electronics

Article

EdgeTrust: A Lightweight Data-Centric Trust Management Approach for IoT-Based Healthcare 4.0

Kamran Ahmad Awan [1], Ikram Ud Din [1,*], Ahmad Almogren [2,*], Hasan Ali Khattak [3] and Joel J. P. C. Rodrigues [4,5]

[1] Department of Information Technology, The University of Haripur, Haripur 22620, Pakistan
[2] Chair of Cyber Security, Department of Computer Science, College of Computer and Information Sciences, King Saud University, Riyadh 11633, Saudi Arabia
[3] School of Electrical Engineering & Computer Science (SEECS), National University of Sciences & Technology (NUST), H12, Islamabad 44000, Pakistan
[4] College of Computer Science and Technology, China University of Petroleum (East China), Qingdao 266555, China
[5] Instituto de Telecomunicações, 6201-001 Covilhã, Portugal
* Correspondence: ikramuddin205@yahoo.com (I.U.D.); ahalmogren@ksu.edu.sa (A.A.)

Abstract: Internet of Things (IoT) is bringing a revolution in today's world where devices in our surroundings become smart and perform daily-life activities and operations with more precision. The architecture of IoT is heterogeneous, providing autonomy to nodes so that they can communicate with other nodes and exchange information at any time. IoT and healthcare together provide notable facilities for patient monitoring. However, one of the most critical challenges is the identification of malicious and compromised nodes. In this article, we propose a machine learning-based trust management approach for edge nodes to identify nodes with malicious behavior. The proposed mechanism utilizes knowledge and experience components of trust, where knowledge is further based on several parameters. To prevent the successful execution of good and bad-mouthing attacks, the proposed approach utilizes edge clouds, i.e., local data centers, to collect recommendations to evaluate indirect and aggregated trust. The trustworthiness of nodes is ranked between a certain limit, and only those nodes that satisfy the threshold value can participate in the network. To validate the performance of the proposed approach, we have performed extensive simulations in comparison with existing approaches. The results show the effectiveness of the proposed approach against several potential attacks.

Keywords: Internet of Things; trust management; healthcare; digital revolution; edge clouds; security; privacy preservation

check for updates

Citation: Awan, K.A.; Ud Din, I.; Almogren, A.; Khattak, H.A.; Rodrigues, J.J.P.C. EdgeTrust: A Lightweight Data-Centric Trust Management Approach for IoT-Based Healthcare 4.0. *Electronics* **2023**, *12*, 140. https://doi.org/10.3390/electronics12010140

Academic Editor: Cheng-Chi Lee

Received: 15 December 2022
Revised: 20 December 2022
Accepted: 24 December 2022
Published: 28 December 2022

1. Introduction

Internet of Things (IoT) [1] consists of diverse standards of nodes in a heterogeneous environment connected with the Internet to communicate and exchange information in the network [2]. The classification of these nodes can be created based on their processing power wherein edge devices, such as sensors, contain the least processing power causing vulnerabilities [3]. The generic architecture of IoT consists of multiple layers, i.e., business, application, middleware, and perception layers [4], which are illustrated in Figure 1. The business layer contains system management solutions that may be varied according to the requirements [5]. The middleware layer is the most critical layer that consists of information processing [6], ubiquitous computing [7], services management [8], databases [9], and decision units [10]. The network layer consists of transmission networks that provide a source by which IoT participating nodes can transmit information among them [11]. These transmission connections will be 4G, 5G, etc. [12]. The perception layer consists of edge nodes that can be RFID [13], sensors [14], or any physical object [15]. In [4], a generic

IoT trust architecture is proposed that integrates trust into all these layers as an integral component to manage security. IoT faces several security challenges [16], e.g., authentication [17,18], access control [19], trust management in cross-domain along with smart edge nodes [20], security management in IoT equipped with VANET nodes, policy enforcement, secure middleware, and confidentiality.

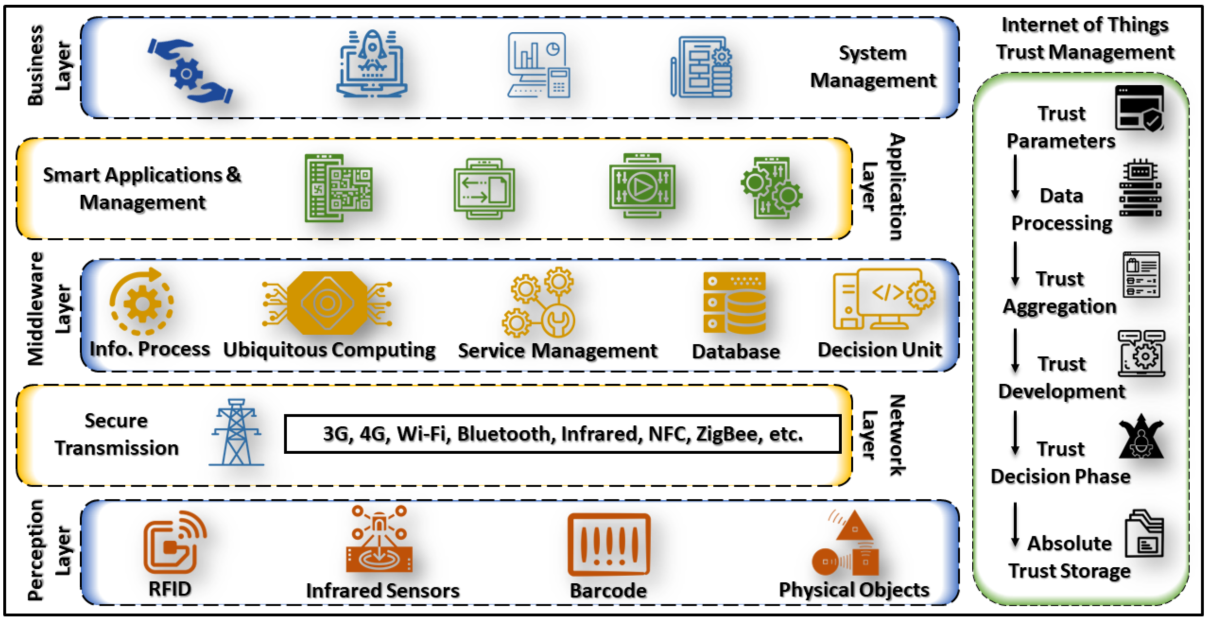

Figure 1. IoT architecture with the integration of trust management.

Due to the heterogeneous environment of IoT, it is inevitable to implement robust approaches that maintain a secure environment by eliminating malicious nodes and are also robust enough to keep resilience towards several potential attacks [21–23]. The maintenance of security is a significant challenge due to wireless technologies that have been extensively deployed in the IoT environment [24]. Healthcare 4.0 [25] is the term used to describe the next generation of healthcare technology, which is focused on harnessing data, and analytic and digital tools to improve patient care and outcomes. The cost of healthcare is a major issue for many people, and patients are looking for ways to obtain the care they need without breaking the bank. The trend toward more affordable healthcare [26] has led to an incredibly promising new technology, i.e., IoT, which allows us to connect devices with sensors so that we can track our health in real-time [27]. With IoT, doctors can use AI [28] to analyze your health data and make predictions about your future health prospects. Healthcare monitoring contains patients' electronic health records [29] that are transmitted to doctors for monitoring. The transmitted data become vulnerable to potential IoT attacks. The most prominent way to maintain a trustworthy environment is to identify and eliminate such nodes. Trust is proposed as the most prominent lightweight mechanism that helps to maintain a secure environment by utilizing parameters.

In this article, we have proposed a trust management approach (EdgeTrust) for those nodes which are not capable to perform complex computations. The proposed approach is a combination of centralized and distributed trust management architectures. The EdgeTrust working consists of two major components, i.e., distributed edge devices and centralized data centers/edge clouds. The proposed mechanism utilizes the direct and indirect trust evaluation mechanism where the pre-observations required to evaluate the trust are provided by a central authority. The absolute direct trust evaluation consists of observations provided by central authority along with the observations stored on nodes' local storage. For indirect trust evaluation, nodes also do not require generating the request to neighboring nodes as the recommendation is to gather by a central authority. The advantage of utilizing recommendations of the centralized authority reduces the time required to evaluate the trust. The trust is further compared with the threshold value for decision-making.

The structure of the rest of the article is as follows: Section 2 discusses and elaborates on the existing trust management approaches. Section 3 explains the working of the proposed mechanism such as trust parameters, computations, trust aggregation, and threshold comparison of trust. Section 4 elaborates and discusses the simulation outcomes and performance comparison of EdgeTrust with existing approaches. Finally, Section 5 concludes the paper.

2. Literature Review

There are several trust management approaches proposed for IoT-based Healthcare, but significant research attention is required to address the computational challenges associated with IoT edge devices that are not capable of performing complex computations. This section will elaborate on the existing approaches along with their contribution and limitation to identify the research gaps, also illustrated in Table 1.

A trust management mechanism is proposed for the Social IoT that maintains trust by self-enforcing in a decentralized manner [30]. The proposed mechanism architecture consists of multiple IoT devices owned by numerous users who interact with others at particular time intervals. After the interaction, these nodes submit user ratings to the IoT decentralized database shared among nodes. These ratings consist of feedback and zero knowledge. The major contribution of the proposed mechanism is the integration of a database that contains the feedback of the nodes. However, the decentralized database can cause data integrity challenges as it is shared and stored without utilizing any central authority.

A game theory-based decentralized trust management mechanism is proposed for IoT to maintain robustness among nodes [31]. The proposed mechanism applies the game theory to identify nodes that are executing good or bad-mouthing attacks by sending mendacious trust degrees. For updating the trust degrees of nodes, the proposed approach utilizes the Dempster–Shafer theory that collects the scores for updating process by excluding disparate scores. To perform a trust computation, the approach utilizes Fuzzy theory to classify trust into none, low, high, and definitely. The major contribution of the proposed mechanism is the utilization of the Fuzzy rule to classify trust. However, the performance of the proposed mechanism needs to be evaluated against potential IoT attacks such as on-off, whitewashing, etc.

In 2017, a study was proposed to design an architecture and protocol for eHealth monitoring with the integration of 5G [32]. The study focuses on the continuous monitoring of patient's health and concludes no notable difference between 4G and 5G. The architecture of the proposed scheme consists of a user, a 5G network-enabled antenna, and a database server on the hospital side. Users/patients are monitored using Bluetooth wearable sensors and gadgets, whereas the monitored data are forwarded to the hospital using a 5G network. The monitored data are received by the database server, which acts as the central authority between the hospital and its users. The database also receives medical analytical data from hospitals and forwards alarms to patients in case of emergency.

In 2020, a blockchain-based trust protocol was proposed for IoT, which maintains trust in a decentralized manner [33]. The study stated that an IoT object can communicate and exchange information, which makes the environment highly dynamic and raise security challenges. The proposed mechanism is a hierarchical blockchain protocol that also supports mobility where the architecture of the proposed mechanism consists of a fog layer, a private blockchain layer, and an IoT layer with different clusters/zones.

In 2018, an energy-efficient trust management mechanism (EET-IoT) [34] is proposed to protect the IoT network and primarily focus on smart cities [35,36]. The proposed mechanism utilizes the IEEE 802.14 protocol to perform computations. The purpose of using the IEEE 802.14 protocol is to sustain the efficiency of the IEET-IoT. The proposed mechanism further uses Jasang's Subjective Logic (JSL) to examine the ambiguity of an entity. The EET-IoT uses a triple variable concept, i.e., b, d, and u. Variable b expresses the belief, d represents the disbelief, and u denotes the uncertainty. The evaluation of EET-IoT shows a significant decrease in energy utilization. The energy consumption evaluation of the proposed algorithms shows that LT consumes maximum energy followed by LDE and NDLF. However, optimization at the MAC Layer is required to overcome adequate energy consumption.

A smart middle-ware mechanism (Smart-TM) [37] is proposed to detect on-off attacks in IoT. The focus of the proposed mechanism is to automatically assess the resources of IoT trust by evaluating the attributes of service providers. The Smart-TM utilizes an approach of machine learning based on the One-Class Support Vector Machine (OneClass-SVM) method. The degree of trust is estimated by examining the distance from a function of the Hyper-plane model. Moreover, the middleware implements the decision function to estimate the trust, and nodes with a higher degree of trust are listed as trusted nodes, while nodes with a lower degree of trust are classified as untrusted ones or specified as attackers. The performance evaluation of Smart-TM represents that the proposed approach successfully distinguishes the behavior to recognize on-off attacks. However, the proposed mechanism is unable to specify the framework of information gathering, trust dissemination, updating, and maintenance.

A scheme of trust management (Tm-SecPro) [38] is proposed that adopts two methods, i.e., maximum ratios combining and selection combining. In Tm-SecPro, service providers and seekers communicate with each other directly, and the mechanism preserves trust between them. The proposed mechanism estimates and concludes the results in three phases. In the first phase, the information about trust control is transmitted to the lower layer. In the second phase, the specified model is used to calculate the trust values. While in the last phase, all relations related to these phases are extracted from each layer. The considerable aspect of this scheme is a fusion of MRC and SC that will help to maintain the reliability of Tm-SecPro.

Table 1. The comparative analysis of the existing approaches.

Ref.	Contribution	Limitation
[30]	Integration of database that contains feedback of the nodes.	Decentralized databases can cause integrity challenges.
[31]	Utilization of Fuzzy rule to classify trustworthy and malicious nodes.	Performance needed to be evaluated in the IoT Environment.
[33]	Hierarchical blockchain protocol that also supports mobility.	Not suitable for nodes with less computational capabilities due to complexity.
[34]	The utilization of Jasang's Subjective Logic (JSL) to examine the ambiguity of an entity.	Optimization at MAC Layer is required to overcome adequate energy consumption.
[37]	Hyper-plane model along with middleware implements the decision function.	Unable to specify the framework of trust management.
[38]	Fusion of MRC and SC that will help to maintain reliability.	Transmission of trust computation between multiple layers may raise integrity challenges.

3. Proposed EdgeTrust Approach

The identification of malicious and compromised is one of the important challenges in Healthcare 4.0 that can affect the network security and privacy of users. In this article, we have proposed EdgeTrust to address the challenges caused by these malicious nodes. The architecture of the proposed approach consists of three major layers which are data center/edge clouds, trust management, and edge nodes as illustrated in Figure 2. The data center contains the data center and edge cloud that have the capability of Naive Bayes [39,40] for the identification and classification and behavior prediction of malicious and compromised nodes by utilizing the stored direct observation collected by the network nodes. These observations are utilized further to formulate direct trust for edge nodes. Indirect trust at the data center layer can be formulated with the help of recommendations collected by the edge nodes. The trust management evaluation is a combination of events and time-driven under a different scenario. The direct trust degree is evaluated-based on the knowledge and experience component, which also involves the trust aggregation, threshold comparison, and decision-making phase. The edge nodes in IoT can be classified concerning their computational power and internal capabilities.

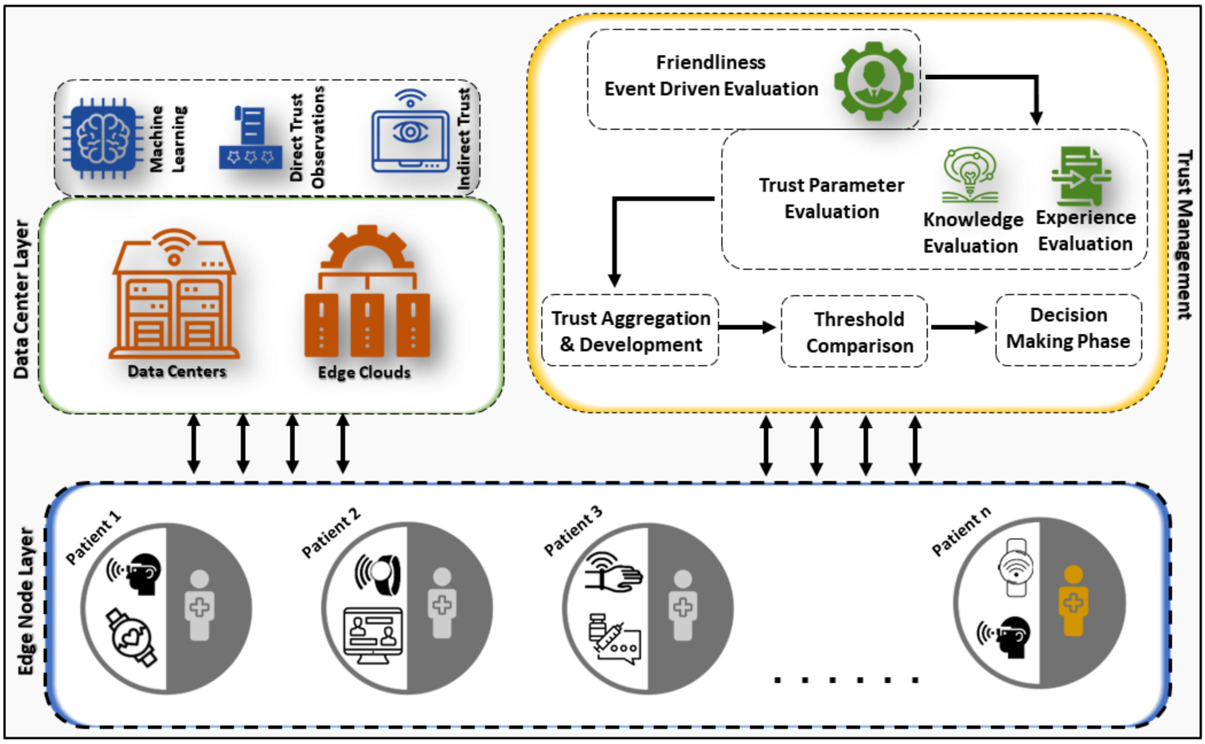

Figure 2. The proposed EdgeTrust architecture.

In the proposed approach, these edge nodes are classified based on their categories, i.e., sensors, home appliances, and smart mobile devices among others. The training phase of the proposed mechanism includes five distinct phases which are features selection, feature scaling, classifier implementation, dataset training, and classification of malicious and compromised nodes. The features of trust parameters used are reliability, cooperativeness along with experience, and the computation depends on sessions created between nodes which are denoted as friendliness. If the friendliness of nodes is higher, then the computations are computed in a time-driven manner while, in the case of low friendliness, trust computation is performed based on events. The next phase is to scale the features in which all the features involved in computations are scaled between 0.0–1, where 0.0 represents the lowest trust and 1 represents a higher trust degree. The complete workflow of trust computation and decision-making is illustrated by Algorithm 1.

Algorithm 1 EdgeTrust trust computation process

```
procedure Trust degree evaluation($d_t^{ob}$)
    Central authority computation: ${}_t^{ob} = \sum\Big[ob_{n-id}^1 + ob_{n-id}^2 + ob_{n-id}^3 + ... + ob_{n-id}^n\Big]$
    Recommendation-based evaluation: $r_{c-id}^{itrust} = \sum\Big[rec_{r_1}^{e_i \to e_j} + rec_{r_2}^{e_i \to e_j} + ... + rec_{r_n}^{e_i \to e_j}\Big]$
procedure Experience gathering and formulation($ab_{e_i \to e_j}^{t \to aggregate}$)
    Previous computation: $ep_{e_{absolute}}^{node-id} = \sum\Big[ep_{e_i \to e_j}^{p_1} + ep_{e_i \to e_j}^{p_2} + ... + ep_{e_i \to e_j}^{p_n}\Big]$
    Aggregated trust: $ab_{e_i \to e_j}^{t \to aggregate} = d_t^{ob} + ep_{e_{absolute}}^{node-id}$
procedure Trust computation
    Friendliness computations: $fr_{n_{id}}^{tr}$
    Reliability observation: $obp_{e_i \to e_j}^{rt} = ob_{n-id}^{t(e_i \to e_j)_1} + ob_{n-id}^{t(e_i \to e_j)_2} + ... + ob_{n-id}^{t(e_i \to e_j)_n}$
    Reliability formulation: $rt_{e_i \to e_j}^{dt}$
    Cooperativeness computation: $obp_{e_i \to e_j}^{cpt} = ob_{n-id}^{cpt_1} + ob_{n-id}^{cpt_2} + ob_{n-id}^{cpt_3} + ... + ob_{n-id}^{cpt_n}$
procedure Trust aggregation($f_{te_i \to e_j}^{dt_{exp}}$)
    Absolute computation: $ct_{d_{e_i \to e_j}}^{ag} = rt_{e_i \to e_j}^{dt} + cpt_{e_i \to e_j}^{dt}$
    Experience formulation: $t_{exp_{e_i \to e_j}}^{pt} = \sum_{i=0}^{n}\Big[et_{e_i \to e_j}^{o_1} + et_{e_i \to e_j}^{o_2} + ... + et_{e_i \to e_j}^{o_n}\Big]$
    Absolute trust degree: $f_{te_i \to e_j}^{dt_{exp}} = ct_{d_{e_i \to e_j}}^{ag} + t_{exp_{e_i \to e_j}}^{pt}$
procedure Decision making
    Decision making: $\theta = t_{exp_{e_i \to e_j}}^{pt}$
Exit
```

To perform classification and prediction, we adopt the Naive Bayes classifier due to its accuracy and low energy consumption for classification. After selecting the classifier, the training phase begins, using a dataset of 120,766 trust values per feature for the classifier to learn from. After training, the classifier calculates the error difference between computed and actual trust values to increase precision.

3.1. Data Centers and Edge Clouds

In the proposed approach, the data center layer is responsible for performing three major operations: machine learning-based prediction and direct and indirect trust observation evaluation. The data centers and edge clouds are able to make predictions based on direct observations transmitted by the nodes. These transmitted values are first stored by the central authorities and later used to predict the behavior of edge nodes by applying the Naive Bayes Classifier. The direct trust evaluation at the data center layer is a time-driven process, evaluated after 90 minutes. When an edge node requests data from the data center layer, the central authorities share the already stored observations for further processing. After receiving the request, the central authorities formulate the direct trust degree using Equation (1), where d_t^{ob} represents the available direct trust observation and ob_{n-id}^1 is the number of observations transmitted by a particular node.

$$d_t^{ob} = \sum\Big[ob_{n-id}^1 + ob_{n-id}^2 + ob_{n-id}^3 + ... + ob_{n-id}^n\Big] \tag{1}$$

The coverage area of central authorities is larger compared to edge trust, so they also provide recommendations that have been computed over a specific time interval. These recommendations help nodes to compute indirect trust. The recommendation-based indirect trust is formulated using Equation (2), where $\mathrm{r}_{c-id}^{itrust}$ represents the recommendation-based trust evaluation, and c-id represents the unique identity of a central authority that computed indirect trust.

$$r_{c-id}^{itrust} = \sum \left[rec_{r_1}^{e_i \to e_j} + rec_{r_2}^{e_i \to e_j} + \ldots + rec_{r_n}^{e_i \to e_j} \right] \tag{2}$$

3.2. IoT Edge Nodes

The edge nodes are those that cannot perform complex computations but are crucial to lightening the burden from them to increase the scalability and security of a network. In the proposed EdgeTrust approach, central authorities compute the direct trust and transmit it to the requested node while the edge nodes just have to aggregate that value with the pre-stored experience. The experience component of trust represents the previous experience of a particular node regarding other nodes that provide services. To evaluate the aggregate value, the edge nodes apply the summation function to the previous experience available as represented by Equation (3), where $ep_{e_{absolute}}^{node-id}$ shows the absolute experience formulation of a node with a unique identity. The $ep_{e_i \to e_j}^{p_1}$ represents the number of previous experiences stored on the internal memory of edge nodes.

$$ep_{e_{absolute}}^{node-id} = \sum \left[ep_{e_i \to e_j}^{p_1} + ep_{e_i \to e_j}^{p_2} + \ldots + ep_{e_i \to e_j}^{p_n} \right] \tag{3}$$

After the formulation of absolute experience, the edge node computes aggregate trust by using the direct trust and experience trust degree computation as represented by Equation (4), where $ab_{e_i \to e_j}$ represents the absolute trust evaluation of edge node i towards j, d_t^{ob} and $ep_{e_{absolute}}^{node-id}$ represent the direct trust evaluated based on observation and experience evaluation of a node with unique identifiers, respectively.

$$ab_{e_i \to e_j}^{t \to aggregate} = d_t^{ob} + ep_{e_{absolute}}^{node-id} \tag{4}$$

3.3. Trust Management Computations

The trust computation in the proposed mechanism consists of multiple features that are computed by the central authorities along with edges to formulate an absolute trust value for decision-making. When edge nodes want to compute the trust value of a particular node, the node transmits a trust computation request to the nearest central authority. The request generated by a particular node consists of the trustee's identification, the trustor's identification, and the previous experience trust degree computed by the edge nodes. The trust computation process begins by first observing the friendliness of the nodes, which represents the number of sessions created over a specific interval of time. If the friendliness of the nodes is high, then trust is computed as time-driven, which reduces the energy consumption of computation. The time-driven trust computation in the case of higher friendliness is 60 min, which means that nodes are not required to compute trust based on events and can use the same trust degree for a pre-defined time. The friendliness is computed based on the sessions created between particular nodes, as represented in Equation (5).

$$fr_{n_{id}}^{tr} = \begin{cases} timedriven & \text{if } fr \geq 50 \\ Eventdriven & \text{if } fr \leq 49 \\ indirecttrust & \text{if } p_{ob} = Yes \end{cases} \tag{5}$$

In Equation (5), *fr*, $n_i d$, and *tr* represent friendliness, nodes' unique identify, and trust degree, respectively. For direct trust, if $fr \geq 50$, the trust is computed as time-driven. When the number of sessions formulated between two nodes becomes event-driven and $fr \leq 49$, the trust is also computed using a time-driven approach. In case of no previous observations $p_o b$, the trust is computed by gathering recommendations from central authorities. After evaluating friendliness, the next phase is to compute the trust parameters, i.e., knowledge and experience. TThe knowledge component of trust consists of reliability and cooperativeness, which are computed by central authorities when a particular node generates a request. In the knowledge parameters, the evaluation is initiated by evaluating the reliability by gathering the pre-stored observations received by the central authorities for a while from network nodes. The process of observation gathering is shown in Equation (6), where the reliability trust degree is formulated by applying summation to these pre-available observations:

$$obp^{rt}_{e_i \to e_j} = ob^{t(e_i \to e_j)_1}_{n-id} + ob^{t(e_i \to e_j)_2}_{n-id} + ... + ob^{t(e_i \to e_j)_n}_{n-id} \tag{6}$$

In Equation (6), *obp* represents previous observations, *rt* shows reliability trust evaluation, and $e_i \to e_j$ is the trust evaluation of edge node *i* towards *j*, where $ob^{t(e_i \to e_j)_1}_{n-id}$ represents the pre-stored previous observations. After reliability observation gathering, the proposed mechanism applies a limit to formulate the absolute trust value of the reliability parameter as shown in Equation (7):

$$rt^{dt}_{e_j} = ob^{t(e_i \to e_j)_1}_{n-id} + ob^{t(e_i \to e_j)_2}_{n-id} + ... + ob^{t(e_i \to e_j)_n}_{n-id} \tag{7a}$$

$$rt^{dt}_{e_i \to e_j} = \sum_{i=0}^{n} [obp^{rt}_{e_i \to e_j} * rt^{dt}_{e_j}] \tag{7b}$$

In Equation (7), $rt^{dt}_{e_i \to e_j}$ represent the evaluation of reliability evaluation based on a direct trust approach, where $\sum_{0.0}^{1}$ is the summation function that applies on the previous trust observation to formulate absolute reliability trust degree with a limit of 0.0–1. The completion of reliability evaluation leads the computation phase to cooperativeness estimation. The cooperativeness evaluation is evaluated with the same process as reliability computation and represented by Equation (8). In Equation (8a), $obp^{cpt}_{e_i \to e_j}$ represents the cooperativeness trust evaluation of edge node *i* towards *j* where $ob^{cpt_(1...n)}_{n-id}$ represents the available observations utilized for the cooperativeness trust evaluation. In Equation (8b), $cpt^{dt}_{e_i \to e_j}$ represents the formulation of absolute cooperativeness trust degree, while *dt* shows the direct trust evaluation. After the trust parameter estimation, the central authority will proceed further for the trust formulation along with experience as explained in Section 3.4:

$$obp^{cpt}_{e_i \to e_j} = ob^{cpt_1}_{n-id} + ob^{cpt_2}_{n-id} + ob^{cpt_3}_{n-id} + ... + ob^{cpt_n}_{n-id} \tag{8a}$$

$$cpt^{dt}_{e_i \to e_j} = \sum_{i=0}^{n} \left[obp^{cpt}_{e_i \to e_j} (ob^{cpt_1}_{n-id} + ob^{cpt_2}_{n-id} + ... + ob^{cpt_n}_{n-id}) \right] \tag{8b}$$

3.4. Trust Aggregation and Development

The trust aggregation process is the procedure in which the previous trust value has been utilized with the current trust to develop an absolute trust value that is used during the phase of decision-making. In the proposed approach, the aggregation and development process is initiated by developing the trust degree of the parameter. Furthermore, it uses that value to compute the aggregated value of trust with the previous experience trust degree of a node. At that phase, the proposed mechanism formulates the absolute trust degree of knowledge component that consists of reliability, and cooperativeness as illustrated in Equation (9):

$$ct^{ag}_{d_{e_i \to e_j}} = rt^{dt}_{e_i \to e_j} + cpt^{dt}_{e_i \to e_j} \tag{9}$$

In Equation (9), the $ct^{ag}_{d_{e_i \to e_j}}$ represents the direct current trust evaluation of edge node *i* towards *j*, where $rt^{dt}_{e_i \to e_j}$ and $cpt^{dt}_{e_i \to e_j}$ illustrate the reliability and cooperativeness trust evaluation. After developing the parameter trust evaluation, the central authorities transmit the trust degree of a particular node towards the edge node for the aggregation of experience with current trust. After receiving the parameter trust degree, the edge node aggregates the experience with current trust by first formulating the previous experience observations using Equation (10):

$$t^{pt}_{exp_{e_i \to e_j}} = \sum_{i=0}^{n} \left[et^{o_1}_{e_i \to e_j} + et^{o_2}_{e_i \to e_j} + ... + et^{o_n}_{e_i \to e_j} \right] \tag{10a}$$

$$f^{dt_{exp}}_{te_i \to e_j} = ct^{ag}_{d_{e_i \to e_j}} + t^{pt}_{exp_{e_i \to e_j}} \tag{10b}$$

In Equation (10a), $t^{pt}_{exp_{e_i \to e_j}}$ represents the absolute experience trust formulation process of edge node i towards j, where $et^{o_{1...n}}_{e_i \to e_j}$ illustrates the number of previous experience evaluation available at local storage of edge nodes. In Equation (10b), $f^{dt_{exp}}_{te_i \to e_j}$ represents the formulation process of final trust degree, where $ct^{ag}_{d_{e_i \to e_j}}$ is the current trust parameter evaluation and $t^{pt}_{exp_{e_i \to e_j}}$ illustrates the absolute experience trust evaluation. After the formulation of the final trust degree, the edge node can compare it with the threshold value for decision-making as discussed in Section 3.5.

3.5. Trust-Based Decision-Making

The decision-making phase is the final phase that utilizes the absolute final trust degree to compare it with a threshold value to determine if the node is trustworthy or malicious. In the proposed mechanism, the range of trust degree is 0.0 to 1. Newly joined edge nodes have a default trust degree of 0.6. A trust degree of 0.7 to 1 is considered trustworthy, while a trust degree of 0.0 to 0.6 is considered flunk/no trust for old edge nodes, as illustrated in Equation (11).

$$\theta = t^{pt}_{exp_{e_i \to e_j}} \tag{11a}$$

$$\theta = \begin{cases} FlunkTrust & \text{if } \theta \leq 0.6 \\ Trustworthy & \text{if } \theta \geq 0.7 \end{cases} \tag{11b}$$

If a node satisfies the threshold value, it is allowed to communicate and transmit monitoring details to hospitals/doctors. If the trust degree of a particular node is less than the minimum requirement, the node cannot communicate and is not allowed to exchange or share information. Furthermore, at the end of communication, the edge node will evaluate the friendliness to determine whether the process of trust degree evaluation should be time-driven or event-driven in the future. This classification is evaluated in Section 3.3.

3.6. Recommendation-Based Indirect Trust

Recommendation-based trust evaluation is an important factor when a node wants to communicate or take services. Furthermore, there are several nodes that do not have previous observations or experience to evaluate trustworthiness. Recommendation-based trust evaluation provides a way to evaluate trust degree by requesting input from neighboring nodes.

EdgeTrust utilizes recommendations when no previous observations are available. To gather recommendations, the node broadcasts requests to surrounding nodes with the node's unique ID to share stored observations. After receiving the recommendations, EdgeTrust develops trust by applying a summation function and then comparing the result with a threshold for decision-making. In the case of indirect trust, the threshold is different from the threshold used for direct trust evaluation. In recommendation-based evaluation, nodes are required to maintain a minimum trust degree of 0.9 to be considered trustworthy. The conditions for decision-making are illustrated by Equation (12):

$$\theta = t^{rt}_{exp_{e_i \to e_j}} \tag{12a}$$

$$\theta = \begin{cases} FlunkTrust & \text{if } \theta \leq 0.8 \\ Trustworthy & \text{if } \theta \geq 0.9 \end{cases} \tag{12b}$$

4. Results and Discussion

In this section, we elaborate on the performance evaluation of the proposed model in comparison with existing schemes. We used an open-source library (Zetta [41,42]) to create a central authority and the IoTivity library [43] to enable inter-object connectivity. Wireless communication is performed using Zigbee (IEEE 802.15) [44]. The complete simulation setup is given in Table 2. We performed comparative analysis using several existing mechanisms: TMEI [45], RobustD [31], and SGSQ-TM [46].

The simulation was performed under different scenarios and attacks by varying the number of network nodes. During the simulation, the number of varying nodes was 50 to 400, and the percentage of malicious and compromised nodes was 35 to 45. The simulation time (t) was also varied between 600 to 1100 minutes (m), with time-based friendliness being performed when the number of sessions created between nodes was 50 or more. For newly joined nodes, the default trust degree was 0.6, while for old nodes, the flunk/no trust was 0.0 to 0.6. A trust degree of 0.7 to 1 was considered trustworthy.

Table 2. Parameters and simulation setup.

Parameters	Value
Area of Network	300 (m^2)
No. of Nodes	400∼600
Simulation Time	600∼1100
Trust Degree	0.0-1
MAC	IEEE 802.11
Transmission Rate	3∼5 Mbps
Size of Packet	20∼30
Peak Transmission Range	323 (m)
Node Placement	Uniform
Maximum Connection	11

4.1. Aggregated Trust Evaluation

Trust aggregation is a process in which certain nodes evaluate the trust degree by using the previous trust and current trust to formulate an absolute trust degree for decision-making. In the proposed mechanism, nodes rank the performance of a particular node after obtaining the services, known as experience, and use that for aggregation purposes in future trust evaluation. We evaluated the impact of experience trust aggregation under two different scenarios in which trust computation is performed by nodes with or without experience aggregation, as illustrated in Figure 3. The figure shows the comparative analysis of trustworthy TWP (Trust with Previous) and trustworthy TNP (Trust with no Previous) observations. The trust evaluation of the trustworthy node with aggregation formulates a stable result and enhances accuracy, while the trust without aggregation illustrates a wavered trust degree over a time interval (t). In the second scenario, we performed an identical evaluation on the trust degree of malicious or compromised nodes, and the result showed similar outcomes in which Flunk TWP (Trust with Previous) represented a uniform trust degree and Flunk TNO (Trust with no Previous) showed notable inconstancy in the trust degree and also assigned a higher trust degree, highlighting the significance of employing previous experience in the proposed approach.

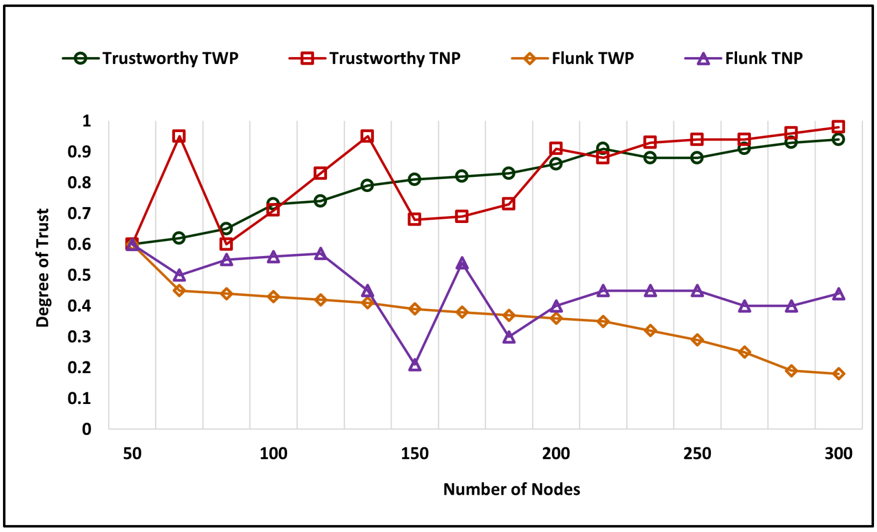

Figure 3. The impact of aggregated trust computation.

4.2. Honest and Dishonest Trust Accuracy

The accuracy of the honest and dishonest trust evaluation is determined by comparing the outcomes of the actual and computed trust degree by the model after the training phase. The simulation was performed to evaluate the trust degree of honest and dishonest nodes, with the comparative analysis illustrated by Figures 4 and 5. The simulation time for the honest and dishonest accuracy evaluation was 300 seconds, with the minimum trust being 0.0 and the maximum trust being 1. The comparative analysis of the computed and actual trust degree of honesty is represented by Figure 4, which shows that the model took 147 seconds to evaluate the actual trust. During the evaluation of the dishonest trust degree, it took 162.5 seconds to remove the difference between computed and actual trust for accurate computations, as illustrated in Figure 5.

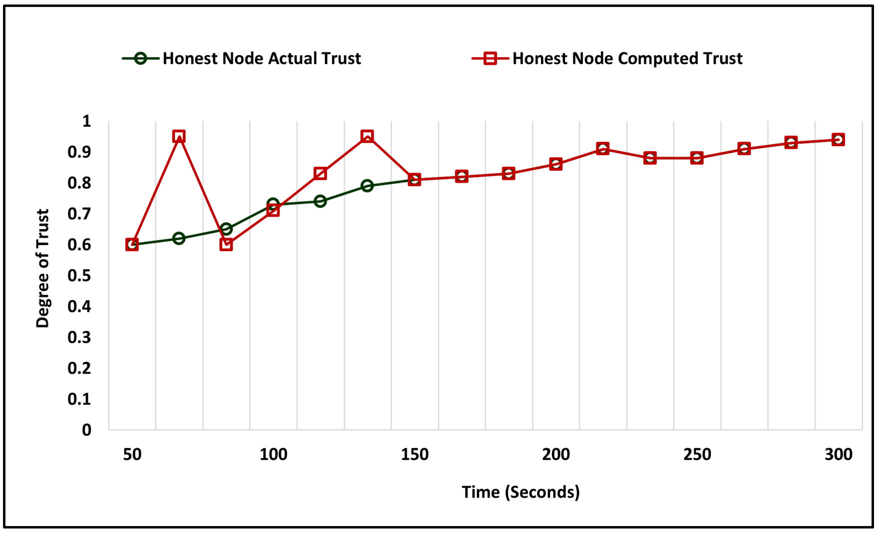

Figure 4. Honest node’s trust degree accuracy.

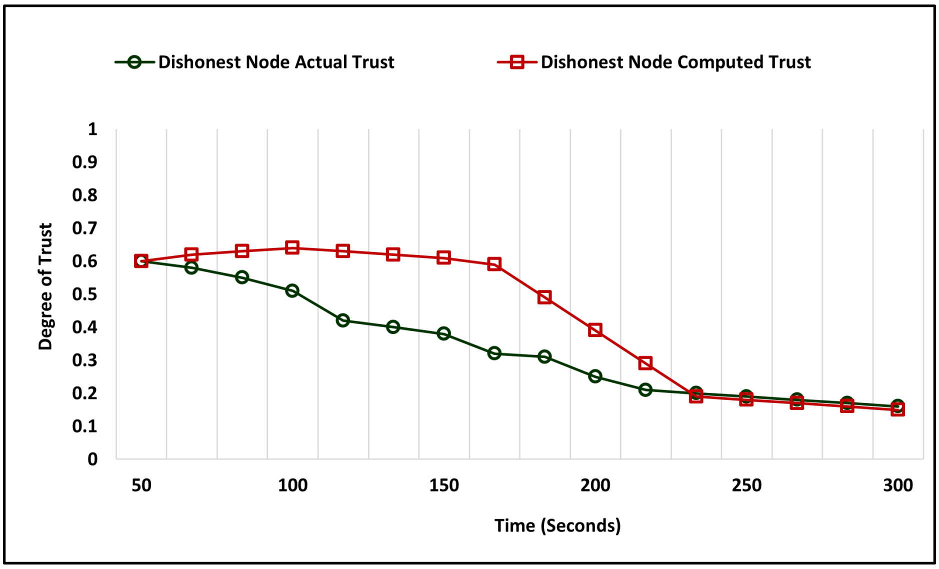

Figure 5. Dishonest node's trust degree accuracy.

4.3. On-Off Attack

The on-off attack is one of the most serious attacks in the IoT heterogeneous environment, where good nodes may become malicious or compromised at any time. It is important to distinguish such nodes that maintain a higher trust degree and whose neighboring nodes also assign a higher rank as an experience, but become malicious after a certain period of time. These nodes may also be compromised by different attacks, making it crucial to recognize these nodes in order to maintain security and privacy. We evaluated the performance of existing approaches under two distinct scenarios by varying the percentage of malicious nodes and time (t).

In the first scenario of an on-off attack, the number of nodes varied from 50 to 400, with a percentage of malicious and compromised nodes at 35%. The simulation time was 600 minutes. Figure 6 shows the simulation outcomes of on-off attack scenario-1, illustrating the performance comparison in which the proposed mechanism successfully recognized the execution and assigned a lower/flunk trust degree as the nodes became malicious after a certain time interval. Initially, the proposed mechanism assigned the default trust degree to nodes with no past experience, and assigned an increasing trust degree at different points that reached 0.64 at point-5, before dropping to 0.55 and then to the lowest trust of 0.01. In the second scenario (Figure 7), the number of nodes was the same as in the previous scenario, and the percentage of malicious nodes increased to 45%. The simulation time was 1100 minutes, with a threshold of 0.0 to 1, and trust was computed with aggregated past experience. The increase in malicious and compromised nodes clearly had an impact on the simulation, and the trust computation assigned to these nodes was lower from the beginning and reached a minimum of 0.25 at the end. In both scenarios, the proposed EdgeTrust mechanism assigned a lower trust degree, indicating the effectiveness of the trust parameters along with the experience component of trust. Therefore, it successfully recognized the on-off attack.

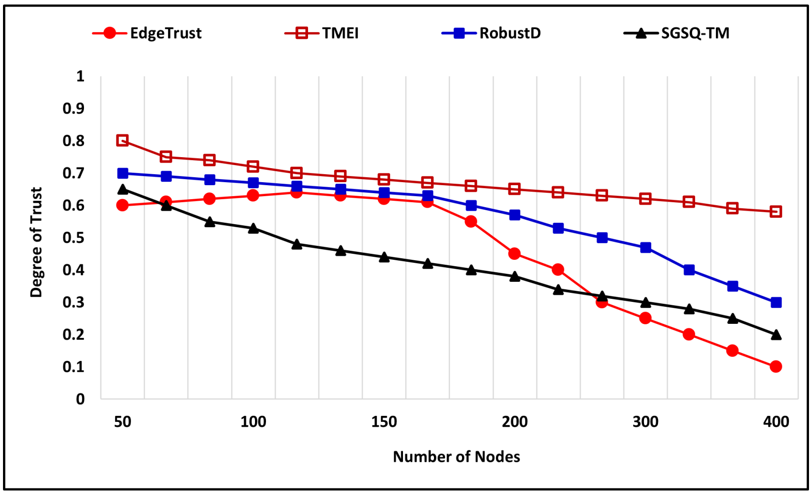

Figure 6. On-off attacks (Scenario-1).

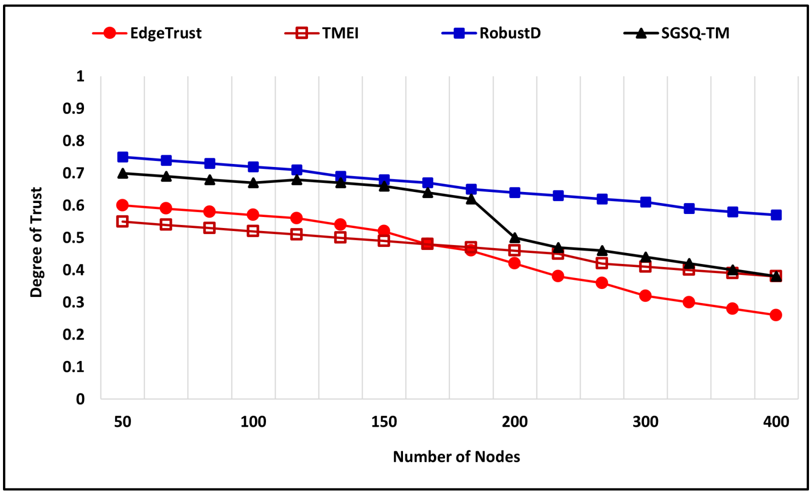

Figure 7. On-off attacks (Scenario-2).

4.4. Self Promoting Attack

It is a kind of attack in which nodes try to promote themselves either alone or in groups to provide the services. The successful execution of a self-promoting attack can have severe consequences that may compromise privacy by gaining access to private and sensitive information. To evaluate the performance of the proposed approach with existing approaches, we have considered two different scenarios in which nodes try to execute a self-promoting attack in different ways. In the first scenario of a self-promoting attack, nodes try to promote themselves alone with any support from the surrounding where the number of nodes is 400 along with varying self-promoting nodes, and the simulation time is 600 (m).

In the first scenario, the total number of nodes is 400 with the percentage of self-promoting nodes being 35%. These nodes self-promote themselves alone and do not have any supporting nodes, where the simulation time consists of 600 (m) with default trust being 0.6 for new nodes, flunk trust is 0.0–0.6, and supreme trust is 0.7–1. Figure 8 illustrates the simulation outcomes of the self-promoting attack in scenario 1, wherein the proposed mechanism assigns the trust degree of 0.86, and the trust degree decreases to reach 0.2, which shows the successful identification of self-promoting nodes. Furthermore, the SGSQ-TM [46] also shows effective performance and assigns a low trust degree, i.e, 0.5. In the second scenario, the total number of nodes is 400 with 45% self-promoting nodes where the simulation time is 600 (m). In this scenario, the self-promoting attack executes in a group, which means a bundle of nodes works in parallel to promote a particular node by assigning a higher fake trust degree. Figure 9 illustrates the simulation outcomes in comparison with the existing approaches, and the results show that the proposed mechanism successfully identifies the malicious nodes and assigns the flunk trust degree of 0.18. Whereas the existing approaches also identify and assign low trust degrees, such as TMEI assigning a lower trust degree of 0.6, RobustD and SGSQ-TM assign a lower trust degree of 0.4 and 0.23, respectively.

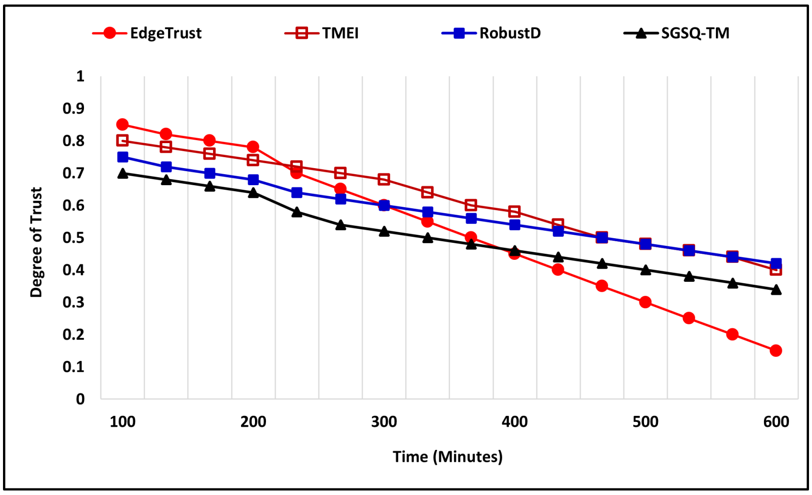

Figure 8. Self-promoting attacks (Scenario-1).

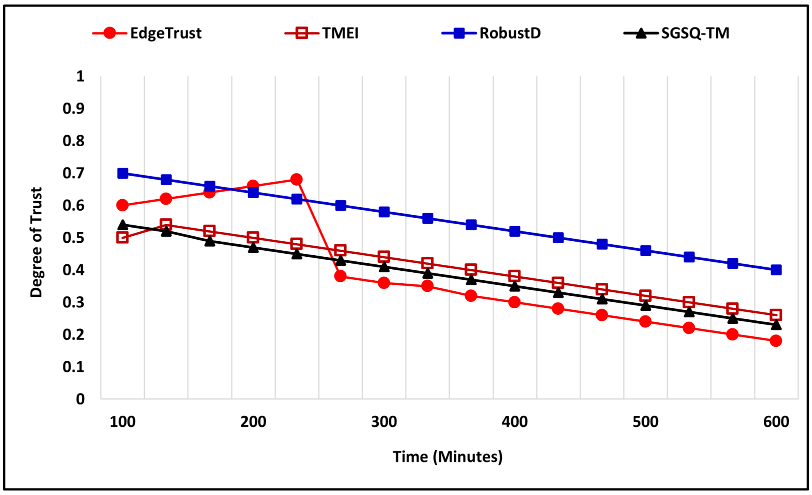

Figure 9. Self-promoting attacks (Scenario-2).

4.5. Good and Bad Mouthing Attacks

Good and Bad mouthing attacks are similar to self-promoting attacks, but in these attacks, nodes do not work together to promote themselves. The good and bad-mouthing attacks are executed by malicious nodes to assign a lower trust degree to the trustworthy nodes called bad-mouthing, while they can assign a higher trust degree to malicious nodes known as a good-mouthing attack. The chances of successful execution of this attack increase when nodes rely on recommendation-based trust evaluation. In the proposed mechanism, the utilization of recommendations is minimal, whereas the central authorities provide the recommendation that has been evaluated based on direct observation. To evaluate the effectiveness of utilizing direct trust-based evaluation as a recommendation, we have performed extensive simulations against good and bad-mouthing attacks under different scenarios. The performance of the proposed approach in comparison to the existing ones is evaluated under two different scenarios for each good and bad-mouthing attack by applying the variation to the number of trustworthy and malicious nodes.

In Figures 10 and 11, the X-axis of the graph shows the simulation time, whereas the Y-axis represents trust, which is computed and assigned at a particular time. In the first scenario of the good mouthing attack, the number of nodes is 600 where the percentage of malicious nodes is 35. Figure 10 illustrates the performance of the proposed mechanism, which shows the trust degree to reach 0.9. After the identification of a good mouthing attack, the trust degree declines to 0.7, and later on, the trust degree assigned by the EdgeTrust declines to flunk trust of 0.4. In comparison, the TMEI and RobustD also show a notable performance and assign a lower trust degree, i.e., 0.4, and 0.5, respectively. In the second scenario of good mouthing evaluation, the number of nodes increases to 800 where the percentage of malicious and compromised nodes is 45, and the simulation time is 600 (m). Figure 11 illustrates the simulation outcomes of the second scenario. In comparison with the first scenario, the result is more fluctuated than what happened due to the percentage ratio of malicious or compromised nodes. When the number of nodes increases and numerous nodes try to execute an attack, then the trust fluctuates between higher and lower degrees. In the second scenario of good mouthing evaluation, the proposed mechanism initially assigns a higher trust degree up to 3 points and then it falls to 0.2 at point 4. Looking at both scenarios, the EdgeTrust assigns the lowest trust to malicious nodes and detects the trustworthy nodes.

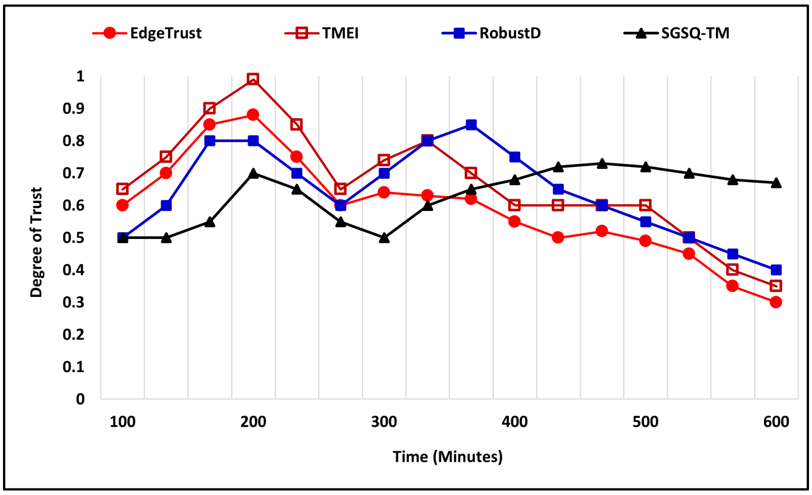

Figure 10. Good mouthing attacks with varying nodes (Scenario-1).

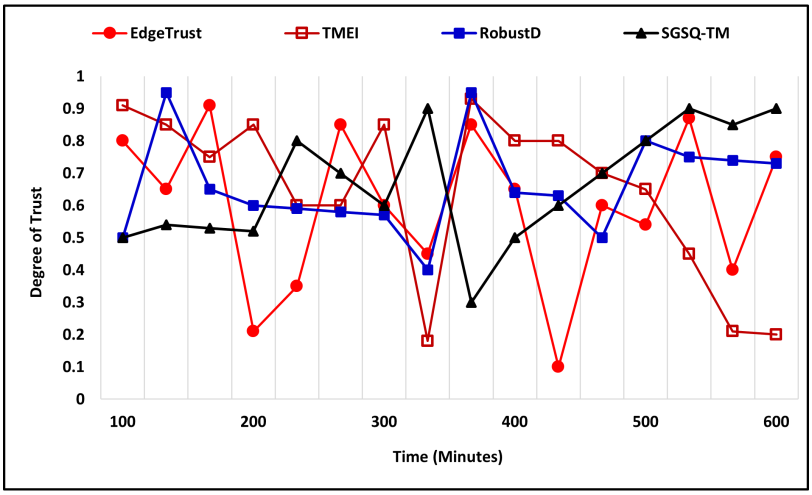

Figure 11. Good mouthing attacks with varying nodes (Scenario-2).

The bad-mouthing attack is also evaluated under two different scenarios by applying variation to the number of total nodes along with the percentage ratio of malicious and compromised nodes. In the first scenario of a bad-mouthing attack, the number of nodes is 400, where the percentage ratio of malicious nodes is 35%, and the simulation time is 600 (m). Figure 12 shows the simulation outcome in which malicious nodes try bad-mouthing trustworthy nodes by assigning a low trust degree while the increasing trust graph of the proposed approach clearly shows that it successfully recognizes the attack and assigns a higher trust degree to the nodes. The proposed EdgeTrust approach initially assigns a lower degree of trust, i.e., 0.3, but later it reaches 0.9, which is the highest trust degree. Furthermore, the existing approaches also show a notable performance against the attack and assign a higher trust degree to the trustworthy nodes. In the second scenario, the total number of nodes is 400, where the malicious and compromised nodes that execute the attack are 45%, and the simulation time is 600 (m). Figure 13 illustrates the comparative performance analysis of the proposed mechanism along with existing approaches. The EdgeTrust approach begins by assigning a default trust degree that increases with time and reaches 0.9, which is the highest trust degree. In comparison, the SGSQ-TM approach also manifests an effective performance and keeps the trust degree of trustworthiness higher, which is 0.4 in the beginning and reaches 0.7. The performance of TMEI is stable and assigns a higher trust degree, whereas the performance of RobustD assigns a lower trust degree, i.e., 0.2, but begins by assigning a higher trust degree after 450 (m) that reaches 0.5.

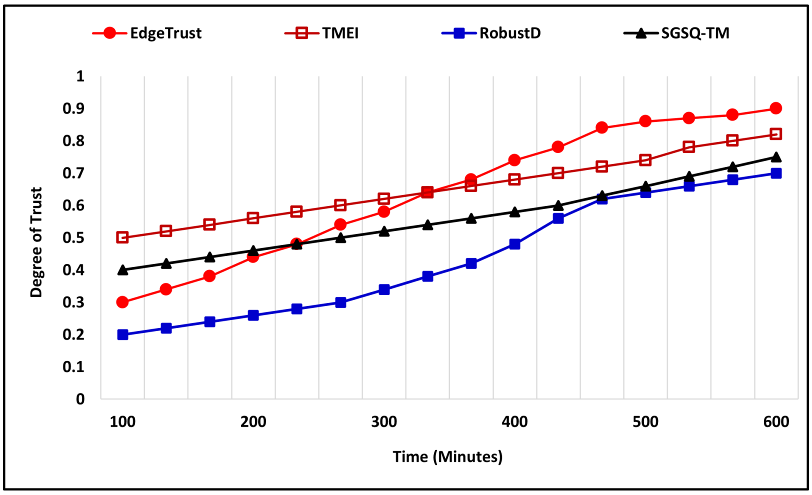

Figure 12. Bad mouthing attacks in Scenario-1.

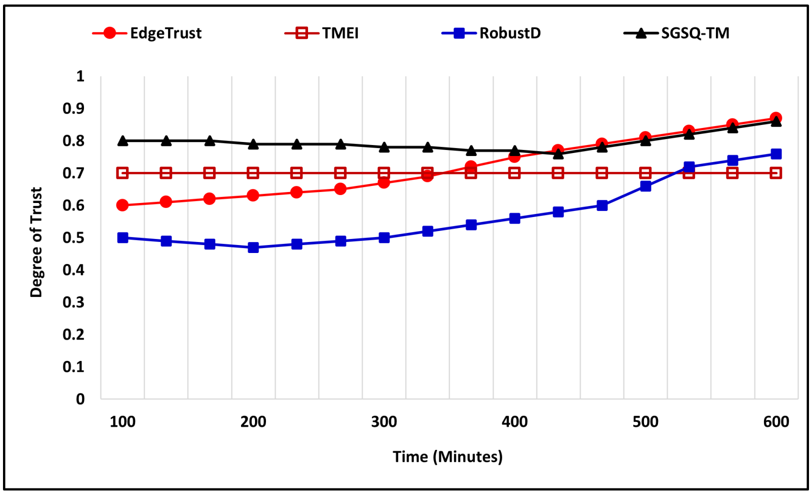

Figure 13. Bad mouthing attacks in Scenario-2.

4.6. Energy Consumption Evaluation

Communication and computation consume a notable amount of energy in IoT, and it is important to propose such approaches that consume less energy to make the implementation of green IoT possible in a real-world scenario. We have evaluated the energy consumption of proposed approaches with existing approaches by applying the variation to the total number of nodes, and the energy consumption is measured in Joules (J). We evaluated the energy consumption of the proposed mechanism with a fixed number of nodes by applying variations to the total time (t). Figure 14 illustrates the simulation which has been performed with 100, 200, up to 600 nodes, where the maximum energy consumed by the proposed approach at 1100 (m) is 240 (J) with 400 nodes, 270 (J) with 500 nodes, and 300 (J) with 600 nodes. The average energy consumption has also been evaluated with varying total numbers of nodes where the simulation time is 1100 (m). Figure 15 illustrates the energy consumption of the approaches that show that the proposed approach has utilized less energy to perform trust computation, whereas, in comparison, RobustD and TMEI use average consumption while SGSQ-TM approaches use a higher amount of energy to perform their computations. The maximum energy consumption of approaches with 600 nodes at 1100 (m) is 360 (J) of EdgeTrust, 450 (J) of TMEI, 400 (J) of RobustD, and 520 (J) of SGSQ-TM. The simulation outcomes of average consumption make the proposed approaches a better way to maintain security among IoT nodes.

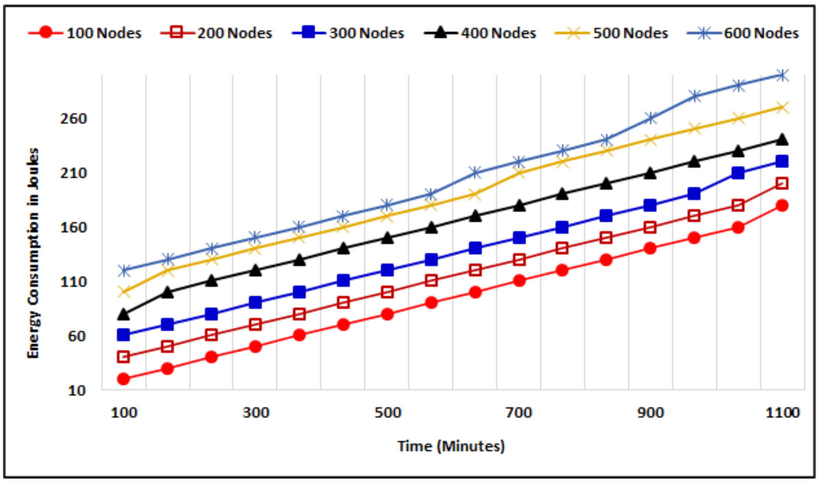

Figure 14. Energy consumption with varying nodes.

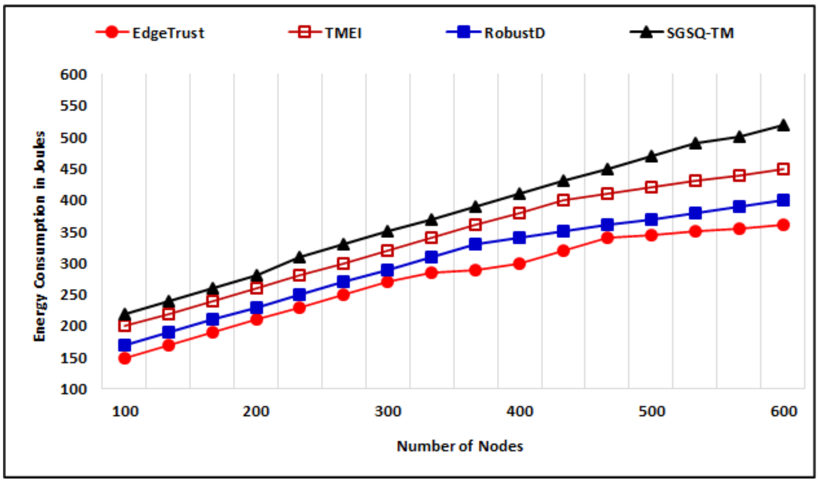

Figure 15. Average energy consumption comparison.

5. Conclusions

Internet of Things (IoT) provides diverse opportunities to the real world to improve daily life by making autonomic devices, which are intelligent and can perform the required operations and given tasks. Healthcare 4.0 and IoT can enhance the facilities provided to patients in remote areas. The monitoring of patients may help to save them in a critical situation. In healthcare 4.0, patients' details are transmitted to the hospital needed to maintain integrity and security. The proposed mechanism addresses the requirements of a lightweight approach to maintain security among nodes. The proposed mechanism utilizes trust parameters and central authority to manage and provide trust observations. The proposed mechanism combines the concept of distributed and centralized trust management along with time-driven and event-driven trust computations. We have also evaluated the performance of the proposed approach with existing approaches among several potential attacks. The extensive simulation outcomes show that EdgeTrust can recognize IoT's possible attacks to maintain a robust environment. In comparison, the proposed approach assigns a lower degree of trust, i.e., 0.25 and 0.18 in the self-promoting attack. Furthermore, EdgeTrust also identifies the good-mouthing instantly and maintains the lower trust degree, whereas, in the case of SGSQ-TM, malicious nodes regain the trustworthiness. Another notable challenge addressed is the lightweight approach that requires less energy consumption, which makes it suitable for the real-world scenario. In the future, the proposed mechanism can be extended by evaluating the storage challenges that the edge nodes may face and formulating a two-way approach to maintain hospital-side trust management.

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

Funding: This work was supported by the Deanship of Scientific Research at King Saud University, Riyadh, Saudi Arabia, through the Vice Deanship of Scientific Research Chairs: Chair of Cyber Security.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

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

References

1. Din, I.U.; Asmat, H.; Guizani, M. A review of information centric network-based internet of things: Communication architectures, design issues, and research opportunities. *Multimed. Tools Appl.* **2019**, *78*, 30241–30256. [CrossRef]
2. 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]
3. Gulzar, M.; Abbas, G. Internet of Things security: A survey and taxonomy. In Proceedings of the 2019 International Conference on Engineering and Emerging Technologies (ICEET), Lahore, Pakistan, 21–22 February 2019; pp. 1–6.
4. Yan, Z.; Zhang, P.; Vasilakos, A.V. A survey on trust management for Internet of Things. *J. Netw. Comput. Appl.* **2014**, *42*, 120–134. [CrossRef]
5. Qu, C.; Tao, M.; Yuan, R. A hypergraph-based blockchain model and application in Internet of Things-enabled smart homes. *Sensors* **2018**, *18*, 2784.
6. Guo, Y.; Wang, N.; Xu, Z.Y.; Wu, K. The internet of things-based decision support system for information processing in intelligent manufacturing using data mining technology. *Mech. Syst. Signal Process.* **2020**, *142*, 106630. [CrossRef]
7. Shafique, K.; Khawaja, B.A.; Sabir, F.; Qazi, S.; Mustaqim, M. Internet of things (IoT) for next-generation smart systems: A review of current challenges, future trends and prospects for emerging 5G-IoT scenarios. *IEEE Access* **2020**, *8*, 23022–23040. [CrossRef]
8. Diène, B.; Rodrigues, J.J.; Diallo, O.; Ndoye, E.H.M.; Korotaev, V.V. Data management techniques for Internet of Things. *Mech. Syst. Signal Process.* **2020**, *138*, 106564. [CrossRef]
9. Tseng, L.; Yao, X.; Otoum, S.; Aloqaily, M.; Jararweh, Y. Blockchain-based database in an IoT environment: Challenges, opportunities, and analysis. *Clust. Comput.* **2020**, *23*, 2151–2165. [CrossRef]

10. Ephzibah, E.; Dharinya, S.S.; Remya, L. Decision Making Models Through AI for Internet of Things. In *Internet of Things for Industry 4.0*; Springer: Berlin/Heidelberg, Germany, 2020; pp. 57–72.
11. Hui, H.; Zhou, C.; Xu, S.; Lin, F. A novel secure data transmission scheme in industrial internet of things. *China Commun.* **2020**, *17*, 73–88. [CrossRef]
12. Sicari, S.; Rizzardi, A.; Coen-Porisini, A. 5G in the Internet of Things era: An overview on security and privacy challenges. *Comput. Netw.* **2020**, *179*, 107345. [CrossRef]
13. Sharif, A.; Ouyang, J.; Yang, F.; Chattha, H.T.; Imran, M.A.; Alomainy, A.; Abbasi, Q.H. Low-cost inkjet-printed UHF RFID tag-based system for internet of things applications using characteristic modes. *IEEE Internet Things J.* **2019**, *6*, 3962–3975. [CrossRef]
14. Wu, F.; Wu, T.; Yuce, M.R. An internet-of-things (IoT) network system for connected safety and health monitoring applications. *Sensors* **2019**, *19*, 21. [CrossRef]
15. Singh, B. The Internet of Things: A Vision for Smart World. In *Advances in Signal Processing and Communication*; Springer: Berlin/Heidelberg, Germany, 2019; pp. 165–172.
16. Janjua, K.; Shah, M.A.; Almogren, A.; Khattak, H.A.; Maple, C.; Din, I.U. Proactive Forensics in IoT: Privacy-Aware Log-Preservation Architecture in Fog-Enabled-Cloud Using Holochain and Containerization Technologies. *Electronics* **2020**, *9*, 1172. [CrossRef]
17. Khan, M.A.; Din, I.U.; Jadoon, S.U.; Khan, M.K.; Guizani, M.; Awan, K.A. G-RAT | A novel graphical randomized authentication technique for consumer smart devices. *IEEE Trans. Consum. Electron.* **2019**, *65*, 215–223. [CrossRef]
18. Gong, X.; Feng, T.; Albettar, M. PEASE: A PUF-Based Efficient Authentication and Session Establishment Protocol for Machine-to-Machine Communication in Industrial IoT. *Electronics* **2022**, *11*, 3920. [CrossRef]
19. 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]
20. Awan, K.A.; Ud Din, I.; Almogren, A.; Almajed, H. AgriTrust—A Trust Management Approach for Smart Agriculture in Cloud-based Internet of Agriculture Things. *Sensors* **2020**, *20*, 6174. [CrossRef]
21. Awan, K.A.; Din, I.U.; Almogren, A.; Almajed, H.; Mohiuddin, I.; Guizani, M. NeuroTrust-Artificial Neural Network-based Intelligent Trust Management Mechanism for Large-Scale Internet of Medical Things. *IEEE Internet Things J.* **2020**, *8*, 15672–15682. [CrossRef]
22. Almogren, A.; Mohiuddin, I.; Din, I.U.; Al Majed, H.; Guizani, N. FTM-IoMT: Fuzzy-based Trust Management for Preventing Sybil Attacks in Internet of Medical Things. *IEEE Internet Things J.* **2020**, *8*, 4485–4497. [CrossRef]
23. Haseeb, K.; Almogren, A.; Ud Din, I.; Islam, N.; Altameem, A. SASC: Secure and Authentication-Based Sensor Cloud Architecture for Intelligent Internet of Things. *Sensors* **2020**, *20*, 2468. [CrossRef]
24. García-García, L.; Jiménez, J.M.; Abdullah, M.T.A.; Lloret, J. Wireless technologies for IoT in smart cities. *Netw. Protoc. Algorithms* **2018**, *10*, 23–64. [CrossRef]
25. Tortorella, G.L.; Fogliatto, F.S.; Esposto, K.F.; Mac Cawley Vergara, A.; Vassolo, R.; Tlapa Mendoza, D.; Narayanamurthy, G. Measuring the effect of Healthcare 4.0 implementation on hospitals' performance. *Prod. Plan. Control* **2022**, *33*, 386–401. [CrossRef]
26. Galletly, C.L.; Barreras, J.L.; Lechuga, J.; Glasman, L.R.; Cruz, G.; Dickson-Gomez, J.B.; Brooks, R.A.; Ruelas, D.M.; Stringfield, B.; Espinoza-Madrigal, I. US public charge policy and Latinx immigrants' thoughts about health and healthcare utilization. *Ethn. Health* 2022, 1–18, *online ahead of print*.
27. Sony, M.; Antony, J.; McDermott, O. The Impact of Healthcare 4.0 on the Healthcare Service Quality: A Systematic Literature Review. *Hosp. Top.* 2022, 1–17. *online ahead of print*.
28. Gardas, B.B. Organizational hindrances to Healthcare 4.0 adoption: An multi-criteria decision analysis framework. *J. Multi-Criteria Decis. Anal.* **2022**, *29*, 186–195. [CrossRef]
29. Mahajan, H.B.; Rashid, A.S.; Junnarkar, A.A.; Uke, N.; Deshpande, S.D.; Futane, P.R.; Alkhayyat, A.; Alhayani, B. Integration of Healthcare 4.0 and blockchain into secure cloud-based electronic health records systems. *Appl. Nanosci.* 2022, 1–14. *online ahead of print*.
30. Azad, M.A.; Bag, S.; Hao, F.; Shalaginov, A. Decentralized self-enforcing trust management system for social Internet of Things. *IEEE Internet Things J.* **2020**, *7*, 2690–2703. [CrossRef]
31. Esposito, C.; Tamburis, O.; Su, X.; Choi, C. Robust Decentralised Trust Management for the Internet of Things by Using Game Theory. *Inf. Process. Manag.* **2020**, *57*, 102308. [CrossRef]
32. 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]
33. Kouicem, D.E.; Imine, Y.; Bouabdallah, A.; Lakhlef, H. A Decentralized Blockchain-Based Trust Management Protocol for the Internet of Things. *IEEE Trans. Dependable Secur. Comput.* **2020**, *19*, 1292–1306. [CrossRef]
34. Khan, Z.A. Using energy-efficient trust management to protect IoT networks for smart cities. *Sustain. Cities Soc.* **2018**, *40*, 1–15. [CrossRef]
35. Khattak, H.A.; Tehreem, K.; Almogren, A.; Ameer, Z.; Din, I.U.; Adnan, M. Dynamic pricing in industrial internet of things: Blockchain application for energy management in smart cities. *J. Inf. Secur. Appl.* **2020**, *55*, 102615. [CrossRef]
36. Siddiqua, A.; Shah, M.A.; Khattak, H.A.; Din, I.U.; Guizani, M. ICAFE: Intelligent congestion avoidance and fast emergency services. *Future Gener. Comput. Syst.* **2019**, *99*, 365–375. [CrossRef]

37. Caminha, J.; Perkusich, A.; Perkusich, M. A smart middleware to detect on-off trust attacks in the Internet of Things. In Proceedings of the 2018 IEEE International Conference on Consumer Electronics (ICCE), Las Vegas, NV, USA, 12–14 January 2018.
38. Chen, J.I.Z. Embedding the MRC and SC Schemes into Trust Management Algorithm Applied to IoT Security Protection. *Wirel. Pers. Commun.* **2018**, *99*, 461–477. [CrossRef]
39. Mukherjee, S.; Sharma, N. Intrusion detection using naive Bayes classifier with feature reduction. *Procedia Technol.* **2012**, *4*, 119–128. [CrossRef]
40. Rish, I. An empirical study of the naive Bayes classifier. In Proceedings of the IJCAI 2001 Workshop on Empirical Methods in Artificial Intelligence, Seattle, WA, USA, 4–6 August 2001; Volume 3, pp. 41–46.
41. Triantafyllou, A.; Sarigiannidis, P.; Lagkas, T.D. Network protocols, schemes, and mechanisms for internet of things (iot): Features, open challenges, and trends. *Wirel. Commun. Mob. Comput.* **2018**, *2018*, 5349894. [CrossRef]
42. Zinca, D.; Popa, M.O. Development of a ZettaJS driver for the ESP8266 IoT hardware. In Proceedings of the 2018 International Symposium on Electronics and Telecommunications (ISETC), Timișoara, Romania, 8–9 November 2018; pp. 1–4.
43. Elsayed, K.; Ibrahim, M.A.B.; Hamza, H.S. Service discovery in heterogeneous IoT environments based on OCF/IoTivity. In Proceedings of the 2019 15th International Wireless Communications & Mobile Computing Conference (IWCMC), Tangier, Morocco, 24–28 June 2019; pp. 1160–1165.
44. Gočal, P.; Macko, D. EEMIP: Energy-efficient communication using timing channels and prioritization in ZigBee. *Sensors* **2019**, *19*, 2246. [CrossRef]
45. Qureshi, K.N.; Iftikhar, A.; Bhatti, S.N.; Piccialli, F.; Giampaolo, F.; Jeon, G. Trust management and evaluation for edge intelligence in the Internet of Things. *Eng. Appl. Artif. Intell.* **2020**, *94*, 103756. [CrossRef]
46. Das, R.; Singh, M.; Majumder, K. SGSQoT: A community-based trust management scheme in Internet of Things. In Proceedings of the International Ethical Hacking Conference, Kolkata, India 31 March–1 April 2018; pp. 209–222.

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.