EdgeTrust - A Lightweight Data-centric Trust Management Approach for Green Internet of Edge Things

Kamran Ahmad Awan
The University of Haripur

Ikram Ud Din (ikramuddin205@yahoo.com)
The University of Haripur https://orcid.org/0000-0001-8896-547X

Ahmad Almogren
King Saud University

Hasan Ali Khattak
NUST: National University of Sciences and Technology

Joel J.P.C. Rodrigues
Federal University of Piaui: Universidade Federal do Piaui

Research Article

Keywords: Internet of Things, Trust Management, Machine Learning, Deep Neural Networks, Malicious Nodes, IoT Attacks, Security, Privacy Preservation.

DOI: https://doi.org/10.21203/rs.3.rs-453986/v1

License: This work is licensed under a Creative Commons Attribution 4.0 International License. Read Full License
Abstract Internet of Things (IoT) is bringing revolution into 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 as it provides autonomy to nodes that they can communicate among other nodes and can also exchange information at any period. Due to the heterogeneous environment, IoT faces numerous security and privacy challenges, and one of the most significant challenges is the identification of malicious and compromised nodes. In this article, we have proposed a Machine Learning-based trust management approach for edge nodes. The proposed approach is a lightweight process to evaluate trust because edge nodes cannot perform complex computations. To evaluate trust, the proposed mechanism utilizes the knowledge and experience component of trust where knowledge is further based on several parameters. To eliminate the triumphant 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 worthiness of nodes is ranked between a certain limit where only those that satisfy the threshold value can participate in the network. To validate the performance of a proposed approach we have performed an extensive simulation in comparison with the existing approaches and the result shows the effectiveness of the proposed approach against several potential attacks.

Keywords Internet of Things; Trust Management; Machine Learning; Deep Neural Networks; Malicious Nodes; IoT Attacks; Security; Privacy Preservation.

1 Introduction

Internet of Things [21] consists of diverse standards of nodes in a heterogeneous environment connected with the Internet to communicate and exchange information in the network [18, 22]. 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 [16, 29]. The generic architecture of IoT consists of multiple layers, i.e., business, application, middleware, and perception layers [63], which are illustrated in Figure 1. The business layer contains system management solutions that may be varied according to the requirements [48, 62]. The middleware layer is the most critical layer that consists of information processing [30], ubiquitous computing [52], services management [20], databases [59, 64], and decision units [24]. The information processing unit processes the incoming information to formulate the result while ubiquitous computing is utilized to provide the output in the most reliable method. The network layer consists of transmission networks that provide a source by which IoT participating nodes can transmit information among them [34, 43, 44]. These transmission connections will be 4G, 5G, etc. [55]. The perception layer consists of edge nodes that can be
RFID [53], sensors [61], or any physical object [57]. In [63], 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 [36], e.g., authentication [3, 31, 37, 38], access control [47, 60], trust management in cross domain along with smart edge nodes [6, 7, 9, 11, 33], security management in IoT equipped with VANET nodes [10, 27, 35, 45], policy enforcement [54], secure middleware [13], and confidentiality [50].

Due to the heterogeneous environment of IoT, it is significant to implement robust approaches that maintain a secure environment by eliminating malicious nodes and also robust enough to keep resilience towards several potential attacks [4, 8, 32]. Trust is proposed as the most prominent lightweight mechanism that helps to maintain a secure environment by utilizing parameters. Nodes that maintain the high trust values are known as trustworthy nodes where nodes with the least trust value are the inadequate nodes. There are two approaches proposed to implement the trust approaches which are distributed and centralized trust management. In distributed trust management, each node is responsible to evaluate and manages trust that raises the vulnerability of self-promoting attack, non-repudiation. Further, another significant drawback of distributed trust management is that the nodes with fewer capabilities are not capable to perform such computation to maintain resilience towards centralized. In contrast, centralized trust management consists of a central authority that manages the trust of network nodes and the major drawback of these approaches is that if the central authority gets compromised then the whole network becomes vulnerable to attacks. 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. 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 is 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 does not require to generate the request to neighboring nodes as the recommendation is to gather by a central authority. The significant advantage of utilizing the recommendations of 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 article is 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, but a 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 elaborated the existing approaches along with their contribution and limitation to identify the research gaps.

A trust management mechanism is proposed for the Social IoT that maintain the trust by self-enforcing in a decentralized manner [12]. The study stated that it is significant to address the challenges of secure information sharing because sharing of information with malicious and compromised nodes can cause serious threat. The proposed mechanism utilizes the decentralized homomorphic encryption. The proposed mechanism architecture consists of multiple IoT devices owned by a numerous users which interact with other on particular time interval. After 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 database that contain all the feedback of the nodes. However, decentralized database can cause data integrity challenges as it is shared and stored without utilizing any central authority. Another trust management mechanism is proposed for IoT edge intelligence. The study stated that the IoT consist of complex network and the security is one of the significant challenges that required to addressed. The proposed addresses the challenges with an evaluation mechanism based on cumulative trust where the trust is computed by utilizing the direct and indirect trust. The proposed model consists of 5-tier which are attack model, trust and behaviour analysis, additive metric function, decision making module and predictable module. The trust parameters use in this approach are packet send and received, time of packet send and receive, packet drop ratio and data rate where the trust evaluation also involves the reputation factor to evaluate cumulative trust. The major contribution of the proposed mechanism is the formulation of cumulative trust. However, to validate the performance of utilized parameters it is also important to evaluate the proposed approach against whitewashing attack to validate it robustness against non-repudiation.

A game theory-based decentralized trust management mechanism is proposed for the IoT to maintain the robustness among nodes [25]. The proposed mechanism applies the game theory to identify nodes that are executing good
or bad mouthing attack by sending mendacious trust degree. For update trust degrees of nodes the proposed approach utilizes Dempster-Shafer theory that collected the scores for updating process by excluding disparate scores. To perform a trust computation the approach utilizes the Fuzzy Theory to classify trust into none, low up to high and definitely. The major contribution of the proposed mechanism is the utilization of Fuzzy rule to classify trust. However, the performance of the proposed mechanism is required to be evaluated against potential IoT attack such as on-off, whitewashing among others. Another trust management mechanism is proposed for the Industrial IoT to protect the sensitive and confidential data [14]. The approach proposed a hybrid architecture for Industrial IoT which consist of member, leader and relationship with centralized industrial IoT server. In 2020, a blockchain-based trust protocol is proposed for IoT which work that maintain trust in decentralized manner [41]. The study stated that IoT object can communicate and exchange information that makes the environment highly dynamic and raise security challenges significant to address for maintaining adequate robustness. The proposed mechanism is a hierarchical block-chain protocol that also supports mobility where the architecture of the proposed mechanism consists of fog layer, Private blockchain layer and an IoT layer with different clusters/ zones. In 2018, an energy-efficient trust management mechanism (EET-IoT) [39] is proposed to protect the IoT network and primarily focus on smart cities [40, 56]. The study stated that many devices may have insufficient power and limited processing power. Also, in some situation, these devices are installed where replacement of a battery is not attainable. 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 IEEE 802.14 protocol is dedicated to PAN (Personal Area Network) and able to connect multiple devices concurrently. The proposed mechanism further uses the 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 dis-belief, where $u$ denotes the uncertainty. In EET-IoT, the trust computation is evaluated by employing direct observations. Moreover, the study developed three algorithms to manage the reputation of a client. These algorithms are No-listening for Data Forwarding (NLDF), Listen-own Data Forwarding (LDF), and Listen-to-all Transmission (LT). In NLDF, the objective is to maximize the energy consumption by activating the sleep mode of a device after receiving an acknowledgment. In LDF, the algorithms employ reduced surveillance and a node supervises its parents according to RPL protocol to maximize the energy saving of the network. In LT, the algorithms collect and estimate the trust values of each neighboring nodes. The objective of collecting trust values of all neighbors is to build the reputation of each node. The evaluation of EET-IoT shows a significant decrease in the energy utilization. The energy consumption evaluation of the proposed algorithms shows that LT consumes maximum energy followed by LDE and NDLF. The authors also stated that the optimization at MAC Layer is required to overcome the adequate energy consumption.

A smart middle-ware mechanism (Smart-TM) [15] is proposed to detect on-off attacks in IoT. The study stated that on-off attacks are the most generally executed attacks. A device can misbehave and provide bad and good services randomly to maintain its degree of trust. The focus of the proposed mechanism is to automatically assess the resources

![IoT architecture with the integration of trust management](image-url)
of IoT trust by evaluating the attributes of services providers. The Smart-TM utilizes an approach of machine learning based on One-Class Support Vector Machine (OneClass-SVM) methodology. OneClass-SVM utilizes the transmitted data to evaluate the degree of trust. Furthermore, the degree of trust is estimated by examining the distance from a function of Hyper-plane model. Moreover, the middleware implements the decision function to estimate the trust and nodes with higher degree of trust are listed as trusted nodes, while nodes with lower degree of trust are classified as un-trusted 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. The machine learning approach, i.e., OneClass-SVM, also performs considerably better as compared to other classifiers. The proposed mechanism is unable to specify the framework of information gathering, trust dissemination, update, and maintenance of trust. A scheme of trust management (Tm-SecPro) [17] is proposed that adopts two methods, i.e., maximum ratios combining and selection combining. The study stated that there are several issues related to the application layer. The major challenge is to preserve adequate security to IoT devices and provide resilience against malicious attacks. In Tm-SecPro, service provider and seeker are able to communicate with each other directly and the mechanism will preserve 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 one later. 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 significant aspect of this scheme is a fusion of MRC and SC that will help to maintain the reliability of Tm-SecPro.

3 Proposed EdgeTrust Mechanism

The identification of malicious and compromised is one of the significant challenges 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 [46, 51] for the identification and classification and behavior prediction of malicious and compromised nodes [1, 42] 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 data centers layer can be formulated with the help of recommendations gather 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 where it 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 [2]. 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 5 distinct phases which are features selection, features scaling, classifier implementation, data-set 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 case of low friendliness then trust computation is performed based on events. The next phase is to scale the features in which all the features involved in computations scaled between 0.0-1.0 where 0.0 represents the lowest trust and 1.0 shows a higher trust degree. To perform the classification and prediction, we have adopted the Naive Bayes classifier because of its accuracy and utilizes less energy to perform classification due to its simplicity. After the selection of classifier, the training phase is started in which a data-set of 2700 trust values per feature is given to the classifier for learning purposes. After training the classifier performed calculations to evaluate the error difference between computed and the actual trust values to increase precision.

3.1 Data Centers & Edge Clouds

In the proposed approach, the data center layer is responsible to perform three major operations, i.e., machine learning-based prediction, direct and indirect trust observation evaluation. The data centers and edge clouds are capable of prediction based on direct observations transmitted by the nodes. These transmitted values are first stored by the central authorities and later on, they utilize the same observations to predict the behavior of edge nodes by applying the Naive Bayes Classifier. The direct trust evaluation at data center layer is a time-driven process and it has been evaluated after 90 minutes (m). When an edge node request the data center layer, then the central authorities share the already stored observations for further processes. After gathering the request the central authorities formulate the direct trust degree by utilizing Equation 1, where $d^{ob}_{t}$ represents the direct trust observation available and $ob_{n-id}^{1}$ is the number of observations transmitted by a particular node.

$$d^{ob}_{t} = \sum \left[ ob_{n-id}^{1} + ob_{n-id}^{2} + ob_{n-id}^{3} + \ldots + ob_{n-id}^{n} \right]$$  \hspace{1cm} (1)
The area coverage of central authorities is more as compared to edge trust, therefore, they also provide recommendations that have computed over a specific interval of time. The recommendation helps nodes to compute indirect trust. The recommendation-based indirect trust is formulated by using Equation 2 where $r_{c-id}$ represents the recommendation-based trust evaluation and $c-id$ represent the unique identify of a central authority that computed indirect trust.

$$ r_{c-id} = \sum \left[ rec_{r_1}^{e_i\rightarrow e_j} + rec_{r_2}^{e_i\rightarrow e_j} + ... + rec_{r_n}^{e_i\rightarrow e_j} \right] $$

### 3.2 IoT Edge Nodes

The edge nodes are those that cannot perform complex computation but significant to lighten the burden from them to increase the scalability and security of a network [5]. In the proposed EdgeTrust approach, central authorities compute the direct trust and transmit that 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 applies the summation function to the previous experience available as represented by the Equation 3, where $e_{p_{ave, absolute}}$ shows the absolute experience formulation of a node with a unique identity while $e_{p_{ave, e_j\rightarrow e_j}}$ represent the number of previous experience stored on the internal memory of edge nodes.

$$ e_{p_{ave, absolute}} = \sum \left[ e_{p_{ave}}^{e_i\rightarrow e_j} + e_{p_{ave}}^{e_i\rightarrow e_j} + ... + e_{p_{ave}}^{e_i\rightarrow e_j} \right] $$

### 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 absolute trust value for decision making. When edge nodes wants to compute the trust value of a particular node then that node transmit a trust computation request to the nearest central authority. The request generated by a particular node consist of trustee identify, trustor identify along with the previous experience trust degree computed by the edge nodes. The trust computation process is begun by first observing the friendliness of the nodes that represent the number of sessions created over a specific interval of time. If the friendliness of nodes is high then the trust is computed as time-driven that will
reduce the energy consumption of computation. The time-driven trust computation in case of higher friendliness is 60 minutes which means that nodes are not required to compute the trust-based on events, and they can utilize the same trust degree for a pre-defined time. The friendliness is computed based on the session created between particular nodes as represented in Equation 5.

\[
fr_{nid} = \begin{cases} 
  \text{timedriven} & \text{if } fr \geq 50 \\
  \text{Eventdriven} & \text{if } fr \leq 49 \\
  \text{indirecttrust} & \text{if } p_{ob} = \text{Yes} 
\end{cases} \quad (5)
\]

In Equation 5, \(fr, n,d, \) and \(tr\) represent friendliness, nodes unique identify, and trust degree, respectively where in case of direct trust when \(fr \geq 50\) then the trust is computed as time-driven and the trust is computed-based on time-driven approach when the number of session formulated between two nodes becomes Eventdriven if \(fr \leq 49\). In case of no previous observations \(p,b\), the trust is computed by gathering the recommendations from central authorities. After the evaluation of friendliness, the next phase is to compute the trust parameters that are knowledge and experience. The knowledge component of trust consists of reliability and cooperativeness that are computed by central authorities in which a particular node generates a request. In knowledge parameters, the evaluation is initiated by evaluating the reliability by gathering the pre-stored observations received by the central authorities over a while by 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.

\[
obp_{e_i \rightarrow e_j}^{rt} = ob_{n-id}^{t(e_i \rightarrow e_j)} + ob_{n-id}^{t(e_i \rightarrow e_j)} + ob_{n-id}^{t(e_i \rightarrow e_j)} + \ldots + ob_{n-id}^{t(e_i \rightarrow e_j)} \quad (6)
\]

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

\[
r_{e_i \rightarrow e_j}^{dt} = \sum_{0}^{1} \left[ obp_{e_i \rightarrow e_j}^{et} \left( ob_{n-id}^{t(e_i \rightarrow e_j)} + ob_{n-id}^{t(e_i \rightarrow e_j)} + ob_{n-id}^{t(e_i \rightarrow e_j)} + \ldots + ob_{n-id}^{t(e_i \rightarrow e_j)} \right) \right] \quad (7)
\]

In Equation 7, \(r_{e_i \rightarrow e_j}^{dt}\) represent the evaluation of reliability evaluation based on direct trust approach where \(\sum_{0}^{1}\) is the summation function that applies on the previous trust observation to formulate absolute reliability trust degree with limit of 0.0-1.0. The completion of reliability evaluation lead 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, \(obp_{e_i \rightarrow e_j}^{ct}\) represent the cooperativeness trust evaluation of edge node \(i\) towards \(j\) where \(ob_{n-id}^{ct(1-n)}\) represents the available observations utilized for the cooperativeness trust evaluation. In Equation 8b, \(c_{e_i \rightarrow e_j}^{dt}\) represent 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.

\[
\begin{align*}
&\text{(8a)} \quad obp_{e_i \rightarrow e_j}^{ct} = ob_{n-id}^{ct1} + ob_{n-id}^{ct2} + ob_{n-id}^{ct3} + \ldots + ob_{n-id}^{ctn} \\
&\text{(8b)} \quad c_{e_i \rightarrow e_j}^{dt} = \sum_{0}^{1} \left[ obp_{e_i \rightarrow e_j}^{ct} \left( ob_{n-id}^{ct1} + ob_{n-id}^{ct2} + ob_{n-id}^{ct3} + \ldots + ob_{n-id}^{ctn} \right) \right]
\end{align*}
\]

3.4 Trust Aggregation & Development

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

\[
c_{e_i \rightarrow e_j}^{et} = r_{e_i \rightarrow e_j}^{dt} + c_{e_i \rightarrow e_j}^{ct} \quad (9)
\]

In Equation 9, the \(c_{e_i \rightarrow e_j}^{et}\) represent the direct current trust evaluation of edge node \(i\) towards \(j\) where \(r_{e_i \rightarrow e_j}^{dt}\) and \(c_{e_i \rightarrow e_j}^{ct}\) 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 edge node for the aggregation of experience current trust. After receiving the parameter trust degree the edge node aggregate the experience with current trust by first formulating the previous experience observations using Equation 10.

\[
\begin{align*}
&\text{(10)} \quad c_{e_i \rightarrow e_j}^{et} = \sum_{0}^{1} \left( et_{e_i \rightarrow e_j}^{et1} + et_{e_i \rightarrow e_j}^{et2} + et_{e_i \rightarrow e_j}^{et3} + \ldots + et_{e_i \rightarrow e_j}^{etn} \right)
\end{align*}
\]
\[ f_{t_{\text{exp}}}^{d_{i \rightarrow j}} = c_{t_{\text{exp}}}^{d_{i \rightarrow j}} + t_{\text{exp}}^{d_{i \rightarrow j}} \]  

(10a)

In Equation 10a, \( t_{\text{exp}}^{d_{i \rightarrow j}} \) represent the absolute experience trust formulation process of edge node \( i \) towards \( j \) where \( c_{t_{\text{exp}}}^{d_{i \rightarrow j}} \) illustrate the number of previous experience evaluation available at local storage of edge nodes. In Equation 10b, \( f_{t_{\text{exp}}}^{d_{i \rightarrow j}} \) represent the formulation process of final trust degree where \( c_{t_{\text{exp}}}^{d_{i \rightarrow j}} \) is the current trust parameter evaluation and \( t_{\text{exp}}^{d_{i \rightarrow j}} \) illustrate the absolute experience trust evaluation. After the formulation of 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 last phase that utilizes the absolute final trust degree to compare it with the threshold value the will help to decide whether the node is trustworthy or malicious. In the proposed mechanism the range of trust degree is from 0.0-1.0 where 0.6 is the default trust degree of newly joined edge nodes and 0.7-1.0 is the trustworthy trust where 0.0-0.6 is the flunk/no trust for old edge nodes as illustrated in Equation 11.

\[ \theta = t_{\text{exp}}^{d_{i \rightarrow j}} \]

(11a)

\[ \theta = \begin{cases} 
    \text{FlunkTrust} & \text{if } \theta \leq 0.6 \\
    \text{Trustworthy} & \text{if } \theta \geq 0.7 
\end{cases} \]

(11b)

If node satisfies the threshold value then they are allowed to communicate with each other while if the trust degree of a particular node is less than the minimum requirement then the node cannot communicate, and also not allowed to exchange or share information. Further, the edge node will also evaluate the friendliness at the end of communication to examine that the process of trust degree evaluation should be time-driven or event-driven in the future where the classification of these process is evaluated in Section 3.3.

3.6 Recommendation-based Indirect Trust

The recommendation-based trust evaluation is an important factor when a node wants to communicate or take services and the other side node does not have any previous observations or experience evaluation to decide that the node is trustworthy or not. The recommendation-based trust evaluation provides a way to evaluate trust degree by requesting the surroundings nocentral authorise we have utilized an open-source library Zetta [58, 65] to create central authorise and IoTivity library [23] to enable inter-object connectivity where the wireless communication is performed by utilizing Zigbee (IEEE 802.15) [28]. Several existing mechanism has been utilized to compare the performance which are TMEI [49], RobustD [26], SGSQ-TM [19].

The simulation has been performed under different scenario and attacks by varying the number of network nodes. During simulation the number of varying nodes are 50-400 where the malicious and compromised nodes percentage ratio are 35%-45%. The simulation time (t) is also varying between 600-1100 Minutes(m) where the time-based friendliness is performed when the number of sessions created between nodes is greater then or equal to 50. For newly joined nodes the default trust degree is 0.6 where for old nodes the flunk/no trust is 0.0-0.6 where 0.7-1.0 is considered as trustworthy trust.

4 Results and Discussion

In this section, the performance evaluation of the proposed model is elaborated in comparison with the existing schemes.

4.1 Aggregated Trust Evaluation

Trust aggregation is a process in which particular 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 getting the services known as experience and uses that for aggregation purposes in future trust evaluation. We have evaluated the impact of experience trust aggregation under two different scenarios in which trust computation is performed by the 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 trustworthy node with aggregation formulate stable result and enhances the accuracy where the trust without aggregation illustrate the wavered trust degree over a time interval (t). In the second scenario, the identical evaluation is performed on the trust degree of malicious or compromised nodes and the result shows similar outcomes in which Flunk TWP (Trust with Previous) represents uniform trust degree and Flunk TNO (Trust with no Previous) notable inconstancy in trust degree and also assign the higher trust degree that shows the significance of employing the previous experience in the proposed approach.
4.2 Honest & Dishonest Trust Accuracy

The evaluation of honest and dishonest trust evaluation accuracy represent outcomes of actual and computed trust degree by the model after the training phase. The simulation is performed to evaluate the trust degree evaluation of honest and dishonest nodes where the comparative analysis is illustrated by Figure 4, and 5. The simulation time of the honest and dishonest accuracy evaluation is 300 Seconds (s) where the minimum trust is 0.0 and maximum trust is 1.0. The comparative analysis of computed and actual trust degree of honest is represented by Figure 4 in which the model takes 147(s) to evaluate the actual trust whereas during the evaluation of dishonest trust degree the time taken to remove the difference between computed and actual trust is 162.5(s) for accurate computations as illustrated by Figure 5.

4.3 On-off Attack

The on-off attack is one of the most significant attacks in the IoT heterogeneous environment where good nodes may become malicious or compromised at any time. When a node maintains a higher trust degree and its neighboring nodes also assign higher rank as an experience then it becomes vital to distinguish such nodes that become malicious after maintaining higher trust. Further, these nodes may be compromised by different attacks that make it significant to recognize these nodes to maintain security and privacy. To evaluate the performance among exiting approaches under two distinct scenarios by varying the percentage of malicious nodes and time(t).

In the first scenario of on-off attack, the number of nodes is varying from 50-400 in which the percentage of malicious and compromised nodes is 35% where the time of the simulation is 600(m). Figure 6 represent the simulation outcomes of on-off attack scenario-1 that illustrate the performance comparison in which the proposed mechanism has successfully recognize the execution and assigns the lower/flunk trust degree as the nodes become malicious after a particular time interval. Initially, the proposed mechanism assigns the default trust degree to the nodes with no past experience and assign increasing trust degree at point different points that reach to 0.64 at point-5 that falls down to 0.55 to the least trust goes to 0.01. In the second scenario, number of nodes is the same as previous the percentage ratio of malicious nodes becomes 45% where the simulation time is now 1100(m) with a threshold is 0.0-1.0, and trust is computed with aggregated past experience. The increase in malicious and compromised nodes shows their effect in simulation and the trust computation assign to these nodes is lower from the beginning and reaches down to 0.25 at the end. In both, the scenario the proposed EdgeTrust mechanism has assigned a low trust degree that represents the effectiveness of the trust parameters along with the experience component of trust that it successfully recognizes the on-off attack.

4.4 Self Promoting Attack

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

In the first scenario, the total number number of nodes are 400 with percentage of self-promoting nodes is 35% and these nodes self promote themselves alone and does not have any supporting nodes where the simulation time consists of 600(m) with default trust is 0.6 for new nodes, flunk trust is 0.0-0.6, and supreme trust of 0.7-1.0. Figure 8 illustrate the simulation outcomes of self promoting attack scenario 1 in which the proposed mechanism initially assign the trust degree of 0.86 and the trust degree decreases to 0.2 that shows the successful identification of self promoting nodes. Further, the SGSQ-TM [19] also shows effective performance and assign the low trust degree i.e, 0.5. In the second scenario, the total number of nodes are 400 with the 45% self-promoting nodes where the simulation time is 600(m). In this scenario, self promoting executes the attack in a group that mean a bundle of nodes works in parallel to promote a particular node by assigning higher fake trust degree. Figure 9 illustrates the simulation outcomes in comparison with the existing approaches and the result shows 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 assigns lower trust degree of 0.6, RobustD and SGSQ-TM assign lower trust degree of 0.4 and 0.23, respectively.

4.5 Good & Bad Mouthing Attack

Good and Bad mouthing attack is very similar to self-promoting attack but in this attack, nodes do not work together to promote themselves. The good and bad-mouthing attack is executed by malicious nodes to assign a lower trust degree to the trustworthy nodes known as bad-mouthing while they can assign a higher trust degree to the malicious nodes that are 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 recommendation is minimum 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 performs extensive simulation against good and bad-mouthing attacks under different scenarios. The performance of proposed among existing approaches is evaluated under two different scenarios.
for each good and bad-mouthing by applying the variation to the number of trustworthy and malicious nodes.

In the first scenario of good mouthing attack, the number of nodes is 600 where the percentage of malicious nodes is 35%. Figure 12 illustrate the performance of the proposed mechanism shows the continuously progressing trust degree to \( \geq 0.9 \) and after the identification of good mouthing attack the trust degree declines to \( \leq 0.7 \), and later on, the trust degree assign by the EdgeTrust declines to flunk trust of \( \leq 0.4 \). In Comparison, the TMEI, and RobustD also shows a notable performance and assign a lower trust degree as 0.4, and \( \leq 0.5 \), 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 and in comparison with the first scenario the result is more fluctuated that happened due to the percentage ratio of malicious or compromised nodes. When the number of nodes increases and numerous nodes tries to execute an attack then the approaches trust degrees fluctuate between higher and lower trust degrees. In the second scenario of good mouthing evaluation, the proposed initially assign higher trust degree up to 3 points where the trust degrees falls to \( \leq 0.2 \) at point 4 and again it increases to \( \geq 0.3 \) and \( \geq 0.8 \) that represent the EdgeTrust assign the lower trust to the malicious nodes and detect the trustworthy nodes to assign higher trust.

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 on trustworthy nodes by assigning a low trust degree while the increasing trust graph of the proposed approach clearly shows that it successfully recognize the attack and assigns a higher trust degree to the nodes. The proposed EdgeTrust approach initially assigns a lower degree of trust which is 0.3 but arises to designate an increasing trust value degree that reaches 0.9 which is a higher trust degree. Further, existing approaches such as TMEI also show notable progressive performance against the attack and assign a higher trust degree to the trustworthy nodes. In the second scenario of attack, the total number of nodes is 400 where the malicious and compromised nodes that execute 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 increased with time and reaches to \( > 0.8 \) which is the higher trust degree. In comparison, the SGSQ-TM approach also manifests an effective performance and maintains the trust degree of trustworthy higher which is 0.8 in the beginning and reaches to \( > 0.7 \). The performance of TMEI is stable and assigns a higher trust degree whereas the performance of RobustD assigns a lower trust degree which is \( < 0.5 \) but begins assigning a higher trust degree after 450(m) that reaches to \( \geq 0.7 \).
4.6 Energy Consumption Evaluation

Communication and computation consume a notable amount of energy and in IoT and it is significant to propose such approaches that consume less energy to make that 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 have first evaluated the energy consumption of the proposed mechanism with a fixed number of nodes and by applying variation to the total time (t). Figure 14 illustrates the simulation which has been performed with 100, 200, ..., 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 is also been evaluated with varying total number of nodes where the simulation time is 1100(m). Figure 15 illustrate the energy consumption of the approaches that show the proposed approach has utilized less energy to performs trust computation whereas in comparison RobustD and TMEI use average consumption while SGSQ-TM approaches use the higher amount of energy to performs it 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 maintains security among IoT nodes.

5 Conclusion

Internet of Things (IoT) provides diverse opportunities to the real-world to improve daily life by making autonomic devices that are intelligent and can communicate and performs required operations and given tasks. Nodes in the IoT environment contain different specifications while the edge nodes like sensors do have such capabilities to maintain security in heterogeneous surroundings. The proposed mechanism address that challenges and proposed a lightweight approach to maintain security among nodes. The proposed mechanism utilizes trust parameters and central authorize 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. The utilization of centralized and distributed trust management makes it suitable for the situation when any of the central authority becomes unavailable at any particular time. The time and event-driven trust computation evaluation makes the proposed mechanism suitable for Green IoT and provides a way to consumes fewer energy resources. 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 potential attacks to maintain a robust environment. In the future, the proposed mechanism can be extended by evaluating the storage challenges that may face by the edge nodes, and also a secure approach is required to maintain the security of central authorize against DOS/DDOS attacks.
Conflicts of Interest

The authors declare that they have no conflicts of interest regarding the publication of this work.

Data and Code Availability

Not applicable.

Funding

This research received funding from King Saud University under the project number RSP-2020/184.

Acknowledgments

This work was supported in part by King Saud University, Saudi Arabia, through research supporting project number RSP-2020/184; in part by FCT/MCTES through national funds and when applicable co-funded EU funds under the project UIDB/50008/2020; and in part by Brazilian National Council for Scientific and Technological Development (CNPq) via Grant No. 309335/2017-5.

References

1. Abiodun OI, Jantan A, Omolara AE, Dada KV, Mohamed NA, Arshad H (2018) State-of-the-art in artificial neural network applications: A survey. Heliyon 4(11):e00938
2. Ali W, Din IU, Almogren A, Guizani M, Zuair M (2020) A lightweight privacy-aware iot-based metering scheme for smart industrial ecosystems. IEEE Transactions on Industrial Informatics
3. Ali W, Din IU, Almogren A, Kumar N (2020) Alpha: An anonymous orthogonal code-based privacy preserving scheme for industrial cyber physical systems. IEEE Transactions on Industrial Informatics
4. Almogren A, Mohiuddin I, Din IU, Al Majed H, Guizani N (2020) Ftm-iomt: Fuzzy-based trust management for preventing sybil attacks in internet of medical things. IEEE Internet of Things Journal
5. Asmat H, Din IU, Ullah F, Talha M, Khan M, Guizani M (2020) Efc: Edge linked caching for content updating in information-centric internet of things. Computer Communications
6. Awan KA, Din IU, Almogren A, Guizani M, Altameem A, Jadoon SU (2019) Robustrust—a pro-privacy robust distributed trust management mechanism for internet of things. IEEE Access 7:62095–62106
7. Awan KA, Din IU, Zareei M, Talha M, Guizani M, Jadoon SU (2019) Holitrust—a holistic cross-domain trust management mechanism for service-centric internet of things. IEEE Access 7:52191–52201
8. Awan KA, Din IU, Almogren A, Almajed H, Mohiuddin I, Guizani M (2020) Neurotrust—artificial neural network-based intelligent trust management mechanism for large-scale internet of medical things. IEEE Internet of Things Journal pp 1–1
9. Awan KA, Din IU, Almogren A, Almajed H, Mohiuddin I, Guizani M (2020) Neurotrust—artificial neural network-based intelligent trust management mechanism for large-scale internet of medical things. IEEE Internet of Things Journal
10. Awan KA, Din IU, Almogren A, Guizani M, Khan S (2020) Stabtrust—a stable and centralized trust-based clustering mechanism for iot enabled vehicular ad-hoc networks. Ieee Access 8:21159–21177
11. Awan KA, Ud Din I, Almogren A, Almajed H (2020) Agritrust—a trust management approach for smart agriculture in cloud-based internet of agriculture things. Sensors 20(21):6174
12. Azad MA, Bag S, Hao F, Shalaginov A (2020) Decentralized self-enforcing trust management system for social internet of things. IEEE Internet of Things Journal 7(4):2690–2703
13. Bandypadhyay S, Sengupta M, Maiti S, Dutta S (2011) A survey of middleware for internet of things. In: Recent trends in wireless and mobile networks, Springer, pp 288–296
14. Boudagdigue C, Benslimane A, Kobbane A, Liu J (2020) Trust management in industrial internet of things. IEEE Transactions on Information Forensics and Security
15. Caminha J, Perkusich A, Perkusich M (2018) A smart middleware to detect on-off trust attacks in the internet of things. In: Consumer Electronics (ICCE), 2018 IEEE International Conference on, IEEE, pp 1–2
16. Cao B, Li Y, Zhang L, Zhang L, Mumtaz S, Zhou Z, Peng M (2019) When internet of things meets blockchain: Challenges in distributed consensus. IEEE Network 33(6):133–139
17. Chen JIZ (2018) Embedding the mrc and sc schemes into trust management algorithm applied to iot security protection. Wireless Personal Communications 99(1):461–477
18. Dai HN, Zheng Z, Zhang Y (2019) Blockchain for internet of things: A survey. IEEE Internet of Things Journal 6(5):8076–8094
19. Das R, Singh M, Majumder K (2019) Sgsqot: A community-based trust management scheme in internet of things. In: Proceedings of International Ethical Hacking Conference 2018, Springer, pp 209–222
20. Diène B, Rodrigues JJ, Diallo O, Ndoye EHM, Korotaev VV (2020) Data management techniques for internet of things. Mechanical Systems and Signal Processing 138:106564

21. Din IU, Asmat H, Guizani M (2019) A review of information centric network-based internet of things: communication architectures, design issues, and research opportunities. Multimedia Tools and Applications 78(21):30241–30256

22. Din IU, Guizani M, Rodrigues JJ, Hassan S, Korotaev VV (2019) Machine learning in the internet of things: Designed techniques for smart cities. Future Generation Computer Systems 100:826–843

23. Elsayed K, Ibrahim MAB, Hamza HS (2019) Service discovery in heterogeneous iot environments based on ocf/iotivity. In: 2019 15th International Wireless Communications & Mobile Computing Conference (IWCMC), IEEE, pp 1160–1165

24. Ephzibah E, Dharinya SS, Remya L (2020) Decision making models through ai for internet of things. In: Internet of Things for Industry 4.0, Springer, pp 57–72

25. Esposito C, Tamburis O, Su X, Choi C (2020) Robust decentralised trust management for the internet of things by using game theory. Information Processing & Management 57(6):102308

26. Esposito C, Tamburis O, Su X, Choi C (2020) Robust decentralised trust management for the internet of things by using game theory. Information Processing & Management 57(6):102308

27. Fotros M, Rezazadeh J, Sianaki OA (2020) A survey on vanets routing protocols for iot intelligent transportation systems. In: Workshops of the International Conference on Advanced Information Networking and Applications, Springer, pp 1097–1115

28. Gočal P, Macko D (2019) Eemip: Energy-efficient communication using timing channels and prioritization in zigbee. Sensors 19(10):2246

29. Gulzar M, Abbas G (2019) Internet of things security: a survey and taxonomy. In: 2019 International Conference on Engineering and Emerging Technologies (ICEET), IEEE, pp 1–6

30. Guo Y, Wang N, Xu ZY, Wu K (2020) The internet of things-based decision support system for information processing in intelligent manufacturing using data mining technology. Mechanical Systems and Signal Processing 142:106630

31. Haseeb K, Almogren A, Islam N, Ud Din I, Jan Z (2019) An energy-efficient and secure routing protocol for intrusion avoidance in iot-based wsn. Energies 12(21):4174

32. Haseeb K, Almogren A, Ud Din I, Islam N, Altameem A (2020) Sasc: Secure and authentication-based sensor cloud architecture for intelligent internet of things. Sensors 20(9):2468

33. Haseeb K, Din IU, Almogren A, Islam N, Altameem A (2020) Rts: A robust and trusted scheme for iot-based mobile wireless mesh networks. IEEE Access 8:68379–68390

34. Hui H, Zhou C, Xu S, Lin F (2020) A novel secure data transmission scheme in industrial internet of things. China Communications 17(1):73–88

35. Jadoon G, Ud Din I, Almogren A, Almajed H (2020) Smart and agile manufacturing framework, a case study for automotive industry. Energies 13(21):5766

36. Janjua K, Shah MA, Almogren A, Khattak HA, Maple C, Din IU (2020) Proactive forensics in iot: Privacy-aware log-preservation architecture in fog-enabled-cloud using holochain and containerization technologies. Electronics 9(7):1172

37. Khan MA, Din IU, Jadoon SU, Khan MK, Guizani M, Awan KA (2019) G-rat—a novel graphical randomized authentication technique for consumer smart devices. IEEE Transactions on Consumer Electronics 65(2):215–223

38. Khan MA, Din IU, Jadoon SU, Khan MK, Guizani M, Awan KA (2019) G-rat—a novel graphical randomized authentication technique for consumer smart devices. IEEE Transactions on Consumer Electronics 65(2):215–223

39. Khan ZA (2018) Using energy-efficient trust management to protect iot networks for smart cities. Sustainable cities and society 40:1–15

40. Khattak HA, Tehreem K, Almogren A, Ameer Z, Din IU, Adnan M (2020) Dynamic pricing in industrial internet of things: Blockchain application for energy management in smart cities. Journal of Information Security and Applications 55:102615

41. Kouicem DE, Imine Y, Bouabdallah A, Lakhlef H (2020) A decentralized blockchain-based trust management protocol for the internet of things. IEEE Transactions on Dependable and Secure Computing

42. Li H, Zhang Z, Liu Z (2017) Application of artificial neural networks for catalysis: a review. Catalysts 7(10):306

43. Li Y, Tu Y, Lu J, Wang Y (2020) A security transmission and storage solution about sensing image for blockchain in the internet of things. Sensors 20(3):916

44. Lyu Y, Yin P (2020) Internet of things transmission and network reliability in complex environment. Computer Communications 150:757–763

45. Malik FM, Khattak HA, Almogren A, Bouachir O, Din IU, Altameem A (2020) Performance evaluation of data dissemination protocols for connected autonomous vehicles. IEEE Access 8:126896–126906

46. Mukherjee S, Sharma N (2012) Intrusion detection using naive bayes classifier with feature reduction. Proce-
47. Qiu J, Tian Z, Du C, Zuo Q, Su S, Fang B (2020) A survey on access control in the age of internet of things. IEEE Internet of Things Journal.

48. Qu C, Tao M, Yuan R (2018) A hypergraph-based blockchain model and application in internet of things-enabled smart homes. Sensors 18(9):2784

49. Qureshi KN, Iftikhar A, Bhatti SN, Piccialli F, Giampaolo F, Jeon G (2020) Trust management and evaluation for edge intelligence in the internet of things. Engineering Applications of Artificial Intelligence 94:103756

50. Razzaque MA, Milojevic-Jevric M, Palade A, Clarke S (2015) Middleware for internet of things: a survey. IEEE Internet of things journal 3(1):70–95

51. Rish I, et al. (2001) An empirical study of the naive bayes classifier. In: IJCAI 2001 workshop on empirical methods in artificial intelligence, vol 3, pp 41–46

52. Shafique K, Khawaja BA, Sabir F, Qazi S, Mustaqim M (2020) 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 8:23022–23040

53. Sharif A, Ouyang J, Yang F, Chattha HT, Imran MA, Alomainy A, Abbasi QH (2019) Low-cost inkjet-printed uhf rfid tag-based system for internet of things applications using characteristic modes. IEEE Internet of Things Journal 6(2):3962–3975

54. Sicari S, Rizzardi A, Grieco L, Piro G, Coen-Porisini A (2017) A policy enforcement framework for internet of things applications in the smart health. Smart Health 3:39–74

55. Sicari S, Rizzardi A, Coen-Porisini A (2020) 5g in the internet of things era: an overview on security and privacy challenges. Computer Networks p 107345

56. Siddiqua A, Shah MA, Khattak HA, Din IU, Guizani M (2019) Icache: Intelligent congestion avoidance and fast emergency services. Future Generation Computer Systems 99:365–375

57. Singh B (2019) The internet of things: A vision for smart world. In: Advances in Signal Processing and Communication, Springer, pp 165–172

58. Triantafyllou A, Sarigiannidis P, Lagkas TD (2018) Network protocols, schemes, and mechanisms for internet of things (iot): Features, open challenges, and trends. Wireless communications and mobile computing 2018

59. Tseng L, Yao X, Otoum S, Aloqaily M, Jararweh Y (2020) Blockchain-based database in an iot environment: challenges, opportunities, and analysis. Cluster Computing pp 1–15

60. Villegas-Ch W, Palacios-Pacheco X, Román-Cañizares M (2020) An internet of things model for improving process management on university campus. Future Internet 12(10):162

61. Wu F, Wu T, Yuce MR (2019) An internet-of-things (iot) network system for connected safety and health monitoring applications. Sensors 19(1):21

62. Yadav P, Vishwakarma S (2018) Application of internet of things and big data towards a smart city. In: 2018 3rd International Conference On Internet of Things: Smart Innovation and Usages (IoT-SIU), IEEE, pp 1–5

63. Yan Z, Zhang P, Vasilakos AV (2014) A survey on trust management for internet of things. Journal of network and computer applications 42:120–134

64. Yu G, Fu W (2020) Analysis of distributed database access path prediction based on recurrent neural network in internet of things. Concurrency and Computation: Practice and Experience 32(1):e5116

65. Zinca D, Popa MO (2018) Development of a zettajs driver for the esp8266 iot hardware. In: 2018 International Symposium on Electronics and Telecommunications (ISETC), IEEE, pp 1–4