sustainability

MDPI

Article

Mobility Support 5G Architecture with Real-Time Routing for Sustainable Smart Cities

Amjad Rehman [1], Khalid Haseeb [2], Tanzila Saba [1], Jaime Lloret [3,4,*] and Zara Ahmed [1,5]

[1] Artificial Intelligence and Data Analytics (AIDA) Lab, CCIS Prince Sultan University, Riyadh 11586, Saudi Arabia; rkamjad@gmail.com (A.R.); drstanzila@gmail.com (T.S.); za1c20@soton.ac.uk (Z.A.)

[2] Department of Computer Science, Islamia College Peshawar, Peshawar 25120, Pakistan; khalid.haseeb@icp.edu.pk

[3] Integrated Management Coastal Research Institute, Universitat Politecnica de Valencia, 46730 Valencia, Spain

[4] School of Computing and Digital Technologies, Staffordshire University, Stoke ST4 2DE, UK

[5] Faculty of Engineering and Physical Sciences, University of Southampton, Southampton SO17 1BJ, UK

* Correspondence: jlloret@dcom.upv.es

Abstract: The Internet of Things (IoT) is an emerging technology and provides connectivity among physical objects with the support of 5G communication. In recent decades, there have been a lot of applications based on IoT technology for the sustainability of smart cities, such as farming, e-healthcare, education, smart homes, weather monitoring, etc. These applications communicate in a collaborative manner between embedded IoT devices and systematize daily routine tasks. In the literature, many solutions facilitate remote users to gather the observed data by accessing the stored information on the cloud network and lead to smart systems. However, most of the solutions raise significant research challenges regarding information sharing in mobile IoT networks and must be able to stabilize the performance of smart operations in terms of security and intelligence. Many solutions are based on 5G communication to support high user mobility and increase the connectivity among a huge number of IoT devices. However, such approaches lack user and data privacy against anonymous threats and incur resource costs. In this paper, we present a mobility support 5G architecture with real-time routing for sustainable smart cities that aims to decrease the loss of data against network disconnectivity and increase the reliability for 5G-based public healthcare networks. The proposed architecture firstly establishes a mutual relationship among the nodes and mobile sink with shared secret information and lightweight processing. Secondly, multi-secured levels are proposed to protect the interaction with smart transmission systems by increasing the trust threshold over the insecure channels. The conducted experiments are analyzed, and it is concluded that their performance significantly increases the information sustainability for mobile networks in terms of security and routing.

Keywords: Internet of Things; threats analysis; 5G; sustainable routing; mobile networks

check for updates

Citation: Rehman, A.; Haseeb, K.; Saba, T.; Lloret, J.; Ahmed, Z. Mobility Support 5G Architecture with Real-Time Routing for Sustainable Smart Cities. *Sustainability* **2021**, *13*, 9092. https://doi.org/10.3390/su13169092

Academic Editor: Manuel Fernandez-Veiga

Received: 15 July 2021
Accepted: 10 August 2021
Published: 13 August 2021

1. Introduction

IoT is a network of intelligent devices that exchange online data and support sustainable services. In all aspects of daily life, IoT plays a significant role with the integration of next-generation 5G networks [1–3] to facilitate many areas such as healthcare, vehicles, entertainment, industrial equipment, sport, homes, social networking, etc. IoT is one of the most advanced developments in the last century and has been used in many applications, but still, privacy and authentication are among research challenges [4–6] for sustainable computing. On the other hand, the number of connected devices is being increased consistently and their number has surpassed 50 billion, with the data produced by these devices also increasing exponentially. Indeed, the overall ubiquity of IoT facilitates day-to-day activities and enables people to interact with each other using 5G networks [7,8]. However, this holistic view also raises security issues such as data preserving, botnet attacks, hijacking IoT devices, etc.

The main challenges faced in IoT applications are manufacturing standards, update management, physical hardening, user's knowledge and awareness [9,10]. As a result, various IoT structures have been used to build and launch many IoT security applications. An IoT structure is a set of instructions, protocols, and specifications that simplifies the implementation of IoT. The accomplishment of these applications depends primarily on the characteristics of the IoT framework's ecosystems, with a special focus on safety mechanisms where protection and privacy problems are of vital importance [11–13]. Traditional IoT architecture is composed of three physical, network, and application layers. Devices are embedded in the physical layer that employ certain techniques to sense the environment and perform wireless communication to other devices [14–16]. A lot of research work has reported on IoT protection and privacy issues. However, once the latest technology arrives, it will overcome the security dilemma in IoT as well.

IoT has various uses in real-time contexts and therefore has made a huge impact in almost every sector of life. It combines sensors, smart devices, and RFID technologies through the Internet to create intelligent coordination. The sensors are tiny energy-constrained devices employed to sense information and deliver it over the network for intelligent decisions. These networks in an IoT environment come in a different structure, such as distributed, ubiquitous, grid, and vehicular. However, due to rapid development, extensive use, and their ubiquitous nature, IoT networks face various protection, privacy, and vulnerability issues in their applications and infrastructure. A few works on these security issues reported in the literature mainly employed machine learning and blockchain approaches. Different researchers have worked on different security aspects of IoT networks, including privacy preservation [17–19], authentications [20–22], access control [23–25], scalability [26–28], information sharing [29–31], and trust management [32–34]. However, proposing a decentralized communication platform for facilitating connected users over the insecure Internet and mobile network is a demanding task. In addition, the gathered data should be transmitted without compromising the identification of nodes and sensitive information. Figure 1 illustrates the components of the proposed architecture. The proposed architecture presents a sustainable development for public health applications, which is a significant factor in optimizing the system management and flow of information to assist society. It utilizes the technology of IoT, sensors, and 5G to share the resources and communication bandwidth efficiently. In addition, the cooperation of mobile sink highly distributes the load of IoT technology using the 5G network and increases mobility support and resource management.

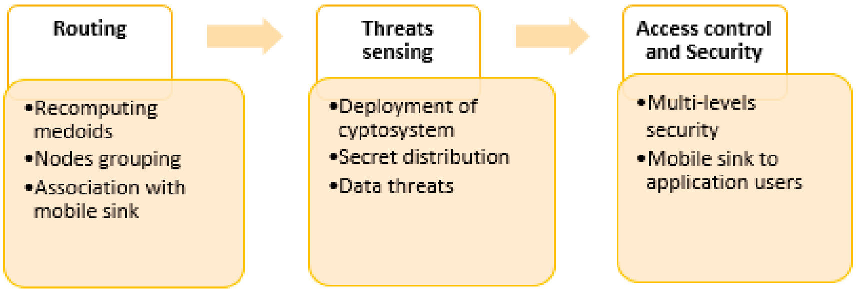

Routing
•Recomputing medoids
•Nodes grouping
•Association with mobile sink
Threats sensing
•Deployment of cyptosystem
•Secret distribution
•Data threats
Access control and Security
•Multi-levels security
•Mobile sink to application users

Figure 1. Main components of the proposed architecture.

The contributions of the proposed architecture are as given below.

i. It provides an algorithm to set the medical nodes into decentralized grouping and increases the connectivity for application users with the support of mobility and manages communication efficiently.

ii. Secret information is generated and shared among individuals using the computing power of gateway nodes. It achieves authentic association before the communication among medical nodes is initiated and improves sustainability using the 5G network.

iii. Multi-secured layers are provided for threat sensing and share the collected data with the confidence of authentication.

iv. The architecture is tested and validated along with the discussion using simulations, and its significance has been proven against other benchmark algorithms.

This research work is structured as follows. Section 2 presents a literature review of the existing work. In Section 3, the proposed architecture is introduced along with a detailed discussion. A simulation-based evaluation and a discussion of the results are presented in Section 4. At the end, Section 5 discusses the conclusion.

2. Related Work

In [35], the authors defined the required infrastructure and the protocol for the secure implementation of the IoT framework. They identified several new methods that could be used to address IoT security problems using machine learning and blockchain-based approaches. Advance 5G wireless sensor technologies [36,37] facilitate mobile communication for complex and highly dynamic environments. These technologies acquiring the information by sensing the data from a real-world environment and transmit to a sink node to fulfill the demands of the application users. To collaborate with mobile IoT networks, the solution should be robust and more reliable to support the requests of application users. In [38], the authors investigated the outage probability (OP) and predicted wireless communication. It was based on the improved grey wolf optimization algorithm and an Elman neural network was proposed. The simulation-based results illustrate that the prediction accuracy was higher than other solutions and managed the wireless transmission system more accurately for mobile IoT networks. The authors in [39] proposed an Internet of Things-based WBAN for disaster cases. It ensures life savings and smooth communication using technologies of the wireless network. In addition, a gateway selection algorithm using fuzzy logic was developed that aims to select a suitable wireless communication technology.

The authors in [40] maximized the task throughput for the IoT-enabled 5G network in the presence of heterogeneous task demands and constraint resources. They utilized multi-graph coloring and proposed an efficient two-stage process. The computational complexity and correctness of the proposed algorithm were analyzed. The simulation-based results demonstrate its efficacy against existing work. The authors in [41] suggested a rigorous prediction model using a rule-based machine learning classification method, i.e., the decision tree, on the noise-free accuracy dataset for real-life cell phone data of individual users. The Naive Bayes classifier and Laplace estimator were used to increase the model's prediction accuracy by minimizing noisy instances in the results. In [42], for Industrial Internet of Things (IIoT) devices, a machine learning-based anomaly detection system was proposed to detect cyber threats such as backdoor, order injection, and Structured Query Language (SQL) injection attacks. A distributed ledger-based blockchain (DLBC) technology was recommended in [43] to fix IoT protection and privacy problems such as spoofing and false authentication. In [44], a distributed intelligence system was proposed to reduce unnecessary data transfer to the cloud through immediate decision-making. They also resolved several security issues in the IoT environment using blockchain technology. In [45], classified devices with an ML approach were used to boost IoT environment security by identifying malicious data in the blockchain network. Similarly, a trust protection mechanism was introduced in [46] to provide stable and effective access control to identify and remove intrusions in a distributed IoT system. The authors in [47] presented a Safe Private Blockchain (SPB) that allows energy prosumers to negotiate energy rates and share energy with an IoT smart grid deployment. It consists of a three-layered trust management system in which trust is tracked based on the interactions between supply chain members, and trust. Finally, credibility is dynamically allocated based on these interaction scores [48]. In [49], a blockchain-based, privacy-preserving update protocol was suggested that allows users to update apps but also preserve their privacy. It increases the security level as compared to an existing solution with improved network performance. The authors in [50] proposed a clustering perturbation algorithm to preserve privacy for social networks that aims to introduce a strategy of exchanging attributes among vertices of the same degree randomly. It makes the network attackers pursue fake targets and accordingly maintains the stable structure of the observing field. In [51], the authors proposed a deep-reinforcement-learning-based quality-of-service (QoS)-aware secure routing protocol (DQSP). It ensures the QoS along with the extraction of knowledge from traffic history. In addition, it optimizes the routing policy and improves the data delivery performance against other solutions. The authors in [52] proposed a telemedicine system based on MEC and artificial intelligence for remote health monitoring and automatic disease diagnosis. The concept of mobile edge computing (MEC) among users and cloud systems reduces the problem of 5G scenarios in terms of latency and processing. Different computing technologies are also utilized in the proposed solution to significantly improve the efficacy of the patient treatment by decreasing the computing cost using an intelligent paradigm.

IoT technology has gained prominent attention for the development of sustainable smart cities with the support of a 5G network. Table 1 describes the research findings along with limitations based on the discussed work.

Table 1. Summary of discussed work.

Comparative Approaches	Contributions and Limitations
Existing solutions	• Many solutions offer quality-aware services and lead to higher bandwidth and improved data delivery performance. • However, most of the solutions face connectivity problems when the load on IoT nodes increases especially in 5G mobile networks. • Due to frequent network disconnectivity issues, it was also observed that most of the proposed solutions have a high data latency for real-time applications. • It was also noticed that 5G communication offers attention to many real-world network technologies for the growth of promising solutions with the collaboration of cloud and mobile infrastructure. • However, most of the network technologies with the collaboration of the 5G network lack security and communication trust.
Proposed architecture	A solution was developed using a 5G network for real-time public health application that increases the sustainability of complex operations in the presence of unpredictable events. It also facilitates application users with high communication bandwidth and optimal performance.

3. The Proposed Architecture

In this section, first, a summary is given of the proposed architecture. Later, the development components are described as depicted in Figure 1. In the first component, the medical nodes are categorized into peer-to-peer associations referred to as clusters. The clusters enable a decentralized communication platform and facilitate the connected nodes over the 5G communication system for gathering and transmitting the information. In addition, the transmission among clusters achieves a high throughput ratio by utilizing efficient bandwidth evaluation. The proposed architecture deploys gateway nodes around every cluster for the management of the IoT nodes. To integrate the mobility feature in the 5G architecture, a mobile sink is utilized that rotates in the proximity of the gateway nodes. It fulfills the demands of end-users regarding data collection and sharing for emergency purposes on time and then increases the delivery performance even if the connected number of users increases. The second component distributes the secret information between connecting nodes using the Rabin cryptosystem by utilizing the gateway's capabilities. Accordingly, the connected nodes within clusters can authenticate each other and avoid the entrance of unauthorized nodes. The medical data is protected based on multi-secured levels with nominal computing and processing overheads. Moreover, the application users are mutually authenticated in storage centers before accessing the online data with nominal processing costs.

In the beginning, the medical network is structured in the directed graph $G(\mathrm{N}, \epsilon)$, which consists of nodes N and edges ϵ. The nodes can be any sensor, physical device, or computing resource for sensing and processing medical data. All the entities are interconnected with neighbors with predefined distances and limited transmission power. During communication, if any entity moves from one cluster, it can be part of another cluster by utilizing the predefined distance factor. The proposed architecture makes use of centroid-based computation and produces various clusters by partitioning the n IoT nodes. The proposed architecture avoids the chances that the same network device may be a part of more than one cluster to decrease the issue of congestion. The proposed architecture exploits greedy search for the grouping of medical nodes and decreases the overall communication cost. Let us consider that m_i is the set of medoids [53] and are selected greedily, such that $i \epsilon k$. It associates each medical node to the nearest medoid m_i and computes the cost function by determining the commutative distance in the forming of clusters. Afterward, it again selects a set of medoids m_i and re-performs the aforementioned process. If it gives a better cost value, the value is swapped with the new m_i. Otherwise, the newly computed value is ignored. The nodes that are closest to the centroid with the highest channel bandwidth are selected as cluster heads. The proposed architecture exploits some gateway nodes in the proximity of computed clusters that act as intermediate points for data management and transmission to mobile sink. The gateway nodes advertise their identities (IDs) and location to the nearest clusters. As a result, the cluster heads located at the boundary of the gateway nodes respond with their ID and positioning information. Accordingly, gateway nodes store their initialization factors in the memory table. Unlike most of the existing work, the proposed architecture adopts a multi-hop transmission model from IoT nodes to gateways and from gateways to the mobile sink using maximum bandwidth Bd and minimum transmission load Tl. Each node computes a score Sc for the determination of forwarding among neighbors and can be defined in Equation (1).

$$Sc = max(Bd) + Min(Tl) \tag{1}$$

In Equation (1), Bd is inversely proportional to the incoming data traffic T for a communication channel. This means that if the value of T is high, then the available bandwidth indicates low weightage, and vice versa, i.e., $Bd \propto \frac{1}{T}$. On the other hand, Tl is directly proportional to the number of data blocks d that are transmitted on the communication channel at a time t. This means that the Tl weightage is high if the ratio of transmitting the data packets is high, i.e., $Tl \propto d$.

To offer a protected 5G communication system against threats among mobile sink and application users, the proposed architecture offers a fault-tolerant and high data rate solution. To cope with security for privacy and authentication, the proposed architecture utilizes the Rabin cryptosystem [54], which is an asymmetric cryptography technique. It generates the pair of public–private keys and distributes securely among associated nodes, where a public key is used for data encryption and the private key is used for data decryption. The cryptography-based security system for the generation of a set of keys is deployed on the gateway nodes. After the key generation, the gateway nodes distribute them among IoT nodes and mobile sink. We consider the sink mobile and rotating across the boundary of gateway nodes to support the real-time data efficiency with minimum delay. Let us consider that x_i and x_j are two large prime numbers and Y is the product of both numbers, as given in Equation (2).

$$Y= x_i.x_j \tag{2}$$

where Y is a public key and the pair of (x_i, x_j) is a private key.

Afterward, the generated keys are concatenated with an MAC value by using the private key of gateway nodes; thus, the IoT nodes authenticate the incoming pair of public–private keys K. The generated data from the nodes is encrypted by converting it to a number using reversible mapping such as $m < n$. Then the encryption process takes place, as given in Equation (3).

$$C= m^2 \ mod \ n \tag{3}$$

where C denotes ciphertext. In addition, the digital signature S' is made on the ciphertext C using source key private key ki to attain the data authentication as given in Equation (4).

$$S' = S_{n,ki}(C),\ ki\ \varepsilon\ \left(x_i, x_j\right) \tag{4}$$

On receiving the ciphertext C, the adjacent node performs the verification function α for both the incoming data and digital signature S', as given in Equation (5).

$$\alpha = D_{ki}\left(m',\ S'\right),\ \ ki\ \varepsilon\ Y \text{ and } m' = h(m) \tag{5}$$

Consequently, the IoT data is transmitted towards gateway nodes for aggregation and further processing in a multi-hop paradigm. In the proposed architecture, the deployed gateway nodes are interconnected with the mobile sink, which explicitly improves the high data rate for the delivery of sensitive information to storage centers. In addition, it offers a security scheme among mobile sink and storage centers in terms of privacy and integrity. In this stage, the sink node establishes a separate session with a storage center using the secret key K_i based on the additive congruential method [55], as given in Equation (6).

$$K_{i+1} = K_i + c \ mod \ m \tag{6}$$

where K is a sequence of pseudo-random numbers, m is modulus and should be > 0, and c is incremental value $0 \leq m$. The sink node integrates the incoming fixed-length IoT data and performs Exclusive-OR cipher C_i for their transmission, as given in Equation (7).

$$C_i = (D_i + D_{i+1} + \cdots + D_n) \oplus K_i + S' \tag{7}$$

Upon receipt in the medical center, first the incoming C_i is decomposed and the hash function S' is verified using the public key of the mobile sink. If successful, then it performs the decryption function using the same session key K_i and obtains the network data.

Figure 2 presents the flow chart of the proposed architecture. The flow chart was created to identify the various activities in transmitting the data of smart cities and increase sustainability against unpredictable conditions and risks. When data are gathered from the IoT network, the proposed architecture first groups the nodes using medoids and selects the most competent nodes for data forwarders. The cost of the medoid is also recomputed until the optimal value is obtained. The data forwarders are tagged as cluster heads for the established group. Tagged nodes are registered with the nearest gateway nodes to minimize the routing cost and improve response time. The mobile sink circulates in the proximity of the gateway nodes and interacts with application users directly. The gateway nodes perform the intermediate role between the IoT network and the mobile sink node. In case of any risk identification, it copes with a lightweight cryptosystem and reduces the chances of data insecurity during attacks. Moreover, the mobile sink establishes direct session dialogue with application users and upon verification of access control, the network data are forwarded. The proposed architecture supports application users in receiving the network data and offers a sustainable solution for emergency and real-time tasks.

Figure 3 shows the message flow of the proposed architecture to achieve a sustainable solution. At the beginning of the connection, the IoT nodes are registered by advertising their attributes and establishing routing tables. On this point, the values of the IoT nodes are advertised on specific conditions instead of preset intervals. Afterward, the data analysis is performed and a set of medoids is determined, and nodes are grouped in clusters using the nearest distance to the medoid. Next, nodes are tagged as cluster heads that are closest to the centroid. However, if more than one node is close to the centroid then the second option of resuming the battery power of the node is incorporated into the decision. The messages flow ends at this point to group the IoT nodes. To forward the collected data from smart cities, all the tagged cluster heads are registered with the gateway nodes. Upon successful registration, they receive a verification message from gateway nodes to send their data. Moreover, the gateway nodes analyze the security risks among incoming packets and upon identifying any threat, take appropriate security actions to eliminate the threat in the communication channels between the nodes and sink node. The message flow ends here to establish secure communication from the nodes to sink node using gateways. The application users send a request message to the sink node to obtain the required data. Upon receipt, first, the sink node establishes a secure session with the requestee and after the authenticity for data accessibility is verified, is the data are forwarded. Then, the message flow ends at this point.

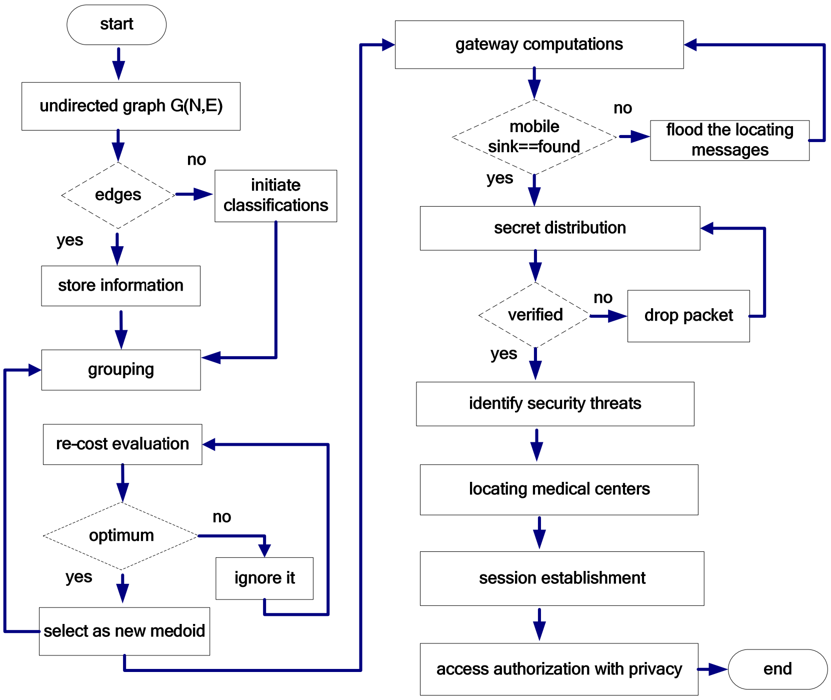


Figure 2. Work flow of the proposed architecture.

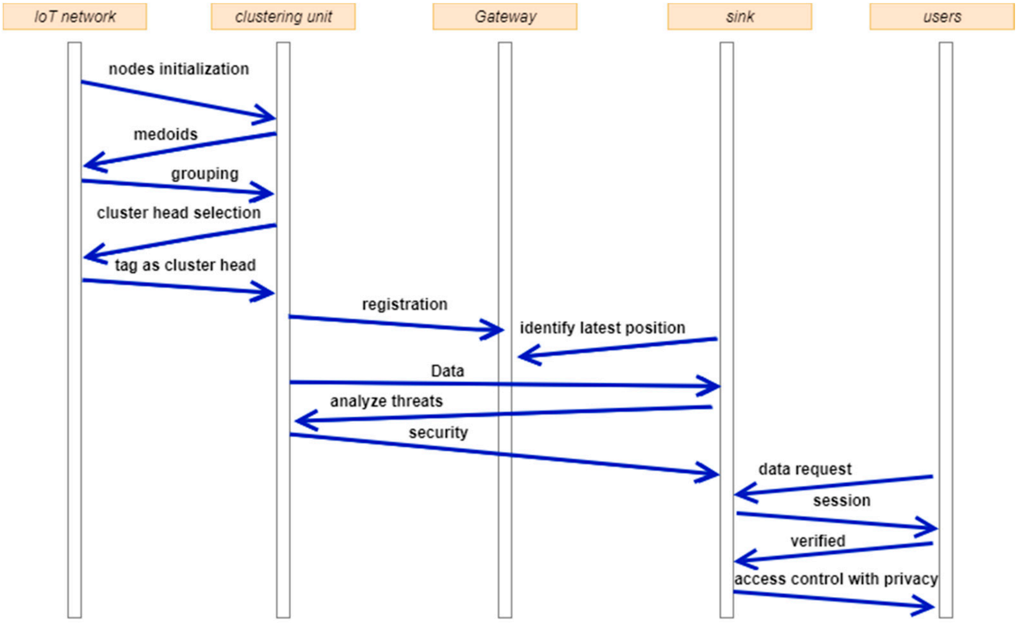


Figure 3. Message flow of the proposed architecture.

4. Simulations

This section presents the simulation setting and experimental results in detail. To simulate the real-time scenarios, we used NS-2 with default parameters that are utilized in various simulator systems [56,57]. In the experiments, we set the parameters as follows: The observing area was 10 × 10 m^2. The area was split into various clusters and the transmission range of each medical node was set to 3 m. The number of medical nodes that can sense and transmit the data continuously to the sink node was set to 20. The simulation was executed for 1000 to 5000 rounds. The initial energy for each node was 2 J and the size of the carrying data packets per node was set to 64 bits. The cache memory for each was set at 15 Mb. In addition, a few nodes were assumed to be malicious entities to identify security threats and evaluate the effectiveness of the proposed architecture. Table 2 demonstrates the simulation environment of the set of experiments.

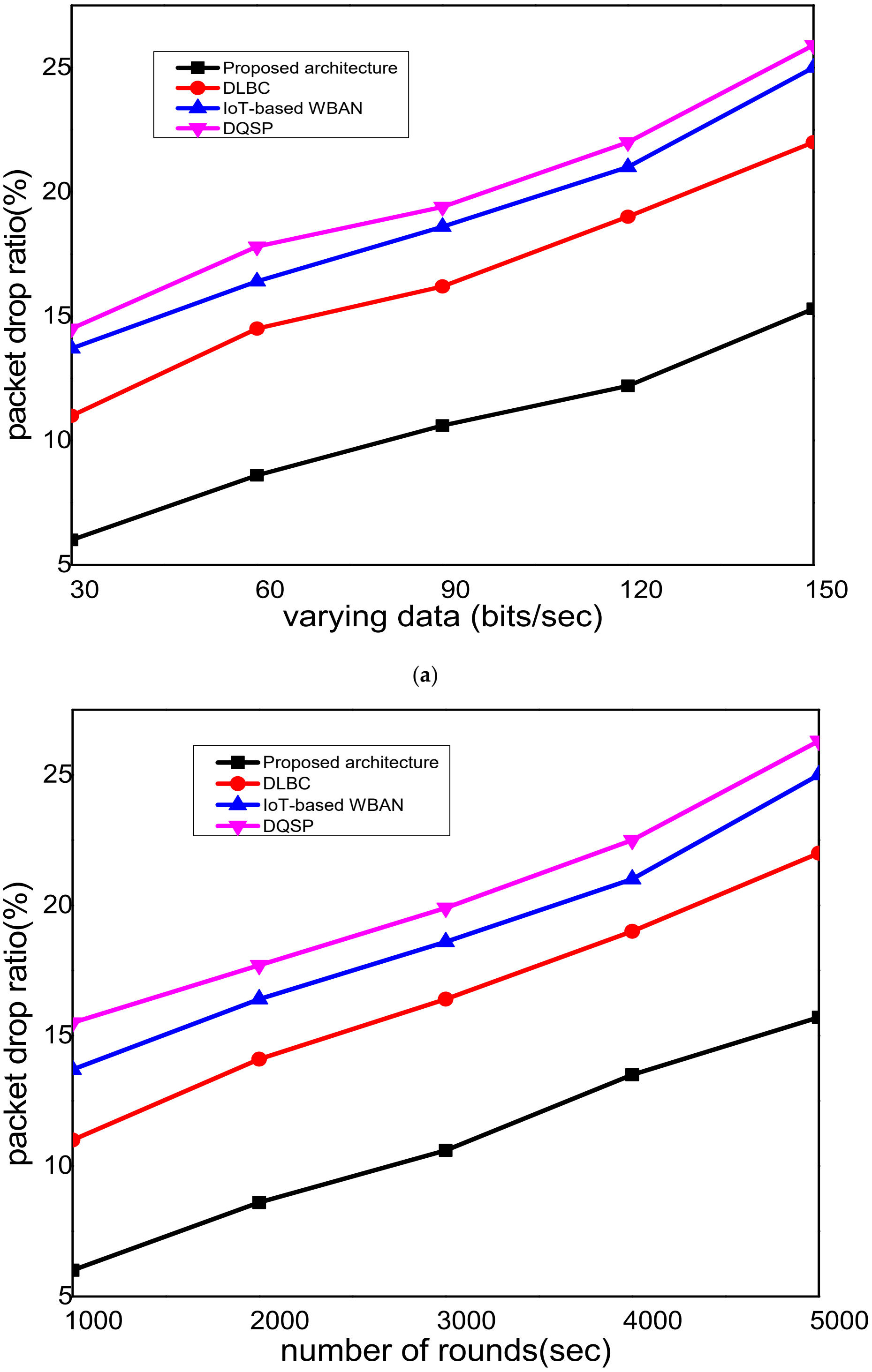
Table 2. Default simulation factors.

Parameter	Value
Medical nodes	50
Wireless links	Asymmetric
Data packet	64 bit
Transmission power	3 m
Initial energy	2 J
Cache memory	15 Mb
Size of payload	512 bytes
Rounds	1000 to 5000
Gateway nodes	10
Malicious nodes	10–20
Observing field	10 × 10 m^2
Frequency	2.4 GHz

Results

This section presents the evaluation results and discussion of the proposed architecture against the existing solution in terms of network packet drop ratio, route breaches, success rate, complexity time, and resource consumption. The experiments were conducted based on the varying data rates and the number of rounds. Figure 4 depicts the performance analysis of the proposed architecture with the existing work in terms of the packet drop ratio and varying data rates and the number of rounds. It was observed that the proposed architecture significantly decreased the packet drop ratio by an average of 12% and 16%, unlike other solutions. This was due to the proposed architecture noticing the bandwidth and transmission load on the selected IoT node for forwarding medical data. It also made use of the gateway nodes that explicitly improved the management of the network nodes and their association in clusters using the *k*-medoid algorithm, which increased the stability of the network with an increased delivery confidence level. Moreover, the proposed architecture exploited a robust secured multi-level algorithm that eliminated the malicious operations on medical data and increased the successful packet delivery performance.

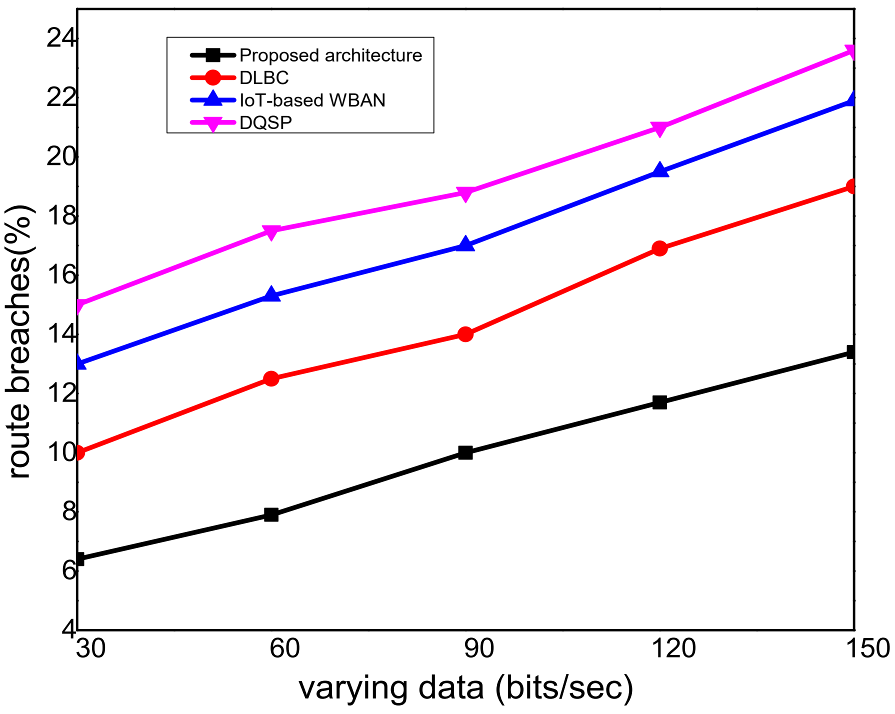
Figure 5 depicts the performance evaluation of the proposed architecture with other solutions in terms of route breaches under varying data rates and the number of rounds. It was seen that the proposed architecture decreased the ratio of route holes by an average of 13% and 15%, unlike the existing solution. It was observed that the existing solution incurred extra communication overheads in routing that explicitly increased the usage of network resources. In addition, the ratio of route breaches rose when the data sending rate increased. It was also observed that with the increasing number of faulty nodes, the number of bogus packets was too high and affected the data integrity. As a result, most of the time, it compromised sensitive information with several times of re-transmission. Therefore, the design of the proposed architecture focuses on providing a more secure and authentic solution for decreasing network threats for connected users. It provides a multi-level of security, i.e., from IoT nodes to gateway nodes, from gateways nodes to mobile sink, and from the mobile sink to storage centers. The proposed architecture assists with reliably connecting users and offers secured delivery performance against malicious attacks.



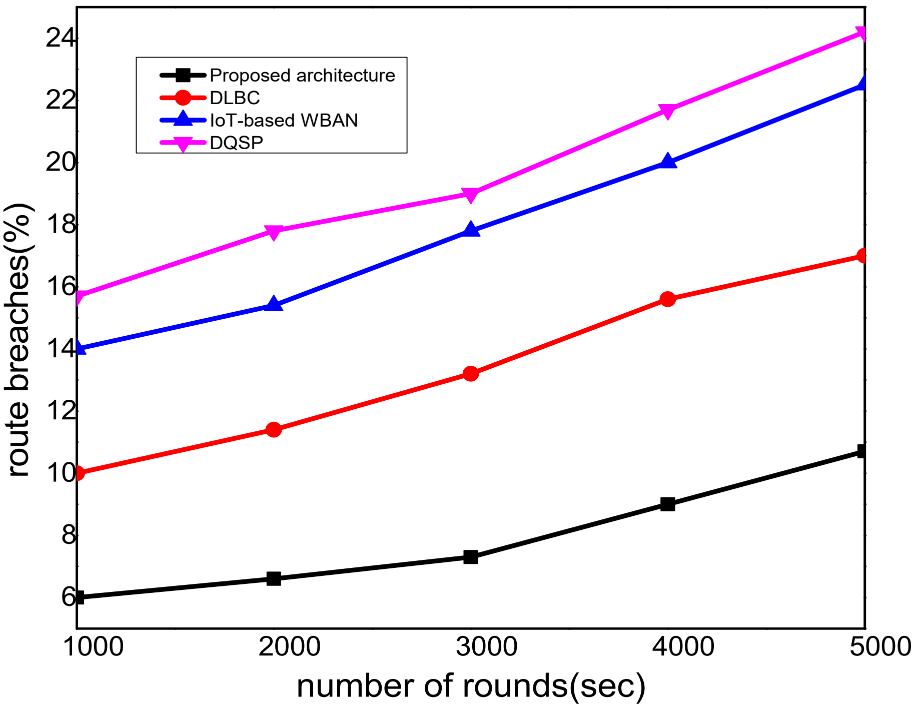
(**a**)

(**b**)

Figure 4. Scenarios of (**a**) analysis of the packet drop ratio under a varying data rate of 30 to 150 bits/s, and (**b**) analysis of the packet drop ratio under a varying number of rounds, from 1000 to 5000.



(**a**)



(**b**)

Figure 5. Scenarios of (**a**) analysis of route breaches under a varying data rate of 30 to 150 bits/s, and (**b**) analysis of route breaches under a varying number of rounds, from 1000 to 5000.

Figure 6 illustrates the experimental results of the proposed architecture in terms of the success rate against existing work and varying data rates and the number of rounds. Based on the numerical finding, it was noticed that the proposed architecture increased the delivery ratio by an average of 11% and 14%. This was because, based on the lowest cost, the network nodes were divided into clusters and they associated with their nearest gateway nodes. The deployed gateway nodes reduced the energy consumption of IoT nodes in forwarding the collected data. Unlike most of the other solutions that do not cope with the optimal transmission system, our proposed architecture adopts a constraint-oriented decision for the selection of forwarders among IoT nodes to gateway nodes. The mobile sink also makes it more realistic to gather the incoming observed data and transmit them to the users' end with the integration of the 5G network. It has a direct association with gateways to increase the network throughput with nominal network overhead. Moreover, the utilization of a 5G network increases the bandwidth capacity of the shared channels and maximizes the ratio of data delivery.

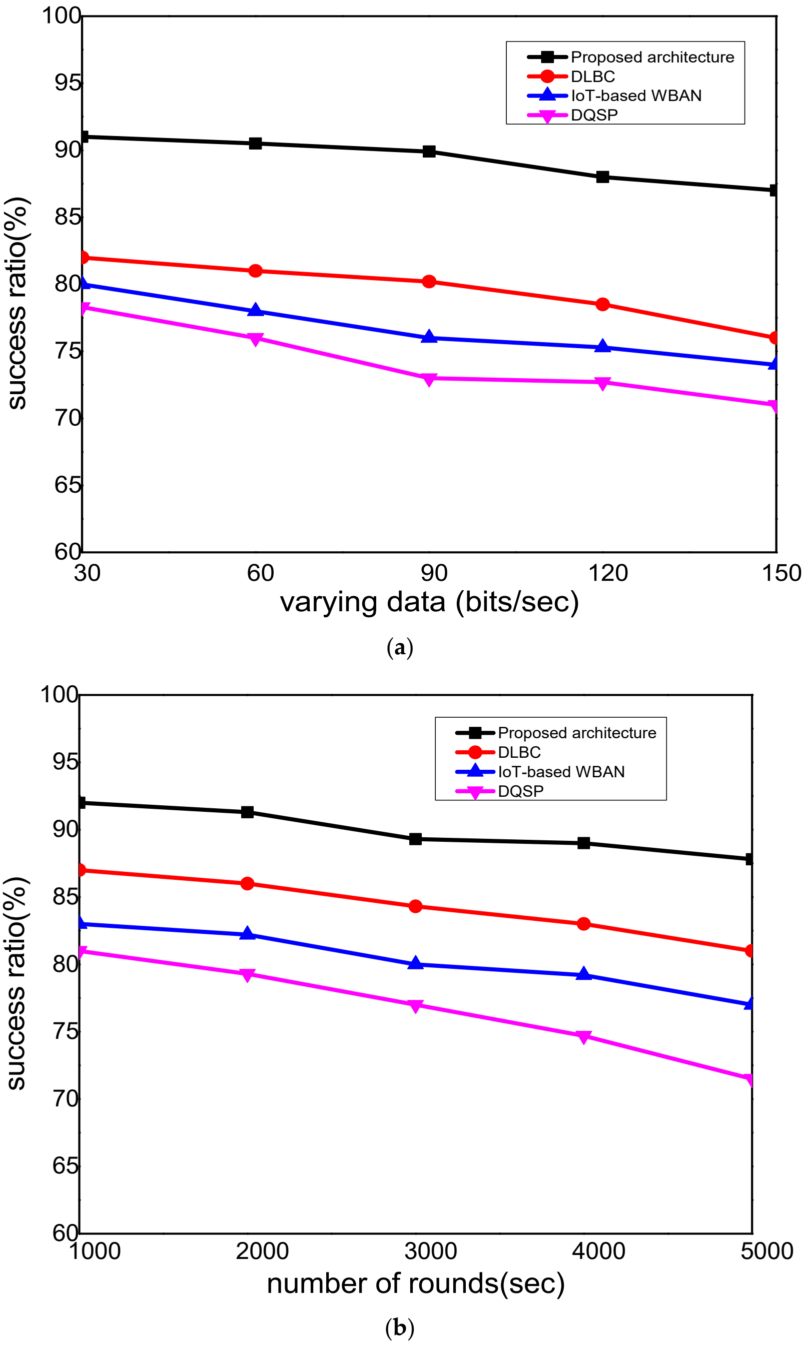
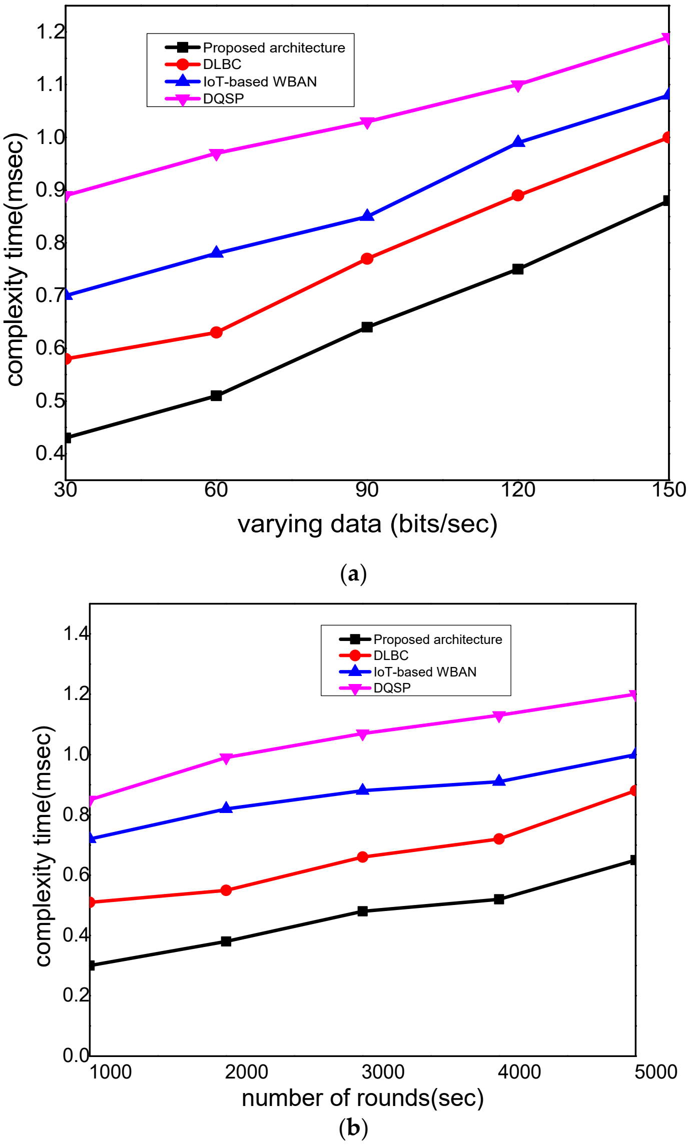


Figure 6. Scenarios of (**a**) analysis of the success ratio under a varying data rate of 30 to 150 bits/s, and (**b**) analysis of the success ratio under a varying number of rounds, from 1000 to 5000.

Figure 7 illustrates the performance of the proposed architecture against existing solutions for complexity time under varying data rates and several rounds. It was seen that it significantly reduced the rate of response time by an average of 13% and 15%, unlike the existing solutions. In the high data generation factor, it was noticed that existing solutions incurred rapid route re-organization and disruption due to the constraint resources of IoT technology being overlooked. In addition, malicious nodes could drop the public health data and include false control packets that further increased the load and created congestion in the transmission medium. Therefore, medical data experienced a delay in forwarding to the end-users and as a result, users were not able to obtain a response to their demands on time. On the other hand, the proposed architecture associates the network nodes with a secure cryptosystem and makes the information private against threats. In addition, it offers authentic communication in the existence of bogus packets and eliminates the irrelevant activities without confirmation of the nodes' uniqueness. Accordingly, it decreases the probability of route damages, and ultimately, it reduces the value of the network complexity.

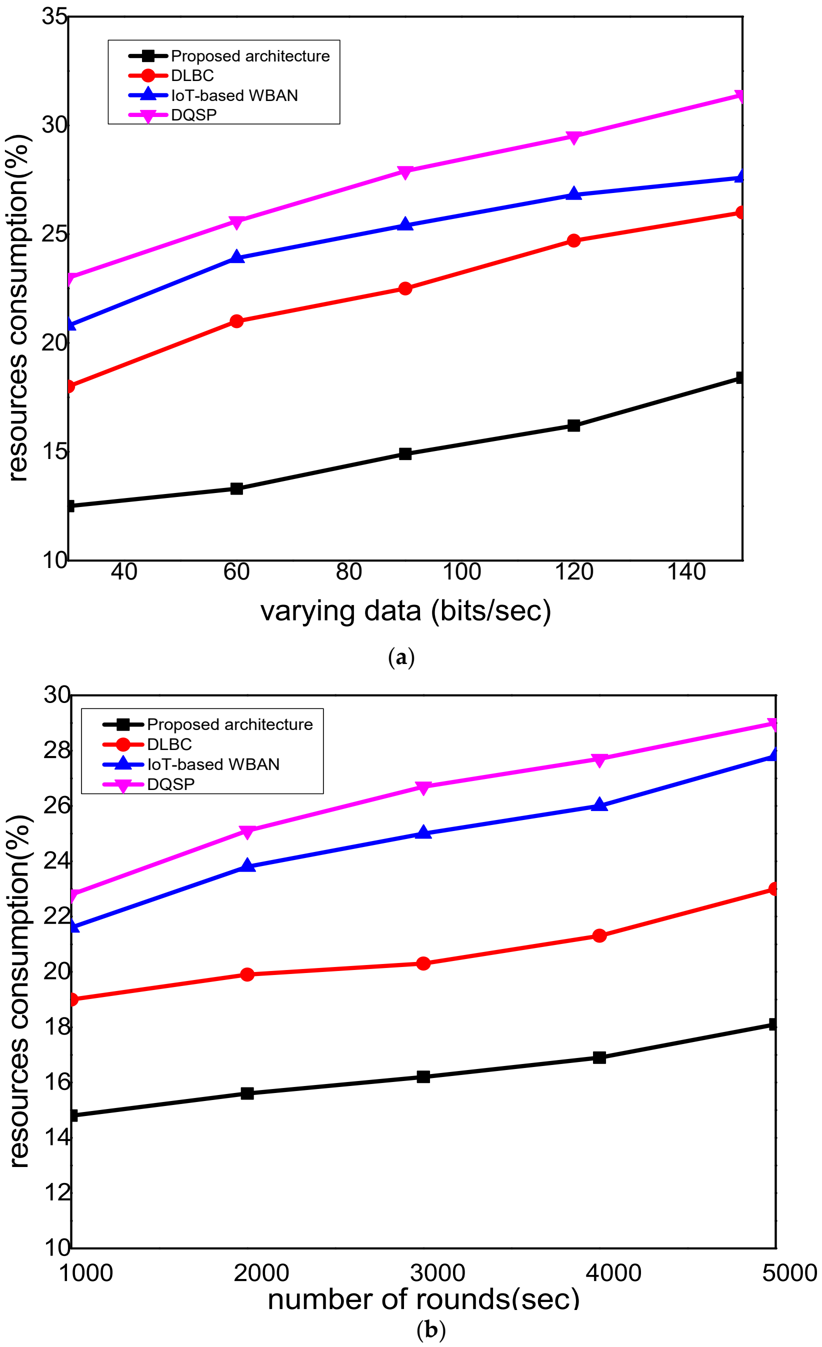


(**a**)

(**b**)

Figure 7. Scenarios of (**a**) analysis of complexity time under a varying data rate of 30 to 150 bits/s, and (**b**) analysis of response time under a varying number of rounds, from 1000 to 5000.

Figure 8 illustrates the performance of the proposed architecture in the comparison of resource consumption under varying data rates and number of rounds. Based on the results, it was observed that it decreased the consumption by an average of 14% and 17%, unlike the existing solutions. This was due to most of the computing operations being done in high resource-oriented gateways and sink nodes. All the secured keys are generated on these high-power nodes, which only the connected nodes use to ensure data security against attacks. Moreover, lightweight XoR operations in data encryption and decryption impose the least storage and processing overheads on the connected end-users IoT devices. Furthermore, the integration of storage centers provides a robust solution for storing big data and decreases the communication overhead.



(**a**)

(**b**)

Figure 8. Scenarios of (**a**) analysis of resource consumption under a varying data rate of 30 to 150 bits/s, and (**b**) analysis of resource consumption under a varying number of rounds, from 1000 to 5000.

5. Conclusions

This paper proposed a mobility support 5G architecture with real-time routing for sustainable smart cities. Its main factors are highlighted as follows:

i. It supports the delivery of online data with a high level of security and network continuity for mobile networks. Unlike other traditional approaches, it leads to few data delays and decreases the processing cost with the availability of higher bandwidth.
ii. It also secures the 5G ecosystem with a nominal risk rate and supports trustworthy communication. The mobile sink collaborates with both gateway nodes and medical storage centers to gather the IoT data, which explicitly increases the success rate of sensitive data with optimum delay.
iii. In addition, instead of only securing the boundary points for data routing, the proposed architecture performs risk analysis for the IoT nodes and links. The proposed architecture was tested and evaluated against existing work in terms of various experiments and it was seen to have significantly better performance. The multi-level security secures the routing for next-generation networks without imposing additional resource usage.

However, it was observed that the proposed architecture still lacks intelligence in distributing the IoT data on established routes and leads to communication complexity when network nodes increase. Therefore, we aim to introduce some machine learning schemes to train the proposed architecture with nominal latency and support emergency communications.

Author Contributions: Conceptualization, A.R. and K.H.; methodology, A.R.; software, A.R.; validation, A.R., K.H. and J.L.; formal analysis, J.L.; investigation, T.S.; resources, T.S.; data curation, Z.A.; writing—original draft preparation, A.R.; writing—review and editing, T.S.; visualization, J.L.; supervision, J.L.; project administration, A.R.; funding acquisition, A.R. All authors have read and agreed to the published version of the manuscript.

Funding: There is no funding for this research.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: All data is available in the manuscript.

Acknowledgments: This research is technically supported by Artificial Intelligence & Data Analytics Lab (AIDA) CCIS Prince Sultan University, Riyadh, Saudi Arabia. Authors are thankful for technical support.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Wang, D.; Chen, D.; Song, B.; Guizani, N.; Yu, X.; Du, X. From IoT to 5G I-IoT: The Next Generation IoT-Based Intelligent Algorithms and 5G Technologies. *IEEE Commun. Mag.* **2018**, *56*, 114–120. [CrossRef]
2. Haseeb, K.; Islam, N.; Saba, T.; Rehman, A.; Mehmood, Z. LSDAR: A light-weight structure based data aggregation routing protocol with secure internet of things integrated next-generation sensor networks. *Sustain. Cities Soc.* **2019**, *54*, 101995. [CrossRef]
3. Lloret, J.; Parra, L.; Taha, M.; Tomás, J. An architecture and protocol for smart continuous eHealth monitoring using 5G. *Comput. Netw.* **2017**, *129*, 340–351. [CrossRef]
4. Mohanta, B.K.; Jena, D.; Satapathy, U.; Patnaik, S. Survey on IoT security: Challenges and solution using machine learning, artificial intelligence and blockchain technology. *Internet Things* **2020**, *11*, 100227. [CrossRef]
5. Singh, S.; Sharma, P.K.; Yoon, B.; Shojafar, M.; Cho, G.H.; Ra, I.-H. Convergence of blockchain and artificial intelligence in IoT network for the sustainable smart city. *Sustain. Cities Soc.* **2020**, *63*, 102364. [CrossRef]
6. Saba, T.; Haseeb, K.; Ahmed, I.; Rehman, A. Secure and energy-efficient framework using Internet of Medical Things for e-healthcare. *J. Infect. Public Health* **2020**, *13*, 1567–1575. [CrossRef]
7. González-Landero, F.; García-Magariño, I.; Lacuesta, R.; Lloret, J. PriorityNet App: A mobile application for establishing priorities in the context of 5G ultra-dense networks. *IEEE Access* **2018**, *6*, 14141–14150. [CrossRef]

8. Sharma, T.; Chehri, A.; Fortier, P. Review of optical and wireless backhaul networks and emerging trends of next generation 5G and 6G technologies. *Trans. Emerg. Telecommun. Technol.* **2020**, *32*, e4155. [CrossRef]
9. Haseeb, K.; Almogren, A.; Din, I.U.; Islam, N.; Altameem, A. SASC: Secure and Authentication-Based Sensor Cloud Architecture for Intelligent Internet of Things. *Sensors* **2020**, *20*, 2468. [CrossRef]
10. Taha, M.; Parra, L.; Garcia, L.; Lloret, J. An Intelligent handover process algorithm in 5G networks: The use case of mobile cameras for environmental surveillance. In Proceedings of the 2017 IEEE International Conference on Communications Workshops (ICC Workshops), Paris, France, 21–25 May 2017.
11. Gubbi, J.; Buyya, R.; Marusic, S.; Palaniswami, M.S. Internet of Things (IoT): A vision, architectural elements, and future directions. *Futur. Gener. Comput. Syst.* **2013**, *29*, 1645–1660. [CrossRef]
12. Elrawy, M.F.; Awad, A.I.; Hamed, H.F. Intrusion detection systems for IoT-based smart environments: A survey. *J. Cloud Comput.* **2018**, *7*, 1–20. [CrossRef]
13. Rehman, A.; Haseeb, K.; Saba, T.; Lloret, J.; Tariq, U. Secured Big Data Analytics for Decision-Oriented Medical System Using Internet of Things. *Electronics* **2021**, *10*, 1273. [CrossRef]
14. Kotenko, I.; Saenko, I.; Branitskiy, A. Framework for Mobile Internet of Things Security Monitoring Based on Big Data Processing and Machine Learning. *IEEE Access* **2018**, *6*, 72714–72723. [CrossRef]
15. Ren, J.; Guo, H.; Xu, C.; Zhang, Y. Serving at the Edge: A Scalable IoT Architecture Based on Transparent Computing. *IEEE Netw.* **2017**, *31*, 96–105. [CrossRef]
16. Yelamarthi, K.; Aman, S.; AbdelGawad, A. An Application-Driven Modular IoT Architecture. *Wirel. Commun. Mob. Comput.* **2017**, *2017*, 1–16. [CrossRef]
17. Sagirlar, G.; Carminati, B.; Ferrari, E. Decentralizing privacy enforcement for Internet of Things smart objects. *Comput. Netw.* **2018**, *143*, 112–125. [CrossRef]
18. Lv, P.; Wang, L.; Zhu, H.; Deng, W.; Gu, L. An IOT-Oriented Privacy-Preserving Publish/Subscribe Model Over Blockchains. *IEEE Access* **2019**, *7*, 41309–41314. [CrossRef]
19. Saba, T.; Haseeb, K.; Shah, A.A.; Rehman, A.; Tariq, U.; Mehmood, Z. A Machine-Learning-Based Approach for Autonomous IoT Security. *IT Prof.* **2021**, *23*, 69–75. [CrossRef]
20. Hossain, E.; Khan, I.; Un-Noor, F.; Sikander, S.S.; Sunny, S.H. Application of Big Data and Machine Learning in Smart Grid, and Associated Security Concerns: A Review. *IEEE Access* **2019**, *7*, 13960–13988. [CrossRef]
21. Liu, Z.; Seo, H. IoT-NUMS: Evaluating NUMS Elliptic Curve Cryptography for IoT Platforms. *IEEE Trans. Inf. Forensics Secur.* **2018**, *14*, 720–729. [CrossRef]
22. Mohanta, B.K.; Sahoo, A.; Patel, S.; Panda, S.S.; Jena, D.; Gountia, D. Decauth: Decentralized authentication scheme for iot device using ethereum blockchain. In Proceedings of the TENCON 2019-2019 IEEE Region 10 Conference (TENCON), Kochi, India, 17–20 October 2019.
23. Chaabouni, N.; Mosbah, M.; Zemmari, A.; Sauvignac, C.; Faruki, P. Network Intrusion Detection for IoT Security Based on Learning Techniques. *IEEE Commun. Surv. Tutorials* **2019**, *21*, 2671–2701. [CrossRef]
24. Ali, G.; Ahmad, N.; Cao, Y.; Asif, S.; Cruickshank, H.; Ali, Q.E. Blockchain based permission delegation and access control in Internet of Things (BACI). *Comput. Secur.* **2019**, *86*, 318–334. [CrossRef]
25. Qiu, J.; Tian, Z.; Du, C.; Zuo, Q.; Su, S.; Fang, B. A Survey on Access Control in the Age of Internet of Things. *IEEE Internet Things J.* **2020**, *7*, 4682–4696. [CrossRef]
26. Dorri, A.; Kanhere, S.S.; Jurdak, R.; Gauravaram, P. LSB: A Lightweight Scalable Blockchain for IoT security and anonymity. *J. Parallel Distrib. Comput.* **2019**, *134*, 180–197. [CrossRef]
27. Rehman, A.; Haseeb, K.; Saba, T.; Kolivand, H. M-SMDM: A model of security measures using Green Internet of Things with Cloud Integrated Data Management for Smart Cities. *Environ. Technol. Innov.* **2021**, *24*, 101802. [CrossRef]
28. Arellanes, D.; Lau, K.-K. Evaluating IoT service composition mechanisms for the scalability of IoT systems. *Futur. Gener. Comput. Syst.* **2020**, *108*, 827–848. [CrossRef]
29. Si, H.; Sun, C.; Li, Y.; Qiao, H.; Shi, L. IoT information sharing security mechanism based on blockchain technology. *Futur. Gener. Comput. Syst.* **2019**, *101*, 1028–1040. [CrossRef]
30. Li, Z.; Liu, L.; Barenji, A.V.; Wang, W. Cloud-based Manufacturing Blockchain: Secure Knowledge Sharing for Injection Mould Redesign. *Procedia CIRP* **2018**, *72*, 961–966. [CrossRef]
31. Gope, P.; Gheraibia, Y.; Kabir, S.; Sikdar, B. A secure IoT-based modern healthcare system with fault-tolerant decision making process. *IEEE J. Biomed. Health Inform.* **2020**, *25*, 862–873. [CrossRef]
32. Danzi, P.; Kalor, A.E.; Stefanovic, C.; Popovski, P. Delay and Communication Tradeoffs for Blockchain Systems With Lightweight IoT Clients. *IEEE Internet Things J.* **2019**, *6*, 2354–2365. [CrossRef]
33. Wang, N.; Jiang, T.; Lv, S.; Xiao, L. Physical-Layer Authentication Based on Extreme Learning Machine. *IEEE Commun. Lett.* **2017**, *21*, 1557–1560. [CrossRef]
34. Xu, X.; Liu, X.; Xu, Z.; Dai, F.; Zhang, X.; Qi, L. Trust-Oriented IoT Service Placement for Smart Cities in Edge Computing. *IEEE Internet Things J.* **2019**, *7*, 4084–4091. [CrossRef]
35. Dedeoglu, V.; Jurdak, R.; Dorri, A.; Lunardi, R.; Michelin, R.; Zorzo, A.; Kanhere, S. Blockchain Technologies for iot. In *Advanced Applications of Blockchain Technology*; Lee, S.-W., Singh, I., Mohammadian, M., Eds.; Springer: Berlin/Heidelberg, Germany, 2020; pp. 55–89.

36. Sadowski, S.; Spachos, P. Wireless technologies for smart agricultural monitoring using internet of things devices with energy harvesting capabilities. *Comput. Electron. Agric.* **2020**, *172*, 105338. [CrossRef]
37. Wang, N.; Wang, P.; Alipour-Fanid, A.; Jiao, L.; Zeng, K. Physical-Layer Security of 5G Wireless Networks for IoT: Challenges and Opportunities. *IEEE Internet Things J.* **2019**, *6*, 8169–8181. [CrossRef]
38. Xu, L.; Yu, X.; Gulliver, T.A. Intelligent Outage Probability Prediction for Mobile IoT Networks Based on an IGWO-Elman Neural Network. *IEEE Trans. Veh. Technol.* **2021**, *70*, 1365–1375. [CrossRef]
39. Cicioğlu, M.; Çalhan, A. IoT-based wireless body area networks for disaster cases. *Int. J. Commun. Syst.* **2018**, *33*, e3864. [CrossRef]
40. Pratap, A.; Gupta, R.; Nadendla, V.S.S.; Das, S.K. Bandwidth-constrained task throughput maximization in IoT-enabled 5G networks. *Pervasive Mob. Comput.* **2020**, *69*, 101281. [CrossRef]
41. Sarker, I.H. A machine learning based robust prediction model for real-life mobile phone data. *Internet Things* **2019**, *5*, 180–193. [CrossRef]
42. Zolanvari, M.; Teixeira, M.A.; Gupta, L.; Khan, K.M.; Jain, R. Machine Learning-Based Network Vulnerability Analysis of Industrial Internet of Things. *IEEE Internet Things J.* **2019**, *6*, 6822–6834. [CrossRef]
43. Kumar, N.M.; Mallick, P.K. Blockchain technology for security issues and challenges in IoT. *Procedia Comput. Sci.* **2018**, *132*, 1815–1823. [CrossRef]
44. Sadique, K.M.; Rahmani, R.; Johannesson, P. Towards Security on Internet of Things: Applications and Challenges in Technology. *Procedia Comput. Sci.* **2018**, *141*, 199–206. [CrossRef]
45. Dorri, A.; Roulin, C.; Jurdak, R.; Kanhere, S.S. On the activity privacy of blockchain for IoT. In Proceedings of the 2019 IEEE 44th Conference on Local Computer Networks (LCN), Osnabrück, Germany, 14–17 October 2019.
46. Putra, G.D.; Dedeoglu, V.; Kanhere, S.S.; Jurdak, R. Trust management in decentralized IoT access control system. In Proceedings of the 2020 IEEE International Conference on Blockchain and Cryptocurrency (ICBC), Toronto, ON, Canada, 2–6 May 2020.
47. Dorri, A.; Luo, F.; Kanhere, S.S.; Jurdak, R.; Dong, Z.Y. SPB: A secure private blockchain-based solution for distributed energy trading. *IEEE Commun. Mag.* **2019**, *57*, 120–126. [CrossRef]
48. Malik, S.; Dedeoglu, V.; Kanhere, S.S.; Jurdak, R. Trustchain: Trust management in blockchain and iot supported supply chains. In Proceedings of the 2019 IEEE International Conference on Blockchain (Blockchain), Seoul, Korea, 14–17 July 2019.
49. Zhao, Y.; Liu, Y.; Tian, A.; Yu, Y.; Du, X. Blockchain based privacy-preserving software updates with proof-of-delivery for Internet of Things. *J. Parallel Distrib. Comput.* **2019**, *132*, 141–149. [CrossRef]
50. Yu, F.; Chen, M.; Yu, B.; Li, W.; Ma, L.; Gao, H. Privacy preservation based on clustering perturbation algorithm for social network. *Multimedia Tools Appl.* **2017**, *77*, 11241–11258. [CrossRef]
51. Guo, X.; Lin, H.; Li, Z.; Peng, M. Deep-reinforcement-learning-based QoS-aware secure routing for SDN-IoT. *IEEE Internet Things J.* **2019**, *7*, 6242–6251. [CrossRef]
52. Zhang, Y.; Chen, G.; Du, H.; Yuan, X.; Kadoch, M.; Cheriet, M. Real-time remote health monitoring system driven by 5G MEC-IoT. *Electronics* **2020**, *9*, 1753. [CrossRef]
53. Kaufman, L.; Rousseeuw, P.J. Clustering by Means of Medoids. Available online: https://www.researchgate.net/publication/243777819_Clustering_by_Means_of_Medoids (accessed on 9 August 2021).
54. Rabin, M.O. *Digitalized Signatures and Public-Key Functions as Intractable as Factorization*; Massachusetts Inst of Tech Cambridge Lab for Computer Science: Cambridge, MA, USA, 1979.
55. Ripley, B.D. Thoughts on pseudorandom number generators. *J. Comput. Appl. Math.* **1990**, *31*, 153–163. [CrossRef]
56. Zarrad, A.; Alsmadi, I. Evaluating network test scenarios for network simulators systems. *Int. J. Distrib. Sens. Netw.* **2017**, *13*. [CrossRef]
57. Shakeel, P.M.; Baskar, S.; Dhulipala, V.R.S.; Mishra, S.; Jaber, M.M. Maintaining Security and Privacy in Health Care System Using Learning Based Deep-Q-Networks. *J. Med Syst.* **2018**, *42*, 1–10.