sustainability

MDPI

Article

Secure and Sustainable Predictive Framework for IoT-Based Multimedia Services Using Machine Learning

Naveed Islam [1], Majid Altamimi [2,*], Khalid Haseeb [1] and Mohammad Siraj [2]

[1] Department of Computer Science, Islamia College Peshawar, Peshawar 25000, Pakistan; naveed.islam@icp.edu.pk (N.I.); khalid.haseeb@icp.edu.pk (K.H.)

[2] Electrical Engineering Department, College of Engineering, King Saud University, Riyadh 11421, Saudi Arabia; siraj@ksu.edu.sa

* Correspondence: mtamimi@ksu.edu.sa

Abstract: In modern years, the Internet of Things (IoT) has gained tremendous growth and development in various sectors because of its scalability, self-configuring, and heterogeneous factors. It performs a vital role in improving multimedia communication and reducing production costs. The multimedia data consist of various types and formats (text, audio, videos, etc.), which are forwarded in the form of blocks of bits in the network layer of TCP/IP. Due to limited resources available to IoT-built devices, most of the Multimedia Internet of Things (MIoT)-based applications are delay constraints, especially for big data content. Similarly, multimedia-based applications are more vulnerable to security burdens and lower the trust of data processing. In this paper, we present a secure and sustainable prediction framework for MIoT data transmission using machine learning, which aims to offer intelligent behavior of the system with information protection. Firstly, the network edges exploit a regression analysis for a real-time multimedia routing scheme and achieve precise delivery towards the media servers. Secondly, an efficient and low-processing asymmetric process is proposed to provide secure data transmission between the IoT devices, edges, and data servers. Extensive experiments are performed over the OMNET++ network simulator, and its significance is achieved by an average for energy consumption by 71%, throughput by 30.5%, latency by 22%, bandwidth by 34.5%, packets overheads by 38.5%, computation time by 12.5%, and packet drop ratio by 35% in the comparison of existing schemes.

Keywords: sustainable network; big data; edge nodes; machine learning; Internet of Things

check for updates

Citation: Islam, N.; Altamimi, M.; Haseeb, K.; Siraj, M. Secure and Sustainable Predictive Framework for IoT-Based Multimedia Services Using Machine Learning. *Sustainability* **2021**, *13*, 13128. https://doi.org/10.3390/su132313128

Academic Editor: Elvira Nica

Received: 16 October 2021
Accepted: 24 November 2021
Published: 26 November 2021

Publisher's Note: MDPI stays neutral with regard to jurisdictional claims in published maps and institutional affiliations.

Copyright: © 2021 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (https://creativecommons.org/licenses/by/4.0/).

1. Introduction

A multimedia network is defined as a distributed system, and application users can exchange traffic, such as audio, video, and images, to remote users by using communication tools. In the case of the wireless sensor network (WSN), the IoT devices can be deployed in dynamic environments and extracting local intended information. The dynamic environment not only changes the states of nodes but also reflects the performance of communication on different events. Machine learning and IoT are combined in different network solutions [1,2]. The gathered information is transmitted to the sink node, and remote machines obtained the needed data either periodically or continuously. In large communication ecosystems, a large number of IoT devices and wireless nodes are exchanging real-time data that deplete high energy consumption and impose additional management costs. The intelligent and dynamic decisions of machine learning algorithms collaborate with IoT devices and generate train models that minimize the processing overheads on wireless systems [3–5]. With the beginning of IoT devices and multimedia services for real-time and robust applications, a lot of heterogeneous services are collaborating in a distributed manner. Such systems offer numerous functions for the sharing and exchanging of graphics data over the Internet. Moreover, IoT devices need to intelligently devise a mechanism for autonomous configuration concerning the network topology [6–8]. Due to the diverse applications of IoT devices, the data extracted from these devices come from different sources with different formats. Therefore, one of the significant tasks for IoT-based systems is to generate algorithms that can assist various characteristics of data for constraint networks [9,10]. Besides this, IoT-based multimedia system also brings many other problems that need to be addressed, such as improving the quality of service and offering consistent data with maximum data delivery performance. Such a system is the collection of network protocols, services, and media-related data that need to be processed in a precise and efficient manner. The multimedia information moves from device to device, along with various limitations, such as bandwidth usage, timely delivery, and quality management, especially for critical IoT architectures. Machine learning techniques for IoT-based multimedia communication depend on various factors involving the data types, data models, and efficient algorithms, which can be used to perform various tasks, such as data processing, segmentation, classification, etc., for analysis and generation of useful information. However, the development for multimedia applications still incurs many issues, such as energy efficiency, quality of service (QoS), bandwidth, data analysis, optimization, cloud communication, etc. [11–13]. Moreover, significant patterns and features from the data of sensors must be extracted and interpreted. Besides other functional objectives, such as an efficient selection of forwarder nodes for multi-hop that need to be achieved, one of the operational objectives in applying machine learning techniques over the MIoT devices is to satisfy the intrinsic constraints, i.e., low energy, low memory, and limited computation power [14,15].

Due to the distributed and dynamic infrastructure of IoT-based multimedia traffic, most of the wireless nodes and IoT devices are mobile; thus, such a communication paradigm intends to be compromised against anonymous attacks. It has been seen that many approaches are proposed for dealing with security and achieving trust among connected objects. However, most of the solutions are not able to reduce the additional usage of resources on communicating nodes, while delivering the high-content multimedia data over the constraint nodes. If the security of any device is compromised, then the integrity of the whole network concedes, which may lead to unauthorized access, data breaches, revelation or exposer of confidential data and identities, or a total suspension of the communication service. Therefore, improving the security with manageable overheads is also an important factor [16–19].

This research work presents a quality assurance framework to handle the multimedia traffic in IoT systems and guaranteed the robust performance of the system under a constrained environment. Moreover, the network resources are collaborated efficiently, using the network edges and intelligently utilizing the selection forwarding process for multimedia data by using machine learning techniques. It balances the data traffic optimally on the IoT network and increases the stability of the media system. Moreover, with the incorporation of security methods, the proposed framework maintains trust and confidentiality between multimedia data and IoT networks. Figure 1 depicts the working flow of the components in the proposed framework.

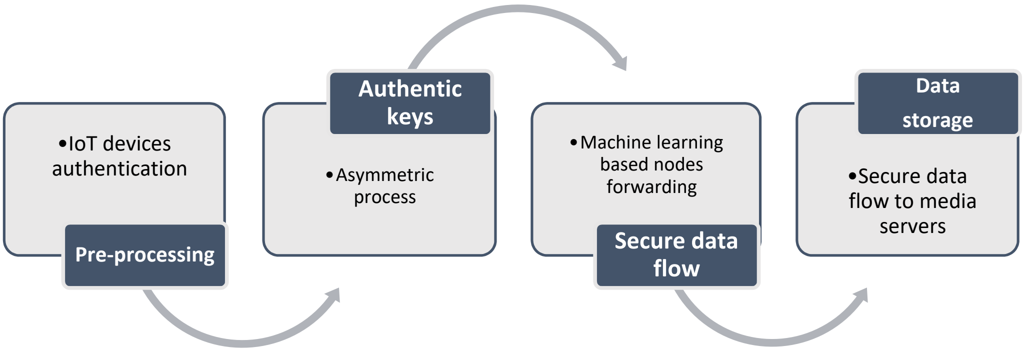

•IoT devices authentication
Pre-processing
Authentic keys
•Asymmetric process
•Machine learning based nodes forwarding
Secure data flow
Data storage
•Secure data flow to media servers

Figure 1. Components of the proposed framework.

In brief, the main contributions of the proposed framework are as follows:

i. A mutual collaborative process is established between the MIoT devices through the verification of identities for multimedia data traffic.
ii. To reduce the latency with the increase in data transfer rate, regression analysis, a machine learning-based predictive technique, is exploited, as it intelligently and efficiently selects the forwarder node.
iii. For the security and protection of multimedia data in MIoT against potential threats, an efficient and low-processing cryptosystem is proposed to increase the reliability among edge computing nodes and the media data servers.
iv. A series of simulation-based experiments are performed to validate the proposed framework that significantly improves the performance of MIoT on the scale of a larger network.

The research work is structured as follows. The literature work is discussed in Section 2. Section 3 explains the proposed model with its developed components. In Section 4, the network model and performance analysis are presented. In the end, Section 5 presents the conclusion.

2. Related Work

In smart cities, the wireless nodes are mainly used for collecting the observing data and further transmitting them to end-users to fulfill their demand [20–23]. In recent decades, machine learning approaches have been widely utilized by the media communication system to connect the physical world and share the required information among IoT devices. However, the research community is still focusing on the support of intelligence in forwarding the IoT data on reliable forwarders with energy efficiency and load balancing [24–26]. On the other hand, edge computing enables the computation of network information directly at the edges nodes and performs the functionality of task offloading [27–29]. In the multimedia network, the IoT devices are connected by using wireless technologies that sense the media traffic and are forwarded toward the sink node. The application users, such as in the smart home, smart agriculture, surety surveillance system, etc., are directly connected with the Internet and retrieve the required information for processing [30–32]. However, most of the solutions are prone to failure in the case of dynamic and realistic network topologies. Multimedia-based routing with optimized performance without disrupting the network users and decreasing latency time is a significant research challenge. Furthermore, securing multimedia data and maintaining its privacy against malicious attacks are also considered important factors. Reference [33] proposed a framework for a cloud-based lightweight cancelable biometric authentication system. It aims to offer reliable solutions for the deployment in the real world and authenticate the objects with nominal communication overhead. The analysis of both theoretical and experimental results demonstrates the significance of the proposed framework with a nominal error rate than other state-of-the-art techniques. Moreover, it has proven to offer less response time and is more suitable for smart environments. In Reference [34], the authors proposed a novel energy-efficient two-stage routing protocol (EETSP) for decreasing energy consumption and increasing network stability. By using the proposed approach, the delivery ratio is improved, and the energy utilization of primary and secondary cluster heads is also reduced. It comprises two stages: that is, the selection of primary and secondary cluster heads is performed in the first phase, while intercluster routing is achieved in the second phase. The obtained results have proven significant improvements, as compared to other solutions. Reference [35] presented a blockchain-based framework for provisioning a privacy-preserving and verifiable query facility to the end-users in the industrial Internet of Things. The proposed solution utilizes the technology of blockchain for storing the network data in the form of on-chain and on the other side, the cloud systems are used to store extensive data as off-chain data. The system extracts the needed data from on-chain and off-chain and generated the aggregated result. Moreover, the query verification model verifies the obtained result before its utilization and increases the security methods. The experiments illustrate the improved efficiency and scalability of the proposed framework. In, the author utilizes the mobile edge server, and the available resources in the proximity of the mobile edge server are effectively used for collaborative computing. It increases the better management of resources for nodes and also improves the computing performance of the system. Moreover, the technique of machine learning is exploited for the distributed task scheduling and stabilizes the distribution among devices. In the end, based on the experiments, the entire system is tested and verified to significantly increase the communication paradigm, as compared to the existing solution. In Reference [36], the authors proposed a lightweight cipher algorithm, using a dynamic structure with a single round. It comprises simple operations and aims to support multimedia IoT. The proposed algorithm generates a dynamic key and produces two robust substitution tables, a dynamic permutation table, and two pseudo-random matrices. It achieves a high level of randomness by minimizing the number of rounds to a single one and increasing the security level. Extensive experiments are performed to evaluate its efficacy and robustness in the presence of network threats. Recently, many solutions are focused on media security, using sensors networks and integrated with IoT devices to support the community. Reference [37] presented the discussion for the issues and architecture of communication in IoT networks. Moreover, they analyze the significant research challenges for data security and privacy in the environment of constraint networks. An Efficient Algorithm for a Media-based Surveillance System (EAMSuS) for IoT network for Smart City Framework is proposed. It combines the two algorithms introduced by other researchers for improving the packet routing and security of WSN. They reclaim the new media compression standard, High Efficiency Video Coding (HEVC), in the proposed algorithm. The performed experiments and their analysis illustrate efficacy of proposed algorithm for various network metrics.

It is seen from the related work that wireless sensor networks and multimedia IoT are utilized in different approaches to support the communication system. However, due to the requirement of high bandwidth and processing power, it is still an open research challenge for the effective management of network structure and computing resources. It is also observed that most of the existing solution adopts traditional fundamentals to increase the performance of the media transmission system. Although such systems facilitating the network tasks lead to various security attacks and overloaded IoT devices in terms of additional processing costs. Some solutions are developed by using machine learning techniques to overcome the additional overheads on the IoT network; however, they do not consider the security system [38–40]. Though, some solutions secure the media-based surveillance systems but incur extra energy resources for connected constraint nodes. Therefore, in the recent era, there is a demand for proposing a quality assurance framework to balance the media traffic on the allocating links and also preserve the distributed collaboration of IoT networks from unknown attacks.

3. Proposed Framework

This section describes the proposed model in the following subsections.

3.1. Network Model

The MIoT network is composed of heterogeneous objects, and they are deployed in a two-dimensional system (x, y). The objects aim to collect the multimedia data, such as video, audio, and graphical images, etc.; however, they have numerous constraints in terms of energy, processing, bandwidth, and storage memory. They have a unique identity and are remain fixed. The object senses the MIoT environment periodically and transmits the data toward the sink node, using multi-hop. Later, the sink node collaborates with media servers over the Internet to store the data. We consider the sink node as more powerful without resource limitations. The data are transmitted over the asymmetric communication links that are unreliable in the presence of faulty nodes. The faulty nodes generate and flood the false route request packets; thus, links are congested when objects are increasing.

Few wireless access points are installed on the edges to communicate with the sink node. Some network assumptions are given as follows:

i. All the edge nodes are mobile.
ii. Wireless channels are asymmetric with varying bandwidths.
iii. The objects have a limited transmission radius.
iv. Not all objects can communicate directly with the sink node.
v. No new nodes are allowed to enter the network after its deployment.

3.2. Sustainable IoT-Based Multimedia Services

In this section, the proposed model is discussed, along with its operations phases, which are based on the two algorithms. We consider various MIoT-based-sensors that can interchange the multimedia data and transmit the observed information to the sink node by using intelligent edges. By considering the limited constraints of MIoT sensors, the proposed model focused on presenting the least cost and more secure communication system to transmit multimedia data. The edge nodes have more abilities for data processing and taking an intelligent decision to forward the data toward media servers for storage. The stored data on media servers can be transferred to the smart devices of the end-users through the Internet. The MIoT devices are verified through the authentication phase to be synchronized with compatible devices, which are later marked as valid entities for the data routing table.

In the beginning, the sink node advertises the identities, IDs, of edge nodes N_i in the network. On receiving, all the MIoT nodes store the IDs of the edge nodes in their local table. The proposed model utilizes a knapsack cryptosystem [41], which is an asymmetric algorithm and ensuring data security with lightweight computing resources. The choice of knapsack cryptosystem is based on the fact that it is lightweight and efficient for MIoT devices, as compared to other asymmetric cryptosystems, such as Rivest–Shamir–Adleman (RSA) [42], which are not only computationally expensive but also require more storage. In the Merkel–Hellman Knapsack cryptosystem, the security of the generated keys is based on the concept of the NP-Complete problem, which requires nondeterministic polynomial time for the attacker. The knapsack algorithm is executed by the edge nodes, initially, it chooses a random superincreasing sequence of n positive integers, i.e., $X = x_1, x_2, \ldots,\ x_n$. The generation of superincreasing sequence x_k is denoted by Equation (1).

$$x_k > \sum_{i=0}^{k-1} x_i\ ,\ 1 < k \leq n \tag{1}$$

Two random numbers, n and m, are selected and multiplied the values of x_i by the number n and then determine the modulo m, as given by Equation (2).

$$P = n.x_i \ mod\ m \tag{2}$$

In the equation, P is the public key of the edge node, while its private key is denoted by (X, n, m).

After the generation of pair of public-private keys, the edge nodes flood their public keys, P_i, among other network devices and keep their private keys, R_i, secret. To communicate with a particular node, the edge node performs an exclusive-OR (XoR) operation over its unique ID_i and public key P_i as given in Equation (3).

$$Y = ID_i \oplus P_i \tag{3}$$

The computed Y is transmitted toward the receiving node, which, for the sack of authentication, performs the exclusive-OR operation on Y and P_i to obtain the unique ID_i of the edge node. After the initialization phase, the proposed model adjusts the data flow among MIoT nodes, using some intelligent computation. Due to the availability of enormous resources to the edge nodes, the flooding of the public key is performed by them, whereas, due to limited resources available to the ordinary nodes, they only perform the authentication of the edge nodes.

In the proposed framework, the MIoT nodes collect the multimedia data and transmit them toward the forwarder node, which is selected based on the machine learning technique of regression analysis.

The use of regression analysis is justified by the fact that the selection of forwarder nodes depends on the time of transmission, the packet sent, and the reception of the packet by receiving node. In this process, the regression analysis is aimed to determine the effects of independent variables over the dependent variable. Considering the data loss rate of each node in the transmission process as a dependent variable and transmitted data, along with its time instant as independent variables, any node wi can transmit data packets pi at time t_i toward neighboring node w_j with loss rate l_i. The records for each node are stored during the transmission and reception of data to carry out the regression analysis, using Equation (4).

$$l_i = \beta_0 + \beta_1 p_i + \beta_2 t_i + \epsilon \tag{4}$$

where l_i represents the data loss rate; β_0 is the y-intercept; $\beta_1 p_i$ is the first regression coefficient, along with the transmitted data packet; $\beta_2 t_i$ is the 2nd regression coefficient, with the time instant, t_i, variable, and ϵ is the residual error. The objective is to find the lowest data loss rate, l_i, for each node, so that the transmitting node can hop the data toward the sink nodes.

The coefficients (β_1 and β_2) are calculated by using Equations (5) and (6).

$$\beta_1 = \frac{\left(\sum t_i^2\right)\left(\sum p_i l_i\right) - \left(\sum p_i t_i\right)\left(\sum t_i l_i\right)}{\left(\sum p_i^2\right)\left(\sum t_i^2\right) - \left(\sum p_i t_i\right)^2} \tag{5}$$

and

$$\beta_2 = \frac{\left(\sum t_i^2\right)\left(\sum t_i l_i\right) - \left(\sum p_i t_i\right)\left(\sum p_i l_i\right)}{\left(\sum p_i^2\right)\left(\sum t_i^2\right) - \left(\sum p_i t_i\right)^2} \tag{6}$$

Similarly, the values' y-intercept, β_0, can be calculated by putting the values of β_1 and β_2 in Equation (7).

$$\beta_0 = l_i - \beta_1 \overline{p_1} - \beta_2 \overline{t_2} \tag{7}$$

The neighboring node with the lowest packet data loss, i.e., min (l_i), is selected as a forwarder by the data sending node for further transmission toward the sink node.

In the next phase, the proposed model transmits the collected data toward the sink node, using the chain of edge nodes. The deployed edge nodes perform the encryption function, using the knapsack algorithm to generate ciphertext C, as given in Equation (8).

$$C = \sum_{i=1}^{n} d_i . P_i \tag{8}$$

where d_i denotes the collected data of size n, and P_i is the public key, as derived by using Equation (2). The sink node receives the integrated ciphertext C and performed decryption D' function, as given in Equation (9).

$$D' = n.\, n^{-1}\ mod\ m \tag{9}$$

Upon receiving the recover data, the sink node considered each datum as a separate block, B_i , and forward toward the cloud platform, which comprises various media servers. During forwarding, it encrypts the individual data block with the computed public key, P_i, of the media server based on XoR. Moreover, each block is digitally signed by sink node private key, R_i, and generates a unique MAC for each block. Afterward, data blocks are added in the singular grouping in a blockchain hashing, which provides data integrity and privacy in each iteration. The encrypted data transmission from sink node to media server is given in Equation (10).

$$B_i{}' = MAC_n(R_n, MAC_{n-i}) \tag{10}$$

where $MAC_n = MAC\ (R_{n-i},MAC_{(n-i)-1})$ and $MAC_0 = MAC\ (R_0,E[B_0, P_0])$.

On the other hand, the encrypted blocks, $B_i{}'$, at media servers, first decrypted by using the public key of sink node for verifying their authenticity, and later recover the original data by using the private key of the media server. Figure 1 depicts the components of the proposed framework. Initially, IoT devices perform authentication processes for verification and distributing authentic keys by using asymmetric cryptosystem. After being validated, the proposed framework executes the process of data flow for routing and maintaining communication paths efficiently, along with the management of data security. Moreover, the data flows are updated by using the intelligent method of machine learning and imposing minimum overheads. All the components are interrelated with each other to attain a sustainable environment for multimedia applications.

Figure 2 illustrates the block diagram of the proposed framework. It has four main phases. In the beginning, the IoT network is initiated in all the devices and sensors to collaborate and exchange their identities. Once they authenticate and verify their ID, then the IoT network can move to the next stage. The asymmetric algorithm is utilized by the proposed framework for generation and distribution security keys. Moreover, the machine learning technique is exploited by the proposed framework for the selection of forwarders and maintaining consistent routing paths with nominal overheads. Moreover, edge nodes collaborate with IoT networks and sink node to manage the network resources efficiently and decrease the data delay with different applications.

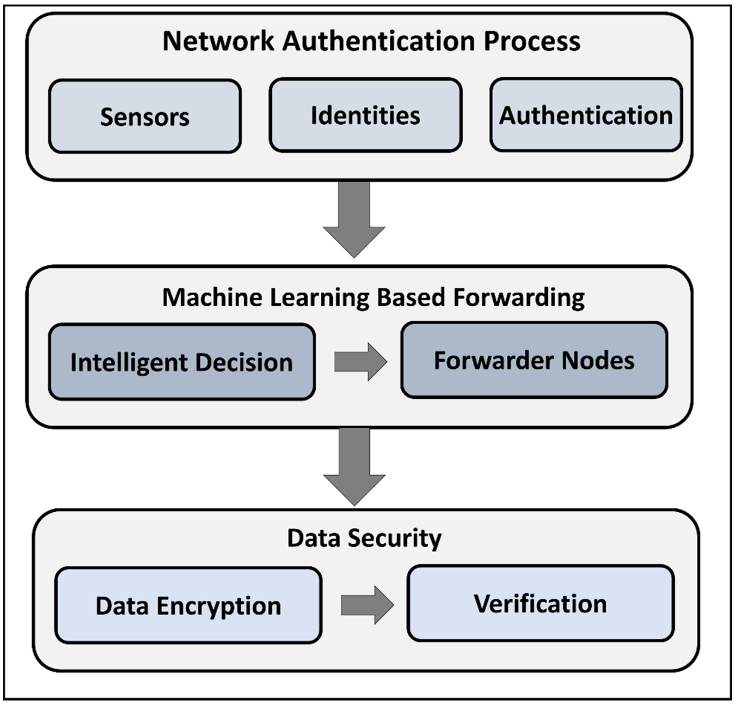
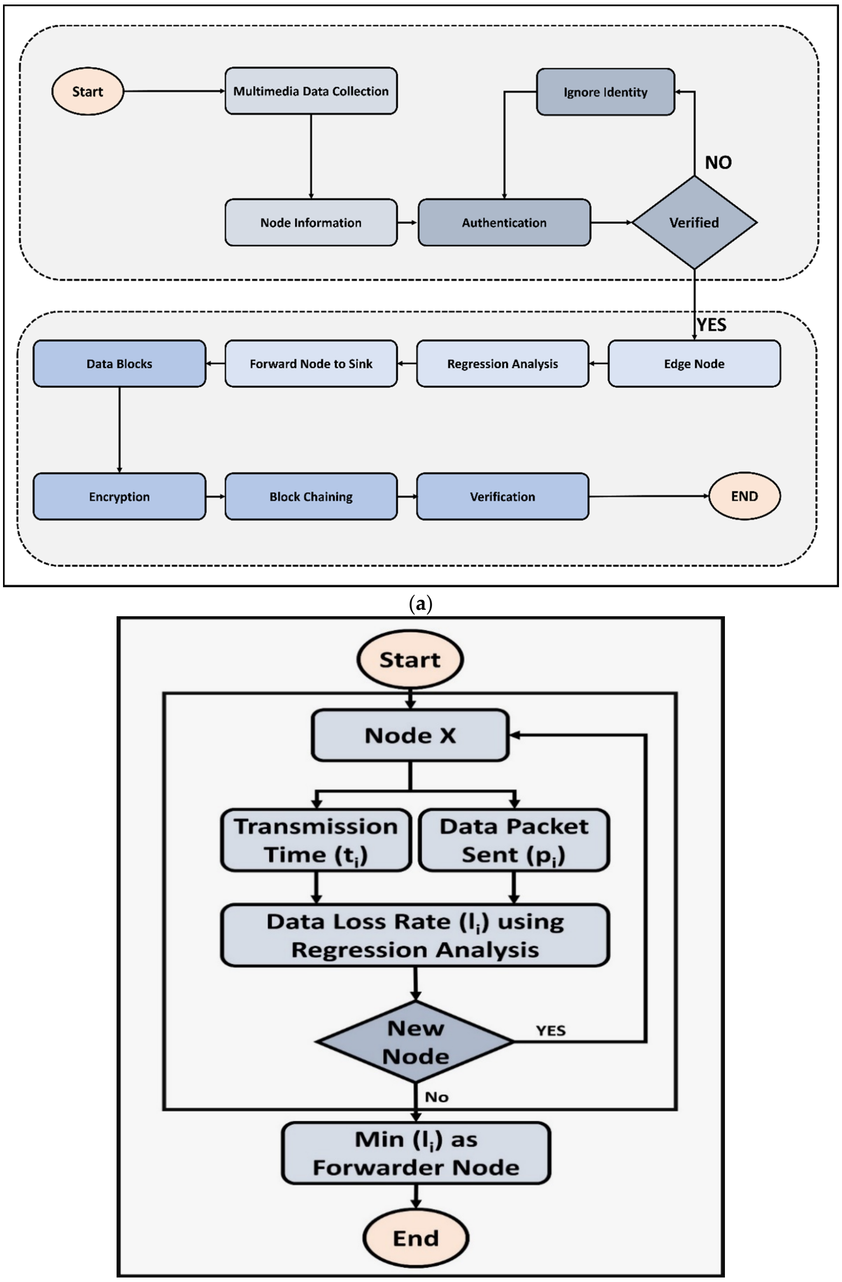


Figure 2. Block diagram of the proposed model.

The graphical representation of the proposed framework is depicted in Figure 3a,b. The media traffic is routed from sensors to sink node and from sink node to cloud systems. The nodes are authenticated on each level until the media data are reached toward network applications. Moreover, machine learning-based regression analysis is performed to select the optimal forwarder for data routing. It leads to low communication and computing overhead on the nodes. The incorporation of edge nodes in the proposed architecture not only decreases the transmission distance with connected IoT devices but also computes the network processing with the utilization of network resources at nominal costs. The forwarders are rotated even within the same due to computing of data lost rate intelligently. Accordingly, among the neighbors, the node with minimum data lost rate is selected as a forwarder based on a regression analysis technique. Moreover, the security level of the proposed framework explicitly increases the trust from the network layer to application users. The application's user retrieves the media data in the form of packets and each datum is encrypted by using lightweight processing power. Accordingly, the proposed framework is reliable in the situation of high media data forwarding even in the presence of malicious attacks in terms of privacy, integrity, and authentication.



(**a**)

(**b**)

Figure 3. Proposed framework for authentication of multimedia traffic, along with machine learning forwarding. (**a**) Process diagram of proposed multimedia devices' information, authentication, and security. (**b**) Process diagram forwarder selection, using machine-learning-based regression analysis.

4. Simulations

In this section, we present the simulation setup and performance evaluation of the proposed framework against existing solutions. The simulations were executed for 3000 s. The experiments are performed in OMNET++ [43,44] and a public-source and open-architecture simulation environment. It is widely used by researchers for simulating the performance of communication networks, dynamic processes, and hardware components. In experiments, IoT devices and sensor nodes are deployed in 300 m^2. The number of sensor nodes is fixed at 400. The transmission range of the nodes is set to 10 m. Some malicious nodes are randomly deployed in the field. The experiments are performed by using realistic scenarios, i.e., varying in data sizes that are expressed in gigabytes (GB). The sink node is immobile and deployed randomly. The edges network comprises 15 edges nodes that are collaborated with the media network and sink node. The performance of the proposed framework is evaluated in terms of energy consumption, network throughput, data latency, bandwidth, packets overheads, and packet drop ratio. The simulation configuration is illustrated in Table 1.

Table 1. Simulation configuration.

Parameters	Values
Simulation area	2-dimensional
Sensor nodes	400
Malicious nodes	15
Initial energy	5 j
Transmission power	10 m
Simulation interval	3000 s
Data flow	Periodic
Edge nodes	15

In Figure 4, the experimental results illustrate that the proposed model improves the energy consumption by 67% and 75% in the comparison of the existing approaches. It is due to that the proposed architecture uses various factors to gather and forward the media data. Moreover, nodes' information is verified and authenticated before initiating the routing from the IoT network to the sink node. In contrast to the EETSP solution that incurs additional energy consumption in the selection of primary and secondary cluster heads, the proposed architecture selects the forwarders by exploiting the intelligent way of machine learning techniques. Due to this reason, the data loss rate significantly decreases the chances of the chosen faulty routes and ultimately reduces the additional usage of network resources. Moreover, the multimedia traffic effectively utilizes the available bandwidth of the system and improves energy efficiency.

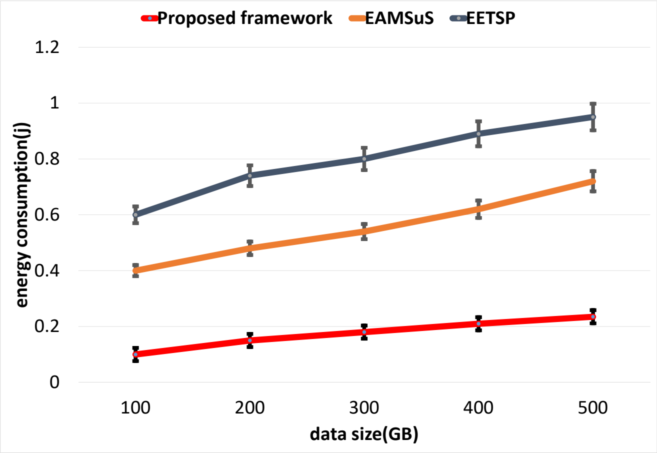


Figure 4. Evaluation of energy consumption with varying data size between proposed framework and existing solutions.

Figure 5 illustrates the performance of the proposed framework for throughput in the comparison of existing solutions. It is seen that, due to the selection of the most reliable forwarders, the proposed architecture increases the network throughput by 27% and 34%; even the data size and congestion increase. It eliminates such links from routing decisions whose error rate is high, as it seems since the malicious nodes or available bandwidth is not enough to carry the media data. In contrast to the EETSP solution, which incurs network overheads without identifying the most reliable inter-cluster routes, the proposed architecture decreases the extra communication overhead on links, using the machine learning technique, and offers the lightweight route request/response process. It not only improves the data delivery rate over the particular link but also strengthens the network stability.

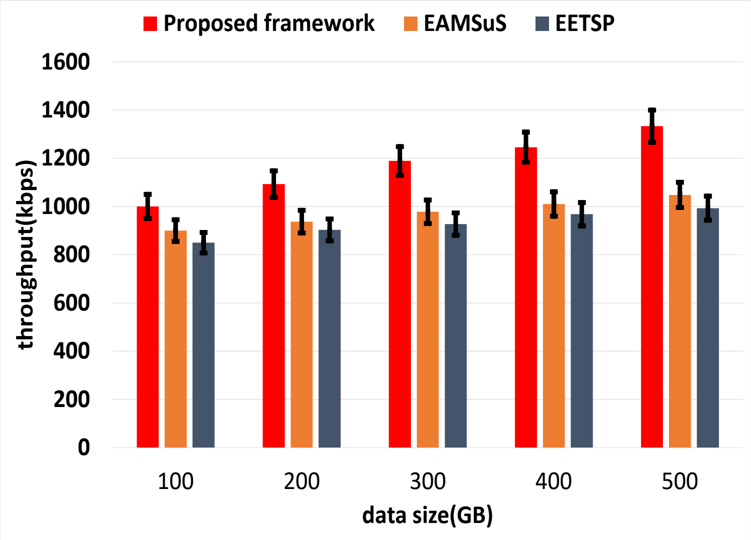


Figure 5. Evaluation of throughput with varying data size between proposed framework and existing solutions.

Figure 6 tested and verified the result of latency of the proposed framework with other solutions. It is observed that the proposed framework decreases the latency in data routing under varying data sizes by 19% and 25%. It is due to the choice multi-hop route toward the sink node when needed. However, sometimes the proposed architecture selects the single-hop if the transmission distance is closer and saves the energy resources. Moreover, the proposed architecture improves a load of data distribution over the forwarders and explicitly optimizes the performance of the links even in heavy media traffic. The incorporation of edge nodes efficiently utilizes the resources of IoT network and communicate with both media sensors and sink node. Therefore, it greatly reduces the response time in the delivery of multimedia traffic and facilitates the network application for the retrieval of timely data.

In Figure 7, the experimental results illustrate the performance of the proposed architecture in terms of bandwidth in the comparison of the existing solution. It has been observed that the proposed framework improves the bandwidth utilization of the media traffic by 29% and 40% than existing work. It is due to that the proposed framework uses the data loss rate in predicting the available channels, using machine learning techniques. Moreover, it offers optimal routes with the consideration of Qos parameters and strengthened the data forwarding process. Moreover, the proposed framework exploits the edge nodes for optimizing the resources usages and supports less congested media traffic on the communication link. In contrast to EETSP, which does not consider the security objectives among constraint nodes, and ultimately, network routes are more congested due to flooding of the unauthorized packet by malicious nodes. The proposed framework efficiently utilizes the bandwidth of the constraint network by integrating the security scheme and identifying the risky links against network threats. Although EAMSuS provides the security for communication, due to high overheads on the nodes, it consumes unnecessary bandwidth and energy resources in the comparison of the proposed framework.

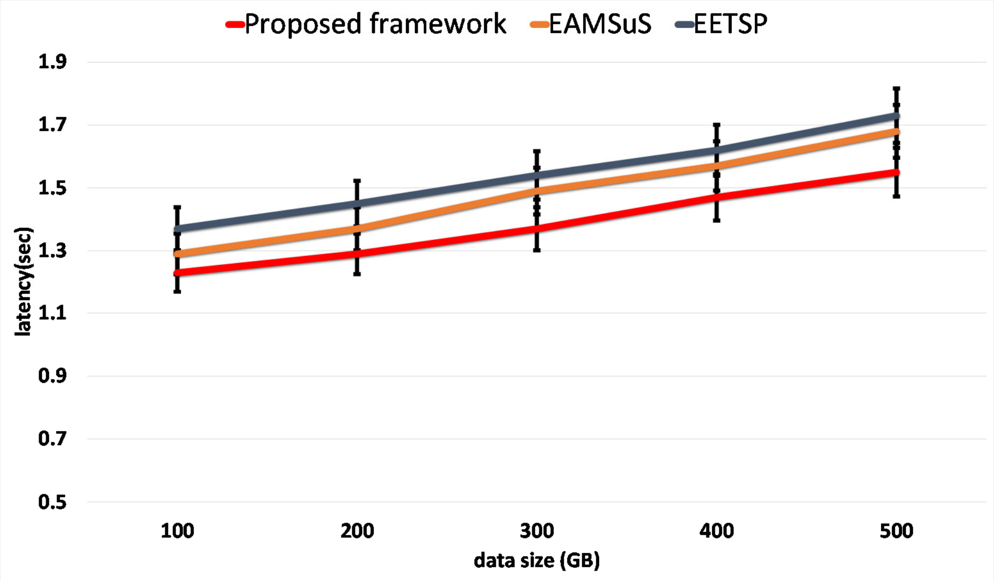


Figure 6. Evaluation of data latency with varying data size between proposed framework and existing solutions.

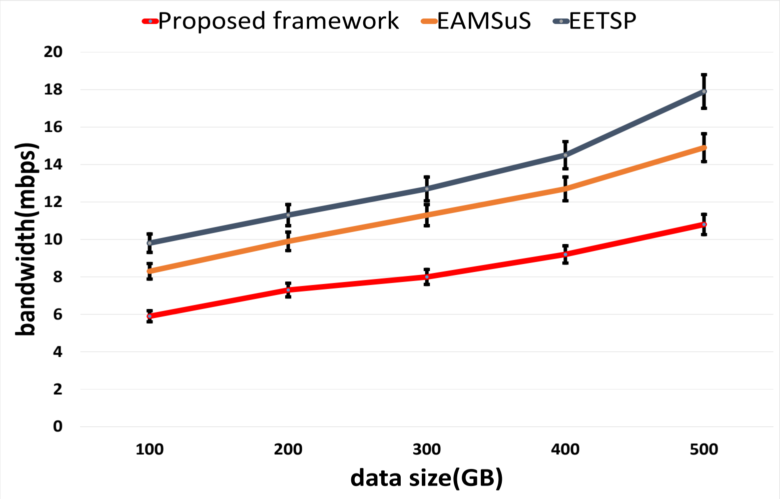


Figure 7. Evaluation of bandwidth with varying data size between proposed framework and existing solutions.

In Figure 8, the proposed framework evaluates the packet overhead in comparison to the existing solution. It has been observed that the proposed framework reduces the overhead by 35% and 44% when compared to other work. It is due to the use of the regression-based machine learning technique for forwarding node selectors that allows efficient transmission of data between the neighboring nodes toward the sink node. The node selection process is accomplished based on the stored data about the packet loss rate of each neighboring node. In contrast to EAMSuS, the proposed framework generates and distributes the security key in a lightweight manner by using the capabilities of network edges. It improves the security system among direct and partially connected devices and lowers the packets overheads while verifying the constraint nodes. Furthermore, the proposed framework enhances the security of the network by adopting multi-hop authentication and encryption protocol, which not only avoids exploitation of the network resources through unauthorized access but also keeps them from broadcasting the data toward targeted nodes.

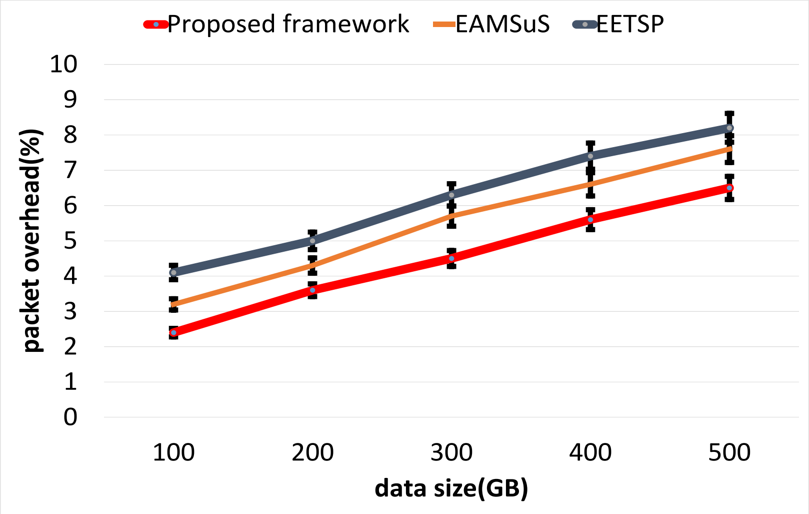


Figure 8. Evaluation of packet overhead with varying data size between proposed framework and existing solutions.

Figure 9 illustrates the computational time of the proposed framework in the comparison of existing work. It is defined as the running time initiated from the source node toward the sink node, while routing the error-free data packets. With the increasing size of data transmission, the computational time is also increasing; however, it was noticed that the proposed framework improved the computational time by 10% and 15% than other work. It is due to the utilization of regressional machine learning technique and optimizes the routing criteria intelligently. In contrast to predefined paths, the routes are updated by using dynamic attributes of a realistic environment. Moreover, the proposed security algorithm also reduces the involvement of non-authorized nodes for storing and processing media data. Consequently, the transportable path of the proposed framework is shorter and takes the least computational time in receiving the multimedia traffic toward media servers.

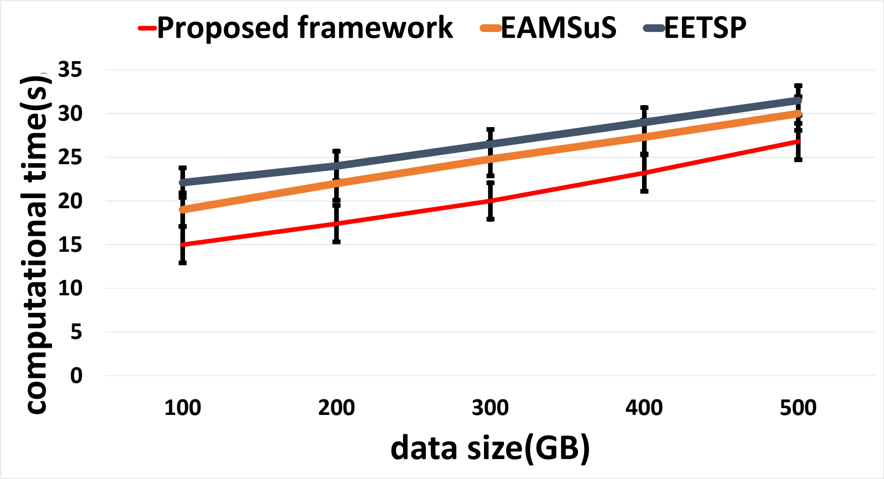


Figure 9. Evaluation of computational time with varying data size between proposed framework and existing solutions.

Figure 10 depicts the performance of the proposed framework against other solutions in terms of packets drop ratio. It was noticed that, with increasing the data sizes, the drop ratio is also increasing. However, the proposed framework reduces the packet drop ratio by 30% and 39% respectively. In contrast to EAMSuS and EETSP, the proposed framework efficiently utilizes the resources of nodes, using the regression analysis technique and selecting the optimal forwarding schemes. Moreover, the large-size media data are routed with a secured algorithm and decrease the congestion over the routing path by predicting the dynamic attributes. The proposed framework significantly minimizes the routing cost in forwarding the media data with affordable collisions in the existence of malicious nodes. Accordingly, the data loss rate is controlled reliably and increases the delivery ratio for unpredictable consequences.

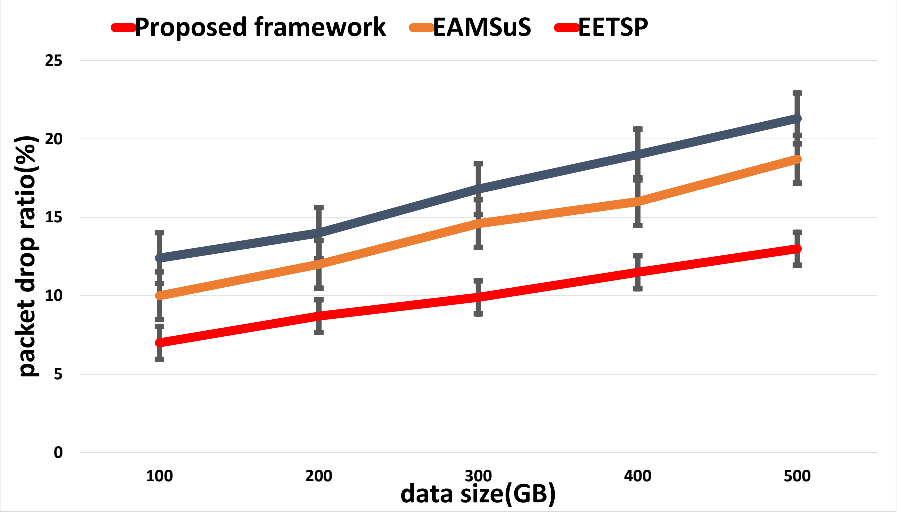


Figure 10. Evaluation of packet drop ratio with varying data size between proposed framework and existing solutions.

5. Conclusions

In this paper, a secure and sustainable prediction framework for multimedia services that uses machine learning was proposed, to improve the bandwidth utilization of the wireless channel with increasing energy efficiency. It uses the edge nodes with the collaboration of media network and sink node to support the on-time delivery and increases the network throughput for the management of big data content. The edges are made intelligent for the routing process, using machine learning regression analysis, based on multiple conditions. Moreover, before initiating the media transmission, the IoT devices are mutually authenticated among each other to verify their identities. In the proposed framework, the knapsack cryptosystem provides asymmetric-based data encryption and decryption in blockchain hashing. The set of experiments is performed in the OMNET++ simulator and based on results analysis; it has been proved that the proposed framework remarkably increases the performance for network metrics under varying data sizes. Although the proposed framework decreases the computing load and identifies the poor links using machine learning techniques for constraint nodes, the communication between mobile media devices needs to be explored. Moreover, there is a further need to improve the performance of the proposed framework in a fully distributed system by using network coding-based analysis. Moreover, in future work, we aim to incorporate software define networking to systematize the IoT environment and further reduce the communication cost by imposing a set of rules, along with the use of computationally secure cryptosystems.

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

Funding: The authors extend their appreciation to the Deanship of Scientific Research at King Saud University for funding this work through Research Project No R6-17-03-73.

Institutional Review Board Statement: None applicable.

Informed Consent Statement: None applicable.

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

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

References

1. Bin Zikria, Y.; Afzal, M.K.; Kim, S.W. Internet of Multimedia Things (IoMT): Opportunities, Challenges and Solutions. *Sensors* **2020**, *20*, 2334. [CrossRef] [PubMed]
2. Gao, H.; Duan, Y.; Shao, L.; Sun, X. Transformation-based processing of typed resources for multimedia sources in the IoT environment. *Wirel. Netw.* **2019**, *27*, 3377–3393. [CrossRef]
3. Hussain, F.; Hussain, R.; Hassan, S.A.; Hossain, E. Machine Learning in IoT Security: Current Solutions and Future Challenges. *IEEE Commun. Surv. Tutor.* **2020**, *22*, 1686–1721. [CrossRef]
4. Cui, L.; Yang, S.; Chen, F.; Ming, Z.; Lu, N.; Qin, J. A survey on application of machine learning for Internet of Things. *Int. J. Mach. Learn. Cybern.* **2018**, *9*, 1399–1417. [CrossRef]
5. Churcher, A.; Ullah, R.; Ahmad, J.; Rehman, S.U.; Masood, F.; Gogate, M.; Alqahtani, F.; Nour, B.; Buchanan, W. An Experimental Analysis of Attack Classification Using Machine Learning in IoT Networks. *Sensors* **2021**, *21*, 446. [CrossRef]
6. Mahdavinejad, M.S.; Rezvan, M.; Barekatain, M.; Adibi, P.; Barnaghi, P.; Sheth, A.P. Machine learning for internet of things data analysis: A survey. *Digit. Commun. Netw.* **2018**, *4*, 161–175. [CrossRef]
7. Okafor, K.C.; Achumba, I.E.; Chukwudebe, G.A.; Ononiwu, G. Leveraging Fog Computing for Scalable IoT Datacenter Using Spine-Leaf Network Topology. *J. Electr. Comput. Eng.* **2017**, *2017*, 1–11. [CrossRef]
8. Dai, M.; Su, Z.; Li, R.; Wang, Y.; Ni, J.; Fang, D. An Edge-Driven Security Framework for Intelligent Internet of Things. *IEEE Netw.* **2020**, *34*, 39–45. [CrossRef]
9. Messaoud, S.; Bradai, A.; Bukhari, S.H.R.; Quang, P.T.A.; Ben Ahmed, O.; Atri, M. A survey on machine learning in Internet of Things: Algorithms, strategies, and applications. *Internet Things* **2020**, *12*, 100314. [CrossRef]
10. Sudharsan, B.; Breslin, J.G.; Ali, M.I. Edge2train: A framework to train machine learning models (svms) on resource-constrained iot edge devices. In Proceedings of the 10th International Conference on the Internet of Things, Malmö, Sweden, 6–9 October 2020.
11. Babu, R.G.; Elangovan, K.; Maurya, S.; Karthika, P. Multimedia Security and Privacy on Real-Time Behavioral Monitoring in Machine Learning IoT Application Using Big Data Analytics. In *Multimedia Technologies in the Internet of Things Environment*; Springer: Berlin/Heidelberg, Germany, 2021; pp. 137–156.
12. Huang, X.; Xie, K.; Leng, S.; Yuan, T.; Ma, M. Improving Quality of Experience in multimedia Internet of Things leveraging machine learning on big data. *Future Gener. Comput. Syst.* **2018**, *86*, 1413–1423. [CrossRef]
13. Skorin-Kapov, L.; Varela, M.; Hoßfeld, T.; Chen, K.-T. A survey of emerging concepts and challenges for QoE management of multimedia services. *ACM Trans. Multimed. Comput. Commun. Appl. TOMM* **2018**, *14*, 1–29. [CrossRef]
14. Saba, T.; Haseeb, K.; Din, I.U.; Almogren, A.; Altameem, A.; Fati, S.M. EGCIR: Energy-Aware Graph Clustering and Intelligent Routing Using Supervised System in Wireless Sensor Networks. *Energies* **2020**, *13*, 4072. [CrossRef]
15. 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]
16. Haseeb, K.; Islam, N.; Almogren, A.; Din, I.U. Intrusion prevention framework for secure routing in WSN-based mobile Internet of Things. *IEEE Access* **2019**, *7*, 185496–185505. [CrossRef]
17. Liao, B.; Ali, Y.; Nazir, S.; He, L.; Khan, H.U. Security analysis of IoT devices by using mobile computing: A systematic literature review. *IEEE Access* **2020**, *8*, 120331–120350. [CrossRef]
18. Vorakulpipat, C.; Rattanalerdnusorn, E.; Thaenkaew, P.; Hai, H.D. Recent challenges, trends, and concerns related to IoT security: An evolutionary study. In Proceedings of the 2018 20th International Conference on Advanced Communication Technology (ICACT), Chuncheon, Korea, 11–14 February 2018; IEEE: Piscataway, NJ, USA, 2018.
19. Islam, N.; Shahid, Z.; Puech, W. Denoising and error correction in noisy AES-encrypted images using statistical measures. *Signal. Process. Image Commun.* **2016**, *41*, 15–27. [CrossRef]
20. Hanif, S.; Khedr, A.M.; al Aghbari, Z.; Agrawal, D.P. Opportunistically exploiting internet of things for wireless sensor network routing in smart cities. *J. Sens. Actuator Netw.* **2018**, *7*, 46. [CrossRef]

21. Haseeb, K.; Jan, Z.; Alzahrani, F.A.; Jeon, G. A Secure Mobile Wireless Sensor Networks based Protocol for Smart Data Gathering with Cloud. *Comput. Electr. Eng.* **2021**, 107584. [CrossRef]
22. Islam, N.; Haseeb, K.; Almogren, A.; Din, I.U.; Guizani, M.; Altameem, A. A framework for topological based map building: A solution to autonomous robot navigation in smart cities. *Future Gener. Comput. Syst.* **2020**, *111*, 644–653. [CrossRef]
23. Badshah, A.; Islam, N.; Shahzad, D.; Jan, B.; Farman, H.; Khan, M.; Jeon, G.; Ahmad, A. Vehicle navigation in GPS denied environment for smart cities using vision sensors. *Comput. Environ. Urban. Syst.* **2019**, *77*, 101281. [CrossRef]
24. Kumar, D.P.; Amgoth, T.; Annavarapu, C.S.R. Machine learning algorithms for wireless sensor networks: A survey. *Inf. Fusion* **2019**, *49*, 1–25. [CrossRef]
25. Din, I.U.; Guizani, M.; Rodrigues, J.J.; Hassan, S.; Korotaev, V.V. Machine learning in the Internet of Things: Designed techniques for smart cities. *Future Gener. Comput. Syst.* **2019**, *100*, 826–843. [CrossRef]
26. Jiang, C.; Zhang, H.; Ren, Y.; Han, Z.; Chen, K.-C.; Hanzo, L. Machine learning paradigms for next-generation wireless networks. *IEEE Wirel. Commun.* **2016**, *24*, 98–105. [CrossRef]
27. Pan, Y.; Chen, M.; Yang, Z.; Huang, N.; Shikh-Bahaei, M. Energy-efficient NOMA-based mobile edge computing offloading. *IEEE Commun. Lett.* **2018**, *23*, 310–313. [CrossRef]
28. Xu, X.; Zhang, X.; Gao, H.; Xue, Y.; Qi, L.; Dou, W. BeCome: Blockchain-enabled computation offloading for IoT in mobile edge computing. *IEEE Trans. Ind. Inform.* **2019**, *16*, 4187–4195. [CrossRef]
29. Haseeb, K.; Din, I.U.; Almogren, A.; Ahmed, I.; Guizani, M. Intelligent and Secure Edge-enabled Computing Model for Sustainable Cities using Green Internet of Things. *Sustain. Cities Soc.* **2021**, *68*, 102779. [CrossRef]
30. Singh, A.; Mahapatra, S. Network-based applications of multimedia big data computing in iot environment. In *Multimedia Big Data Computing for IoT Applications*; Springer: Berlin/Heidelberg, Germany, 2020; pp. 435–452.
31. Khan, P.W.; Byun, Y.-C.; Park, N. A data verification system for CCTV surveillance cameras using blockchain technology in smart cities. *Electronics* **2020**, *9*, 484. [CrossRef]
32. Merzoug, M.A.; Mostefaoui, A.; Gianini, G.; Damiani, E. Smart connected parking lots based on secured multimedia IoT devices. *Computing* **2021**, *103*, 1143–1164. [CrossRef]
33. Punithavathi, P.; Geetha, S.; Karuppiah, M.; Islam, S.H.; Hassan, M.M.; Choo, K.-K.R. A lightweight machine learning-based authentication framework for smart IoT devices. *Inf. Sci.* **2019**, *484*, 255–268. [CrossRef]
34. Dwivedi, A.K.; Mehra, P.S.; Pal, O.; Doja, M.N.; Alam, B. EETSP: Energy-efficient two-stage routing protocol for wireless sensor network-assisted Internet of Things. *Int. J. Commun. Syst.* **2021**, *34*, e4965. [CrossRef]
35. Rahman, M.S.; Khalil, I.; Moustafa, N.; Kalapaaking, A.P.; Bouras, A. A Blockchain-enabled Privacy-Preserving Verifiable Query Framework for Securing Cloud-Assisted Industrial Internet of Things Systems. *IEEE Trans. Ind. Inform.* **2021**. [CrossRef]
36. Noura, H.; Chehab, A.; Sleem, L.; Noura, M.; Couturier, R.; Mansour, M.M. One round cipher algorithm for multimedia IoT devices. *Multimed. Tools Appl.* **2018**, *77*, 18383–18413. [CrossRef]
37. Memos, V.A.; Psannis, K.E.; Ishibashi, Y.; Kim, B.-G.; Gupta, B.B. An efficient algorithm for media-based surveillance system (EAMSuS) in IoT smart city framework. *Future Gener. Comput. Syst.* **2018**, *83*, 619–628. [CrossRef]
38. Mydhili, S.; Periyanayagi, S.; Baskar, S.; Shakeel, P.M.; Hariharan, P. Machine learning based multi scale parallel K-means++ clustering for cloud assisted internet of things. *Peer Peer Netw. Appl.* **2020**, *13*, 2023–2035. [CrossRef]
39. Radhika, S.; Rangarajan, P. On improving the lifespan of wireless sensor networks with fuzzy based clustering and machine learning based data reduction. *Appl. Soft Comput.* **2019**, *83*, 105610. [CrossRef]
40. Ancillotti, E.; Vallati, C.; Bruno, R.; Mingozzi, E. A reinforcement learning-based link quality estimation strategy for RPL and its impact on topology management. *Comput. Commun.* **2017**, *112*, 1–13. [CrossRef]
41. Merkle, R.; Hellman, M. Hiding information and signatures in trapdoor knapsacks. *IEEE Trans. Inf. Theory* **1978**, *24*, 525–530. [CrossRef]
42. Zhou, X.; Tang, X. Research and implementation of RSA algorithm for encryption and decryption. In Proceedings of the 2011 6th International Forum on Strategic Technology, Harbin, China, 22–24 August 2011; IEEE: Piscataway, NJ, USA, 2011.
43. Varga, A. A practical introduction to the OMNeT++ simulation framework. In *Recent Advances in Network Simulation*; Springer: Berlin/Heidelberg, Germany, 2019; pp. 3–51.
44. Nardini, G.; Sabella, D.; Stea, G.; Thakkar, P.; Virdis, A. Simu5G–An OMNeT++ Library for End-to-End Performance Evaluation of 5G Networks. *IEEE Access* **2020**, *8*, 181176–181191. [CrossRef]