic advancement, and the imperative for environmental preservation. The creation of smart cities demands sophisticated, interactive management of essential urban systems and infrastructures, encompassing energy grids, communication networks, water supply systems, transportation networks (roads, highways, vehicles, airports), healthcare facilities, and critical structures like bridges, tunnels, and subways [12]. This ambitious vision is made possible through the integration of information and communication technologies (ICT), which streamline and enhance the provision of services to citizens.

2.2. IoT, fog, and cloud

The IoT, fog, and cloud are rapidly evolving technologies that hold immense potential for application in smart cities. When integrated, these technologies can significantly boost the overall efficiency of urban systems. **Figure 1** illustrates a model showcasing the integration of these technologies for smart city applications. Fog-based platforms enhance the IoT-cloud framework by deploying small fog nodes at the network's edge, closer to IoT devices. Many smart city applications demand real-time control and localized services, which fog computing provides by bridging the gap between IoT devices and distant cloud servers [3].

For smart city applications, fog architectures are primarily categorized into two types: flat and hierarchical. In a flat fog architecture (as shown in **Figure 1**), all nodes perform similar functions and connect directly to IoT devices, with the fog layer positioned between the IoT and cloud layers. In contrast, hierarchical fog architecture (depicted in **Figure 2**) organizes fog nodes into multiple levels, each with varying capabilities. This hierarchical structure is preferred for its efficient communication and operational effectiveness, making it suitable for diverse smart city applications [13].

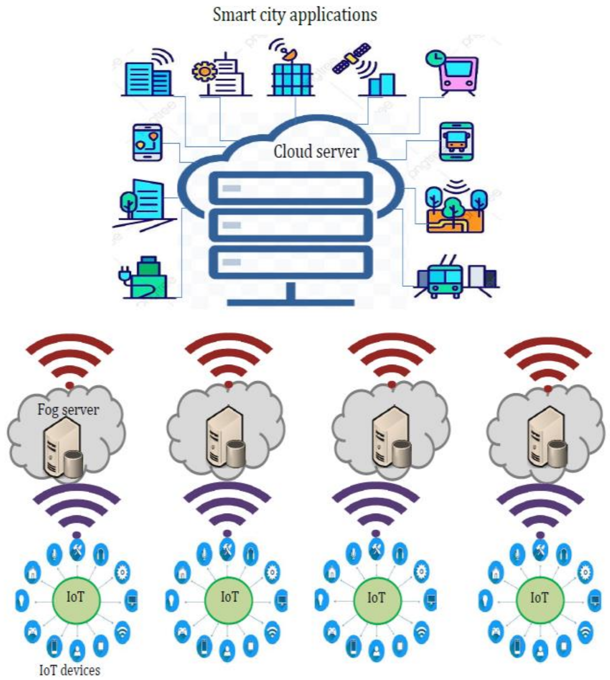

Figure 1. Integration of IoT, fog, and cloud for smart city applications (flat fog architecture).

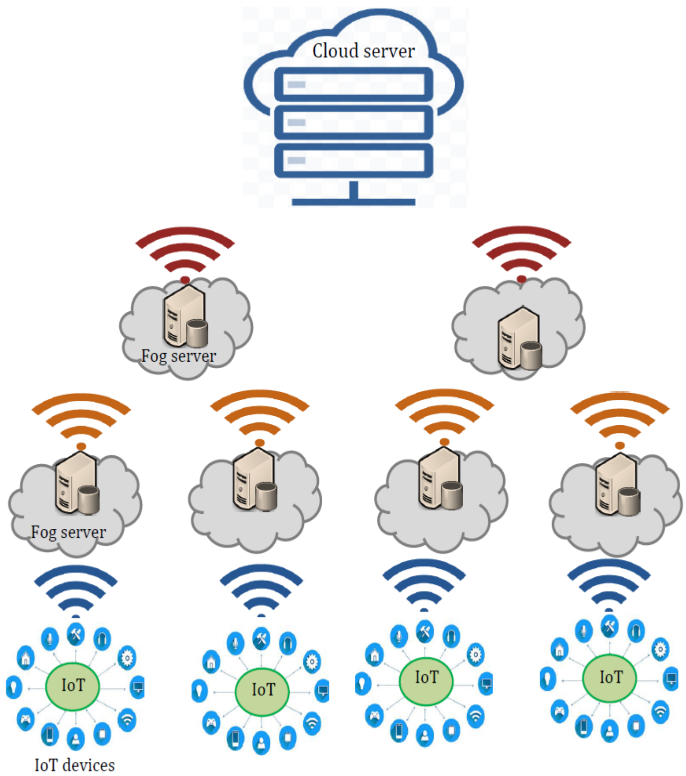

Figure 2. Integration of IoT, fog, and cloud for smart city applications (hierarchical fog architecture).

In a hierarchical setup, fog nodes are arranged in multiple tiers, facilitating communication and service delivery between IoT devices and the cloud. This creates several intermediary layers of fog nodes, where each level interacts with and activates services for both its upper and lower levels [14]. For example, in a two-level fog architecture designed for smart traffic lights or buildings, lower-level fog nodes handle functionalities specific to individual buildings or traffic lights, while higher-level nodes manage services for an entire neighborhood. While fog nodes are typically static, such as computers or routers, they can also be mobile, as seen in UAV-based fog systems [15].

Figure 3 presents the architectural layers of the integrated platform for smart cities [16]. Within this IoT-fog-cloud framework, IoT provides services like Sensing-as-a-Service (SaaS) and Configuration-as-a-Service (CaaS). Fog computing enhances these offerings by delivering localized, responsive services such as device control, data streaming, data caching, and location-based support.

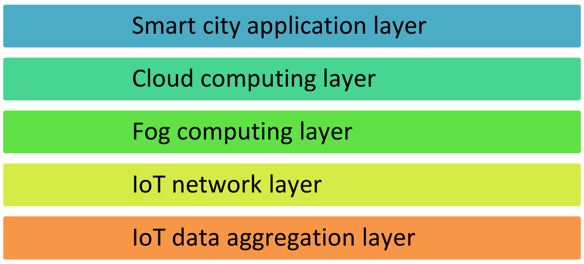

Figure 3. IoT-fog-cloud platform layers in smart cities [16].

Cloud computing also plays a vital role in the integrated platform, offering services like Software as a Service (SaaS). This allows developers to leverage cloud-based software for advanced functionalities such as data mining, machine learning (ML), decision support, and optimization tasks that demand substantial computational resources. Additionally, cloud computing provides Platform as a Service (PaaS), enabling developers to deploy applications directly onto the cloud infrastructure.

2.3. Related works

Currently, many cities in the developed world are progressing toward the implementation of smart city technologies. Notable examples include London, Stockholm, Dubai, New York, Barcelona, Hong Kong, Amsterdam, Singapore, Tokyo, Paris, and Copenhagen [17]. It is important to recognize that the term "smart city" can have different interpretations depending on cultural, economic, and geographical contexts. The significance of the smart city concept may vary from one location to another, influenced by factors such as growth rates, aspirations for improvement and reform, and the opportunities and expectations of residents. For instance, a smart city in India may differ significantly from those in countries like Russia, China, or the USA, as each region has unique needs shaped by the lifestyle of its citizens and its geographical characteristics [18].

The recognition and adoption of integrated technologies, such as fog, cloud, and IoT, have been integral to real smart city projects around the globe. Some smart cities have acknowledged the value of employing IoT-based fog computing and cloud integration to enhance their applications. Among the countries leading in smart city implementation, Spain stands out as one of the pioneers, currently boasting approximately 80 smart cities [19].

Barcelona, in particular, is focusing on utilizing fog computing to advance its smart city applications. The city emphasizes fog computing initiatives for various aspects, including energy management, access control, event-based video monitoring, traffic management, and on-demand connectivity. Similarly, Denver is investing in IoT solutions to develop its smart city programs. City officials have recognized the critical role of fog computing in their plans. "We see fog computing as a critical tool for enabling advanced digital applications that will enrich the experiences of the region's businesses, citizens, and visitors in the future," stated Jake Rishavy, Vice President of Innovation for Denver South [16].

Numerous studies have explored the use of an integrated platform combining fog, cloud, and IoT technologies. One significant application within smart cities is electronic healthcare systems. For instance, a study examines the use of an integrated Fog-Cloud-IoT platform for real-time remote diagnosis of cardiovascular diseases [20]. Extensive research efforts have focused on various applications and technologies pertinent to smart cities and urban areas. In this section, we review relevant studies related to the subject of this article, categorizing them into four main areas: IoT, cloud, fog, and their integration.

A detail analysis of various smart city technologies, data management strategies, and security challenges is provided in a study [21]. The network architecture and communication protocols for smart city systems are explored [22]. A study explores urban applications of wireless sensor networks (WSN) (a key element of the IoT) with an emphasis on monitoring and network challenges [23]. Several studies [24–26] have investigated a wide range of challenges faced by smart cities utilizing IoT technologies. Furthermore, a study examines the role of big data in smart city cloud services [12]. The significance of fog computing in smart cities has been highlighted in various studies [27], including proposals for multi-level hierarchical fog architectures designed for big data analysis in urban environments [28]. A thorough review of fog computing applications in smart cities is presented in the literature [29]. Additionally, a classification framework and potential applications for managing fog computing systems are explored in the study [30].

The studies mentioned above have been evaluated based on their architectural design, location-specific implementations, and maintenance requirements. The study examines fog computing applications in smart cities, including case studies from multiple urban environments [31]. The study reviews enabling technologies for fog computing in smart cities [32]. Other studies have addressed specific aspects of fog computing, such as architecture, security, and challenges in smart city applications [33–35]. The study examines IoT communication protocols for integration with fog and cloud technologies [36]. The study investigates the technical advantages of integrating IoT, fog, and cloud technologies [37].

In this study, we propose a novel model that integrates IoT, fog, and cloud technologies within a blockchain-based platform tailored for smart cities. This model not only harnesses the strengths of IoT, fog, and cloud systems but also incorporates blockchain technology to address critical security requirements, ensuring a robust and secure framework for smart city applications.

3. Blockchain technology

Per the National Institute of Standards and Technology (NIST), blockchain is characterized as a decentralized and immutable distributed ledger system that functions without central oversight. In this framework, every node in the blockchain ecosystem retains a copy of the ledger (or database). The technology utilizes a peer-to-peer network model to enable decentralized and distributed computing, which aims to enhance data sharing throughout the network. Notably, blockchain is not a standalone technology; it comprises multiple core technologies, including distribution, cryptography, consensus mechanisms, and smart contracts [38].

Currently, the distinctive features and functionalities of blockchain have drawn the attention of researchers interested in its potential applications across multiple domains such as manufacturing, insurance, finance, energy, and smart cities. A blockchain network is constructed from a sequence of "blocks" linked together, as depicted in **Figure 4**. Each block holds encrypted transactions (data) [39].

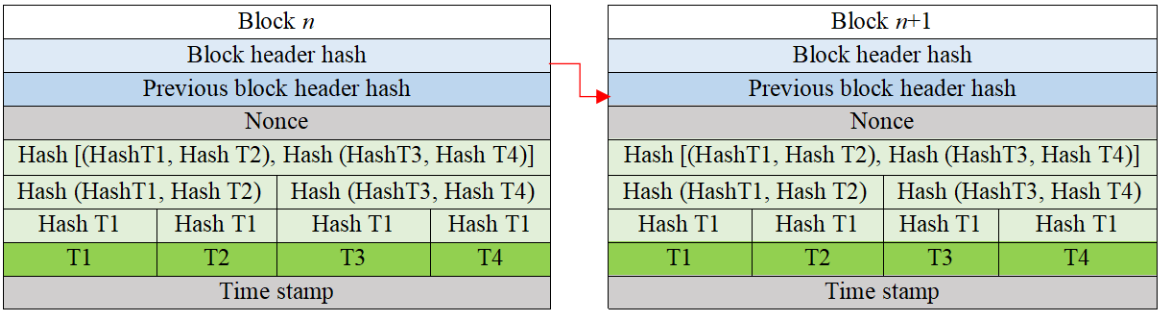

Figure 4. Blockchain structure.

Blockchain serves as a robust framework for ensuring data protection, decentralization, and distributed databases through its ledger structure (database), decentralized consensus protocols [40], smart contracts [41], and encryption of data [42]. All transaction records are stored within distributed blocks, making them immutable, which helps prevent alteration or tampering. This immutability is a vital characteristic that enhances network reliability and assists smart cities in tackling IT issues.

Each block within the blockchain includes data (transactions) that are disseminated across the network to ensure that the information remains accessible to all nodes (distribution feature). Furthermore, each block contains a "block header" that holds essential details such as the hash from the preceding block header, the creation timestamp of the block, a nonce, and the hash of the current block. A hash is produced by a hash function, while the nonce acts as an incremental counter included in the block header during the creation of a new block, enabling it to achieve the targeted hash by hashing all the block's data.

To validate transactions in the blockchain, network nodes engage in a consensus process [40]. After confirming a new transaction, this action leads to the formation of a new block that incorporates a set of preceding transactions. This newly created block is then propagated and stored across all network nodes. The integrity of the blocks and transactions established in the blockchain is maintained, offering a substantial benefit in mitigating data security concerns within smart cities. A consensus mechanism is utilized to authenticate newly added blocks, with various algorithms being proposed for different consensus methods utilized across blockchains [41].

4. Proposed model: Blockchain-based integration of IoT-fog-cloud

4.1. IT challenges and blockchain solutions

A. Challenges

- Data security: To enhance urban management and provide better public services, effective data collection and analysis are essential. The integrity and reliability of this data are crucial, as unauthorized alterations can lead to severe consequences and undermine the validity of data analysis. Thus, ensuring data security presents a significant challenge in smart cities, where vast amounts of data are generated.
- Centralized systems: The complexity of applications and the number of devices in smart cities are increasing exponentially. IoT networks, as the backbone of information technology, continuously generate large volumes of data. In traditional centralized systems, all data is stored on a single server, which creates a single point of failure (SPoF) and raises the risk of data loss. Additionally, IoT nodes in smart city networks require flexibility to connect to or exit the network as needed. Therefore, decentralized systems are more appropriate for smart cities than conventional centralized systems.
- Non-distributed databases: Citizens seek transparency, democracy, and participation in urban governance. Consequently, governments must share specific information, such as decision-making processes and environmental data, with the public. Sharing citizens' personal data, organizational data, and IoT-generated data can enhance city decision-making and management. However, traditional systems, which store data centrally, not only risk data loss but also fail to provide the transparency necessary for data review and tracking. As a result, conventional non-distributed systems cannot effectively support transparency, democracy, and public participation in smart cities.

B. Solutions

Blockchain-based security models can effectively address security challenges in smart city applications. Below are the proposed solutions to the IT challenges discussed earlier:

- Encryption and hashing: This approach addresses data security challenges. In a blockchain, data security is maintained through encryption and hashing techniques. Every transaction is secured by digital signatures, and data blocks are interconnected using a hash function, which performs one-way encryption. The hash function accepts input of any length and generates a fixed-length string as output. A minor change in the input data results in significant changes in the hash output. Therefore, if data in any block is altered, it affects all subsequent blocks, ensuring data immutability. This feature of blockchain is crucial for maintaining data security in smart cities.

- Decentralization: This solution counters the centralization challenge. Centralized systems for data aggregation and utilization inherently rely on a central authority for transaction authentication, which can lead to reduced system performance and higher costs. In contrast, blockchain operates without a centralized third party. Peer-to-peer networks in public blockchains function in a fully decentralized environment, enabling trust among unknown or unreliable nodes. Private blockchains, while operating in a closed and secure environment, utilize access control schemes to establish trust. All blockchain systems leverage decentralization to maintain data integrity and eliminate single points of failure.
- Distributed database: This solution tackles the non-distributed database challenge. Before a block is added to a blockchain network, all network nodes validate the block using consensus algorithms to reach a collective agreement. This process democratizes decision-making, as each node in the blockchain system contributes to the validation process. Moreover, each node is assigned an alias address to protect user identities, which is crucial for applications requiring user privacy. Since all transaction records are stored in a blockchain (akin to a general ledger or database) transparency is inherently maintained, with records equally distributed and accessible to all nodes in the network.

4.2. Proposed model

One of the primary advantages of blockchain is its ability to facilitate agreements among a group of institutions without needing a third party. In this context, the agreed-upon activities are recorded and securely shared across the network. Blockchain leverages a shared general ledger that is distributed among entities or users, utilizing a peer-to-peer network and cryptographic techniques for security. Consequently, once transactions are added to the blockchain, they become immutable and cannot be altered.

Additionally, the intrinsic features of blockchain enable the establishment of traceable audit trails, quantifiable components, and access to precise information about recorded transactions. This functionality allows for the validation, tracking, and accurate measurement of data within the blockchain network, making it highly effective for integrating diverse IoT, fog, and cloud systems managed by various organizations in a smart city. Such integration fosters a high degree of trust between organizations and their users.

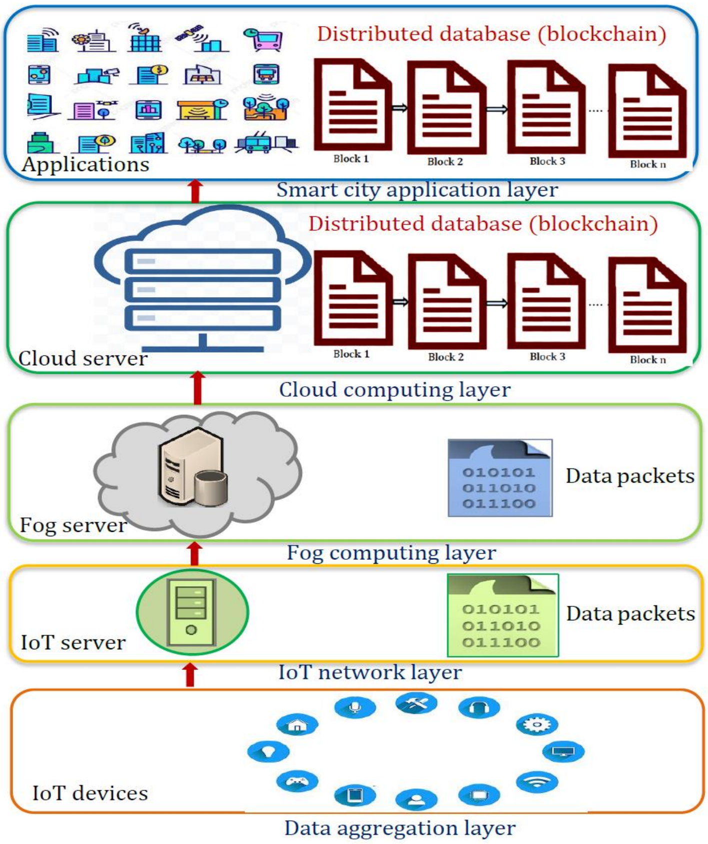

Figure 5. Blockchain-based proposed model based on IoT-fog-cloud layers in smart cities.

The proposed system model is depicted in **Figure 5**. In this framework, data collected from IoT systems (servers) across different regions of the smart city is stored using blockchain technology in an encrypted format. This data is distributed across databases within the fog, cloud, and application layers. The blockchain-based storage, operating within a peer-to-peer network and distributed databases, ensures that data can be traced across the system without the risk of tampering. In this architecture, blockchain extends from the edge of the IoT network layer through to the application layer, providing a secure and transparent foundation for data management.

A. Data flow

Figure 6 illustrates the data flow in the proposed model. In the first layer, where sensors and IoT devices are located, environmental data is collected and transmitted as binary data packets to the IoT network gateways. Thanks to the layered architecture of the model, these binary data packets are forwarded to fog servers and subsequently to the cloud.

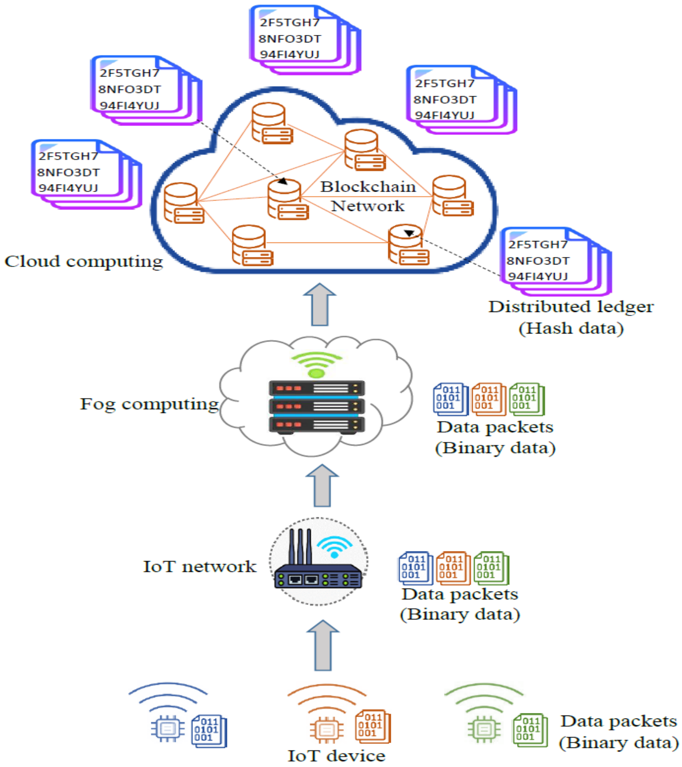

Figure 6. Data flow in proposed model.

Within the cloud system, a blockchain network is established. In this environment, the data packets are processed according to blockchain protocols, which convert them into encrypted hash data. This encrypted data is then distributed throughout the network, functioning as a distributed ledger or database. Users and applications can access this distributed database through the blockchain-based cloud system, ensuring secure and efficient retrieval of information.

B. Requirements

The IoT framework is pivotal in revolutionizing urban areas by improving aspects of city life such as energy efficiency, power distribution networks, waste management systems, transportation solutions, and safety protocols. While IoT provides insightful data to inhabitants and infrastructures, blockchain technology plays a key role in tackling data security issues, offering transparency and traceability. For a highly effective utilization of a unified platform catering to smart city services, several essential conditions must be fulfilled.

A primary challenge lies in the amalgamation of diverse IoT elements and devices, including sensors, actuators, wearable technology, and automation tools, alongside indispensable software services. This unified platform must be adaptable, scalable, and secure to meet the escalating needs of smart city initiatives. Furthermore, it should adeptly manage various components, mobile devices, and unpredictable operational environments.

Considering the substantial volume of data generated in urban areas, integrated platforms must effectively process big data and exploit it at different tiers. Immediate responsiveness is also vital, as numerous smart city solutions necessitate prompt decision-making and interventions. Most of these services require an integration of current optimization features, which typically depend on considerable cloud computing resources for both storage and processing tasks.

Unified platforms enable direct access to cloud resources while efficiently utilizing fog computing for data handling, real-time assistance, and information consolidation. This strategy also offers adaptability in various optimization levels. The type of optimization necessary is influenced by elements like productivity, availability of time, and precision, with data volume processed significantly affecting the required resources.

To adequately tackle optimization in smart cities, three essential elements need differentiation: 1) efficiency, 2) optimization, and 3) data management. The influence of these components varies based on the attributes and constraints of the needed services. Additionally, numerous smart city applications engage with decision-making processes or multi-objective optimization challenges. Hence, considering the intricate features, structure, and resources of the unified platform, it is vital to implement intelligent and adaptable decision support systems to facilitate suitable solutions. This need intensifies as the quantity of data collected and concerns demanding attention increase. The integration of pre-processing decision support can significantly enhance the effectiveness of smart city solutions. Moreover, decision-making and optimization strategies should have clearly defined objectives to steer their methodologies appropriately.

C. Advantages and disadvantages

The main benefit of combining fog, cloud, and IoT technologies for smart city initiatives is the capability to transfer data from IoT devices to cloud servers through fog nodes with minimal latency. This configuration facilitates real-time data sharing and processing via distributed fog nodes in smart city settings. Implementing these integrated technologies on a blockchain platform greatly improves aspects such as data security, integrity, and reliability.

On the downside, there are challenges associated with this setup. If fog nodes do not have adequate resources and energy to manage incoming data volumes, it may lead to delays in data transmission and processing at cloud servers. Such delays can profoundly influence essential smart city applications, especially in critical sectors like healthcare. Moreover, the need for blockchain infrastructure adds the requirement for additional hardware, consequently driving up costs due to its decentralized nature.

While the synergy of fog and cloud technologies with IoT on a blockchain platform provides advantages like rapid data transfer and secure processing, these benefits are accompanied by increased demands for resources and energy.

In conclusion, the integration of fog, cloud, IoT, and blockchain within smart cities brings both benefits and drawbacks, alongside a range of challenges and opportunities. These aspects need thorough consideration based on the significance and sensitivity of the smart city applications in question, ultimately resulting in a necessary balance between performance and resource allocation.

5. Platform challenges

While the integration of fog, cloud, IoT, and blockchain technologies offers numerous advantages for smart city applications, it also presents several challenges that need to be addressed, including reliability, heterogeneity, and integration effectiveness. These challenges warrant careful consideration.

To better understand these issues, we will examine them in two distinct sections: Challenges of Fog/Cloud/IoT Integration and Challenges of Blockchain Integration.

5.1. Fog/cloud/IoT challenges

1) Reliability

For IoT-based smart city applications to operate accurately and reliably, uninterrupted availability is critical. To avoid service disruptions or failures, it is essential to ensure the reliability and fault tolerance of both the applications and the infrastructure that connects the distributed components of fog, cloud, and IoT systems. Numerous studies have proposed solutions to tackle these challenges, many of which depend on the availability of extensive computing and storage resources.

To improve network reliability and fault tolerance between IoT nodes and fog systems, various solutions have been developed. These solutions primarily emphasize efficient resource management and fault tolerance mechanisms, especially for advanced and intricate fog computing architectures, such as multilayer structures. Resolving these issues is crucial for maximizing the performance and dependability of smart city applications.

2) Cost

The systems implemented in a smart city must be designed, developed, and operated efficiently and economically, as the integrated framework of cloud, fog, and IoT supports the services provided. Leveraging economies of scale can lead to cost reductions, particularly by creating and utilizing more integrated systems for various programs across different smart cities.

Additionally, designing modular structures can lower software development costs, as modules can be reused across different applications that require them. Employing advanced independent operational tools and controls can also minimize the need for manual monitoring and human intervention in the technology integration system, thereby significantly reducing operational costs.

3) Heterogeneity

In the IoT network, devices such as sensors, actuators, wearable sensors, surveillance cameras, mobile robots, personal smart devices, and drones are heterogeneous and serve various smart city applications. Their performance varies due to differences in processing, communication, and storage capabilities. In an integrated system, fog nodes can also be heterogeneous regarding their capabilities and services and may be deployed in different locations based on their specific communication capabilities. This diversity can pose difficulties for the effective use of integrated systems in smart city applications.

To address these challenges, employing abstract and modular concepts can be beneficial in managing heterogeneity. Careful design of interfaces that take into account the various capabilities of IoT devices and the software modules they utilize can significantly enhance interoperability and overall system performance.

4) Security and privacy

The integration of fog, cloud, and IoT technologies represents a shift from a centralized model, where computing services, data storage, and software operations are managed by a single system, to a distributed model. This transition brings about significant challenges related to security and privacy.

In distributed systems, ensuring compliance and the ability to verify security and privacy are paramount. As services are distributed across multiple platforms and data transmission within connected networks increases, smart city information becomes more vulnerable to a wide array of threats and security breaches.

To successfully implement integrated systems for smart city applications, it is essential to incorporate strong and efficient security and privacy mechanisms. These measures are vital to safeguarding the integration components and the services provided, ensuring a secure and reliable environment for smart city operations.

5) Integration efficiency

Another major challenge in implementing the integrated system is achieving optimal efficiency in connecting IoT devices with fog and cloud computing nodes and services for smart city applications. The diverse range of IoT devices, fog nodes, and cloud services often come with varying interfaces and connectivity limitations, complicating the integration process.

To ensure seamless operation, an integrated system may require additional services or adapters, which can reduce integration efficiency and potentially affect the overall performance of the applications. As a result, designing and managing effective yet efficient integration models becomes a complex endeavor.

One potential solution to address the integration of IoT devices and fog nodes is system standardization. Standardization can simplify connections and improve compatibility among the diverse components, thereby enhancing the efficiency of the overall integration process.

6) Mobility

In smart city environments where mobility is a critical factor, such as in vehicular systems, fog computing nodes are essential for ensuring uninterrupted connectivity and efficient network communication. These nodes enable interactions between mobile devices and IoT components, IoT devices and fog/cloud nodes, as well as among fog nodes themselves. However, supporting mobility introduces challenges, such as maintaining stable connections and addressing inefficiencies in resource utilization, particularly in dynamic systems like drones or autonomous vehicles. To overcome these challenges, real-time monitoring of connections and the implementation of efficient data delivery mechanisms are vital for system success. Additionally, enabling seamless service migration across fog nodes while meeting key performance metrics like reliability and low latency is crucial for effective mobility support [43].

7) Communication technologies

Integrating all components within a unified system often requires the use of multiple communication technologies, as relying on a single type is rarely sufficient. Typically, the communication channels connecting fog and cloud nodes differ from those used elsewhere. In terms of resource availability and energy consumption, fog and cloud nodes are far less constrained compared to IoT devices. Certain applications require interactions between IoT devices with varying capabilities, necessitating the adoption of diverse communication protocols and technologies. This heterogeneity introduces additional challenges in the design and deployment of such systems. As a result, smart city initiatives must be carefully planned and executed to accommodate the wide range of communication technologies involved.

8) Supervision and management

Smart city networks comprise thousands of IoT devices, hundreds of fog nodes, and multiple cloud systems, all of which must work together to ensure seamless connectivity and application functionality. To enable the smooth operation of these applications, the network must deliver a variety of functions. Effective and efficient communication within these networks relies heavily on robust monitoring and management systems. Advanced tools are essential for overseeing and controlling such large-scale networks. The deployment of sophisticated dashboards and monitoring solutions depends on the network's size and complexity. These tools play a critical role in maintaining the integrity of network components, simplifying reconfiguration processes, and identifying performance bottlenecks to ensure optimal network performance.

9) Real-time support

In smart city environments, fog nodes are often positioned near IoT devices, where data is produced and immediate actions are frequently needed. This proximity is a key benefit of fog nodes, as it enables them to deliver real-time support for IoT-based applications. By leveraging local system resources, fog nodes can facilitate real-time functionality for these applications [3]. However, the limited resources of fog nodes may hinder their ability to provide adequate real-time support as workloads increase, diminishing their overall effectiveness. One potential solution to this challenge is fostering active collaboration among multiple fog nodes. Such cooperation can enhance load balancing across the network, preventing situations where some nodes are overloaded while others remain underutilized, thereby achieving a more balanced network state [44]. It's important to recognize, however, that implementing this mechanism involves complex processes, such as enabling fog nodes to monitor each other's loads, developing efficient replication and migration strategies, managing resources collectively, and optimizing service and resource allocation to ensure effective load balancing.

5.2. Blockchain challenges

There are several challenges in integrating blockchain with smart city aspects, which are [45]:

1) Uncertainty

Blockchain technology is still a relatively new concept and as a result, viable blockchain models are scarce. This challenge is an obstacle to blockchain because it increases uncertainty.

2) Failure to display the identity of citizens

In blockchain networks, users typically operate under pseudonyms to maintain a degree of anonymity, which introduces privacy concerns. While these pseudonyms make users difficult to trace, ensuring their anonymity, the inherent transparency of blockchain technology means that all transactions are publicly visible. This transparency persists even though each user is linked to a public alias address, which serves as their identifier within the network [46].

3) Standardization

There is a lack of uniformity in the design of blockchain networks. This can create challenges during implementation as the platforms used for implementation include multiple partners from different sectors. For different use cases and different blockchain applications, the lack of a strong integration layer and blockchain standardization is observed [47].

4) Legal uncertainty

Several complex jurisdictional challenges can be presented in relation to the creation and operation of blockchain networks [48]. This is because blockchain-based applications sometimes lack a thorough understanding of the governing laws and regulations.

5.3. Scalability

We examine the issue of scalability in the proposed platform in two parts. The first part deals with scalability in cloud, fog, and IoT technologies and the second part deals with the infrastructure used for these technologies, i.e., blockchain.

5.3.1. Fog/cloud/IoT scalability

In a unified platform that integrates fog, cloud, and IoT, data storage is primarily managed by cloud computing, which also provides scalable, on-demand computing resources for smart city applications. Fog computing complements this by enabling the creation of large-scale, scalable IoT networks to support these applications. To achieve scalability, smart city systems can adopt either flat or hierarchical fog architectures. While flat architectures are simpler and easier to manage, hierarchical architectures introduce several challenges. These include determining the optimal number of levels, identifying the necessary services for each level, and allocating appropriate resource capacities to fog nodes at each level [16].

The choice of architecture plays a critical role in the scalability of the fog-cloud-IoT integration platform. While hierarchical structures offer greater flexibility, they can also introduce complexity, potentially impacting the performance and efficiency of smart city applications. To address these challenges, services must be strategically assigned to levels based on their resource requirements. Misplacement of services can lead to increased network traffic and unnecessary system loads, ultimately degrading application performance. Therefore, careful placement of services at the most suitable levels is essential to address scalability challenges, manage network traffic, and optimize system load. This approach ensures that scalability aligns with both the functional and non-functional requirements of smart city applications. Additionally, the resource capacities of fog nodes at each level must be carefully selected to support current service demands while accommodating future scalability needs.

5.3.2. Blockchain scalability

A key challenge in realizing the potential of blockchain technology is blockchain scalability [49]. Various factors such as cost and capacity, network and global define blockchain scalability.

- Blockchain scalability factors
    - Cost & capacity

Blockchain scalability requires storing a large amount of data in the block chain. This issue is an effective factor in blockchain scalability.

- Networking

In blockchain, each transaction is broadcasted to all nodes and subsequently; after mining a block, it is re-broadcasted to all nodes. In addition to consuming significant network resources, this process can also cause an increase in the propagation delay.

- Operating capacity

The time required to confirm a transaction and the block size for the transaction represent the throughput of the blockchain. When the network transactions increase, the block size will also increase, thus requiring more resources.

▪ Factors affecting scalability in blockchain

Scalability in blockchain is influenced by four factors: constraints, transaction costs, block size, and response time:

- Limitations

When processing a new transaction, information about the transaction is added to the ledger by each node. The increase in transaction history can create a big challenge for the whole system. Meanwhile, all data should be carefully preserved in the blockchain network. Because blockchain also faces limitations in terms of hardware, therefore blockchain scalability problems are created due to hardware limitations.

- Block size

The process of executing transactions by increasing the number of transactions in blockchain networks leads to an increase in transaction execution time. In addition, the increase in the number of transactions leads to an increase in the block size and thus affects the scalability.

- Response time

All transactions in the blockchain network should go through a validation process. As the number of transactions increases in general, they have to wait for longer periods for validation.

▪ Blockchain scalability solutions

However, various scaling challenges in blockchain can be tackled with smart solutions [50].

- Better consensus mechanisms

Improving consensus protocols in the blockchain network is one of the most commonly recommended solutions to the blockchain scalability challenge.

- Crushing

Sharding is a well-established approach to tackling the blockchain scalability issue as an on-chain solution. It involves dividing transactions into smaller, more manageable data sets known as “shards.” Rooted in the principles of distributed databases, sharding stands out as one of the most impactful layer 1 scaling solutions for blockchain networks. By distributing the workload across multiple shards, it enhances transaction throughput and overall network efficiency while maintaining the integrity and security of the blockchain.

- Nested blockchain

A decentralized network infrastructure leverages the main blockchain to establish parameters for the broader blockchain network. It also facilitates the execution of transactions across an interconnected network of secondary chains. Nested blockchain is a promising layer 2 solution designed to address the scalability challenges of blockchain systems. By operating on top of the main chain, it enables faster and more efficient transaction processing while maintaining the security and decentralization of the underlying blockchain.

6. Conclusion

The combination of IoT, fog, and cloud technologies offers a robust platform for developing smart city applications, with blockchain technology enhancing its security. This paper proposes a blockchain-based model that integrates IoT, fog, and cloud to support smart city applications while addressing security concerns. In this model, each technology fulfills specific roles within a secure framework, ensuring comprehensive functionality for smart city solutions. However, a major challenge lies in managing this integrated system as a unified entity. While the integration promises significant benefits, such as optimized resource utilization and improved quality of life (QoL), these advantages can only be realized after overcoming key challenges and resolving critical issues.

The fusion of fog, cloud, and IoT is poised to revolutionize the future of the Internet, enabling innovative applications in smart cities. Examples include smart homes and communities, efficient resource management, sustainable urban development, and advanced construction practices. This integration also addresses challenges associated with "Industry 4.0," such as data integration, networking, analytics, and the development of intelligent, self-adaptive, and resilient cyber-physical systems. Additionally, blockchain technology can be leveraged to tackle one of the most pressing challenges in smart cities: cybersecurity. By integrating blockchain with fog, cloud, and IoT, it becomes possible to establish secure, immutable, and decentralized data management systems. Blockchain ensures reliable data management and authentication control, addressing the shortcomings of traditional platforms that often connect IoT devices through insecure channels without proper authentication. Unlike conventional databases, blockchain restricts unauthorized access, making it a more secure alternative.

Despite significant progress in integrating fog, cloud, and IoT technologies for smart cities, several challenges remain unresolved. Key areas requiring further exploration include trust management, identity authentication, privacy protection, energy efficiency, and the optimal placement of fog nodes across a smart city. These issues are particularly critical given the potential deployment of thousands of fog nodes to support smart city applications. Future research directions for designing smart cities using this integrated infrastructure could focus on the following areas:

1) Computational cost

To enhance the design of heterogeneous IoT networks at the physical and media access control (MAC) layers, it is essential to reduce computational delays and minimize end-to-end computational costs. Further research is needed to develop resource allocation solutions that meet the demands of low latency, wide connectivity, high reliability, and high data volume for transferring, computing, and storing big data.

Additionally, addressing the challenges of connecting large numbers of IoT devices with limited radio resources and providing high-speed computing through edge computing servers requires innovative solutions.

2) Security of wireless communication networks

Current approaches to securing wireless communication networks still have limitations. Future research could focus on ensuring secure wireless communication within the integrated network infrastructure of smart cities. This includes developing robust security protocols and frameworks to protect data transmission and network integrity in the context of IoT, fog, and cloud integration.

3) Privacy

Authentication and identity protection using advanced security solutions are critical areas for future research. Strengthening existing security measures, such as efficient intrusion detection systems, intrusion prevention mechanisms, and the detection of malicious cyber activities, should be prioritized. These efforts will help safeguard sensitive data and ensure user privacy in smart city applications.

4) Application of nano networks

The use of cloud-based nano networks in smart cities, considering parameters such as bandwidth, hardware resource allocation, energy efficiency, and cost, presents a promising area for future study. Research could explore artificial intelligence (AI) and machine learning (ML)-based approaches for efficient management of these nanogrids. Integrating the IoT-Fog paradigm with cloud computing for nano network implementation is another topic worthy of investigation.

5) Increasing data processing power

The rapid development of smart city applications generates vast amounts of data that require efficient processing. For instance, data from smart transportation systems must be analyzed using big data techniques. As data volumes continue to grow over time, enhancing data processing capabilities will remain a critical focus for future research. This includes developing scalable and efficient methods to handle, analyze, and store large datasets in real time. These research directions aim to address the existing gaps and challenges in the integration of fog, cloud, and IoT technologies, paving the way for more efficient, secure, and scalable smart city solutions.

Author contributions: Conceptualization, YG and MRG; methodology, YG; software, MRG; validation, YG and MRG; formal analysis, YG; investigation, YG; resources, MRG; data curation, YG; writing—original draft preparation, YG; writing—review and editing, YG; visualization, YG; supervision, YG; project administration, YG; funding acquisition, MRG. All authors have read and agreed to the published version of the manuscript.

Conflict of interest: The authors declare no conflict of interest.

References

1. Datta A. New urban utopias of postcolonial India. Dialogues in Human Geography. 2015; 5(1): 3-22. doi: 10.1177/2043820614565748
2. Bibri SE, Krogstie J. Smart sustainable cities of the future: An extensive interdisciplinary literature review. Sustainable Cities and Society. 2017; 31: 183-212. doi: 10.1016/j.scs.2017.02.016
3. Bonomi F, Milito R, Zhu J, et al. Fog computing and its role in the internet of things. In: Proceedings of the first edition of the MCC workshop on Mobile cloud computing; 2012; ACM: New York, NY, USA. pp. 13–16.
4. Dutta J, Roy S. IoT-fog-cloud based architecture for smart city: Prototype of a smart building. In: Proceedings of the 2017 7th International Conference on Cloud Computing, Data Science & Engineering—Confluence. pp. 237–242.
5. Ahmed I, Zhang Y, Jeon G, et al. A blockchain- and artificial intelligence-enabled smart IoT framework for sustainable city. International Journal of Intelligent Systems. 2022; 37(9): 6493-6507. doi: 10.1002/int.22852
6. Zhang C. Design and application of fog computing and Internet of Things service platform for smart city. Future Generation Computer Systems. 2020; 112: 630-640. doi: 10.1016/j.future.2020.06.016
7. Songhorabadi M, Rahimi M, MoghadamFarid A, et al. Fog computing approaches in IoT-enabled smart cities. Journal of Network and Computer Applications. 2023; 211: 103557. doi: 10.1016/j.jnca.2022.103557
8. Escamilla-Ambrosio PJ, Rodríguez-Mota A, Aguirre-Anaya E, et al. Distributing computing in the internet of things: cloud, fog and edge computing overview. In: NEO 2016: Results of the Numerical and Evolutionary Optimization Workshop NEO 2016 and the NEO Cities 2016 Workshop. Springer International Publishing; 2018. pp. 87-115.
9. Mohamed N, Al-Jaroodi J, Jawhar I. Towards Fault Tolerant Fog Computing for IoT-Based Smart City Applications. In: Proceedings of the 2019 IEEE 9th Annual Computing and Communication Workshop and Conference (CCWC). pp. 0752-0757.
10. Khanna A, Sah A, Bolshev V, et al. Blockchain–Cloud Integration: A Survey. Sensors. 2022; 22(14): 5238. doi: 10.3390/s22145238
11. Roy M, Singh M, Radhakrishnan B. Blockchain Scalability: Solutions, Challenges and Future Possibilities. In: Proceedings of the International Conference on Signal & Data Processing; 2022. pp. 133-149.
12. Al Nuaimi E, Al Neyadi H, Mohamed N, et al. Applications of big data to smart cities. Journal of Internet Services and Applications. 2015; 6(1). doi: 10.1186/s13174-015-0041-5
13. Tang B, Chen Z, Hefferman G, et al. A Hierarchical Distributed Fog Computing Architecture for Big Data Analysis in Smart Cities. In: Proceedings of the ASE BigData & SocialInformatics 2015; 7–9 October 2015; Kaohsiung, Taiwan. p. 28.
14. Al-Jaroodi J, Mohamed N. PsCPS: A Distributed Platform for Cloud and Fog Integrated Smart Cyber-Physical Systems. IEEE Access. 2018; 6: 41432-41449. doi: 10.1109/access.2018.2856509
15. Mohamed N, Al-Jaroodi J, Jawhar I, et al. UAVFog: A UAV-based fog computing for Internet of Things. In: Proceedings of the 2017 IEEE SmartWorld, Ubiquitous Intelligence & Computing, Advanced & Trusted Computed, Scalable Computing & Communications, Cloud & Big Data Computing, Internet of People and Smart City Innovation (SmartWorld/SCALCOM/UIC/ATC/CBDCom/IOP/SCI); 4–8 August 2017; San Francisco, CA, USA. pp. 1758–1765.
16. Mohamed N, Al-Jaroodi J, Lazarova-Molnar S, et al. Applications of Integrated IoT-Fog-Cloud Systems to Smart Cities: A Survey. Electronics. 2021; 10(23): 2918. doi: 10.3390/electronics10232918
17. Javed AR, Shahzad F, Rehman S ur, et al. Future smart cities: requirements, emerging technologies, applications, challenges, and future aspects. Cities. 2022; 129: 103794. doi: 10.1016/j.cities.2022.103794
18. Malik S, Gupta K. Smart City: A new phase of sustainable development using fog computing and IoT. IOP Conference Series: Materials Science and Engineering. 2021; 1022(1): 012093. doi: 10.1088/1757-899x/1022/1/012093
19. Orejon-Sanchez RD, Crespo-Garcia D, Andres-Diaz JR, et al. Smart cities’ development in Spain: A comparison of technical and social indicators with reference to European cities. Sustainable Cities and Society. 2022; 81: 103828. doi: 10.1016/j.scs.2022.103828
20. Pati A, Parhi M, Alnabhan M, et al. An IoT-Fog-Cloud Integrated Framework for Real-Time Remote Cardiovascular Disease Diagnosis. Informatics. 2023; 10(1): 21. doi: 10.3390/informatics10010021
21. Gharaibeh A, Salahuddin MA, Hussini SJ, et al. Smart Cities: A Survey on Data Management, Security, and Enabling Technologies. IEEE Communications Surveys & Tutorials. 2017; 19(4): 2456-2501. doi: 10.1109/comst.2017.2736886
22. Jawhar I, Mohamed N, Al-Jaroodi J. Networking architectures and protocols for smart city systems. Journal of Internet

Services and Applications. 2018; 9(1). doi: 10.1186/s13174-018-0097-0
23. Rashid B, Rehmani MH. Applications of wireless sensor networks for urban areas: A survey. Journal of Network and Computer Applications. 2016; 60: 192-219. doi: 10.1016/j.jnca.2015.09.008
24. Arasteh H, Hosseinnezhad V, Loia V, et al. Iot-based smart cities: A survey. In: Proceedings of the 2016 IEEE 16th International Conference on Environment and Electrical Engineering (EEEIC); 7–10 June 2016; Florence, Italy. pp. 1–6.
25. Zanella A, Bui N, Castellani A, et al. Internet of Things for Smart Cities. IEEE Internet of Things Journal. 2014; 1(1): 22-32. doi: 10.1109/jiot.2014.2306328
26. Jin J, Gubbi J, Marusic S, et al. An Information Framework for Creating a Smart City Through Internet of Things. IEEE Internet of Things Journal. 2014; 1(2): 112-121. doi: 10.1109/jiot.2013.2296516
27. Tang B, Chen Z, Hefferman G, et al. Incorporating Intelligence in Fog Computing for Big Data Analysis in Smart Cities. IEEE Transactions on Industrial Informatics. 2017; 13(5): 2140-2150. doi: 10.1109/tii.2017.2679740
28. He J, Wei J, Chen K, et al. Multitier Fog Computing with Large-Scale IoT Data Analytics for Smart Cities. IEEE Internet of Things Journal. 2018; 5(2): 677-686. doi: 10.1109/jiot.2017.2724845
29. Javadzadeh G, Rahmani AM. Fog Computing Applications in Smart Cities: A Systematic Survey. Wireless Networks. 2019; 26(2): 1433-1457. doi: 10.1007/s11276-019-02208-y
30. Mahmud R, Ramamohanarao K, Buyya R. Application Management in Fog Computing Environments. ACM Computing Surveys. 2020; 53(4): 1-43. doi: 10.1145/3403955
31. Perera C, Qin Y, Estrella JC, et al. Fog Computing for Sustainable Smart Cities. ACM Computing Surveys. 2017; 50(3): 1-43. doi: 10.1145/3057266
32. Zahmatkesh H, Al-Turjman F. Fog computing for sustainable smart cities in the IoT era: Caching techniques and enabling technologies - an overview. Sustainable Cities and Society. 2020; 59: 102139. doi: 10.1016/j.scs.2020.102139
33. Naha RK, Garg S, Georgakopoulos D, et al. Fog Computing: Survey of Trends, Architectures, Requirements, and Research Directions. IEEE Access. 2018; 6: 47980-48009. doi: 10.1109/access.2018.2866491
34. Mukherjee M, Shu L, Wang D. Survey of Fog Computing: Fundamental, Network Applications, and Research Challenges. IEEE Communications Surveys & Tutorials. 2018; 20(3): 1826-1857. doi: 10.1109/comst.2018.2814571
35. Mouradian C, Naboulsi D, Yangui S, et al. A Comprehensive Survey on Fog Computing: State-of-the-Art and Research Challenges. IEEE Communications Surveys & Tutorials. 2018; 20(1): 416-464. doi: 10.1109/comst.2017.2771153
36. Dizdarević J, Carpio F, Jukan A, et al. A Survey of Communication Protocols for Internet of Things and Related Challenges of Fog and Cloud Computing Integration. ACM Computing Surveys. 2019; 51(6): 1-29. doi: 10.1145/3292674
37. Bittencourt L, Immich R, Sakellariou R, et al. The Internet of Things, Fog and Cloud continuum: Integration and challenges. Internet of Things. 2018; 3-4: 134-155. doi: 10.1016/j.iot.2018.09.005
38. Sikorski JJ, Haughton J, Kraft M. Blockchain technology in the chemical industry: Machine-to-machine electricity market. Applied Energy. 2017; 195: 234-246. doi: 10.1016/j.apenergy.2017.03.039
39. Wattenhofer R. The science of the blockchain. Inverted Forest Publishing; 2016.
40. Danzi P, Angjelichinoski M, Stefanovic C, et al. Distributed proportional-fairness control in microgrids via blockchain smart contracts. In: Proceedings of the 2017 IEEE International Conference on Smart Grid Communications (SmartGridComm). pp. 45-51.
41. Mengelkamp E, Gärttner J, Rock K, et al. Designing microgrid energy markets. Applied Energy. 2018; 210: 870-880. doi: 10.1016/j.apenergy.2017.06.054
42. Arslan-Ayaydin Ö, Shrestha P, Thewissen J. Blockchain as a Technology Backbone for an Open Energy Market. In: Regulations in the Energy Industry. Springer, Cham; 2020. pp. 65-84.
43. Li J, Shen X, Chen L, et al. Service Migration in Fog Computing Enabled Cellular Networks to Support Real-Time Vehicular Communications. IEEE Access. 2019; 7: 13704-13714. doi: 10.1109/access.2019.2893571
44. Qayyum T, Trabelsi Z, Malik AW, et al. Multi-Level Resource Sharing Framework Using Collaborative Fog Environment for Smart Cities. IEEE Access. 2021; 9: 21859-21869. doi: 10.1109/access.2021.3054420
45. Whaiduzzaman M, Barros A, Chanda M, et al. A Review of Emerging Technologies for IoT-Based Smart Cities. Sensors. 2022; 22(23): 9271. doi: 10.3390/s22239271
46. Xie J, Tang H, Huang T, et al. A Survey of Blockchain Technology Applied to Smart Cities: Research Issues and Challenges. IEEE Communications Surveys & Tutorials. 2019; 21(3): 2794-2830. doi: 10.1109/comst.2019.2899617
47. Deshpande A, Stewart K, Lepetit L, Gunashekar S. Distributed Ledger Technologies/Blockchain: Challenges, opportunities

and the prospects for standards. Overv. Rep. Br. Stand. Inst. 2017; 40: 40.

48. Zetzsche DA, Buckley RP, Arner DW. The Distributed Liability of Distributed Ledgers: Legal Risks of Blockchain. SSRN Electronic Journal. Published online 2017. doi: 10.2139/ssrn.3018214
49. Nasir MH, Arshad J, Khan MM, et al. Scalable blockchains—A systematic review. Future Generation Computer Systems. 2022; 126: 136-162. doi: 10.1016/j.future.2021.07.035
50. Kaur G, Gandhi C. Scalability in Blockchain: Challenges and Solutions. Handbook of Research on Blockchain Technology. Academic Press; 2020. pp. 373-406.