INDIAN JOURNAL OF SCIENCE AND TECHNOLOGY

RESEARCH ARTICLE

Efficient Reputation-based Cyber Attack Detection Mechanism for Big Data Environment

Vinod Desai[1]*, **H A Dinesh**[2,3]

1 Assistant Professor, Department of Computer Science and Engineering, Angadi Institute of Technology and Management, Belagavi, 590009, Karnataka, India
2 Professor and HOD, Department of Computer Science and Engineering, Nagarjuna College of Engineering and Technology, Bangalore
3 Founder and Director, Cybersena (R&D) India Private Limited, Shreenagar, Belagavi, 590016

OPEN ACCESS

Received: 12-11-2021

Accepted: 23-02-2022

Published: 29.03.2022

Citation: Desai V, Dinesh HA (2022) Efficient Reputation-based Cyber Attack Detection Mechanism for Big Data Environment. Indian Journal of Science and Technology 15(13): 592-602. https://doi.org/10.17485/IJST/v15i13.2102

* **Corresponding author**.

vinod.cd0891@gmail.com

Funding: None

Competing Interests: None

Published By Indian Society for Education and Environment (iSee)

ISSN
Print: 0974-6846
Electronic: 0974-5645

Abstract

Objective: To reduce the cyber-attacks in IoT devices and also to provide security and reliable communication among the IoT devices and Edge servers, we have designed an Efficient Reputation-based Cyber-Attack Detection (ERCAD) mechanism for the Bigdata environment. **Methods:** This work presents an Efficient Reputation-based Cyber-Attack Detection (ERCAD) mechanism using the trust-based method. This work provides reliability and security by employing a trust-based security model and a feedback-based model. Moreover, to increase the network performance of the model which the existing system lacks, our model provides a reputation metric that classifies the malicious IoT nodes. Also, our model provides an efficient reputation cyber-attack detection communication metric for Bigdata Environment. **Findings:** Most of the Existing Reputation-Based Security (ERS)(1),(2),(3) models have achieved a good detection rate but have an increased failure rate. Furthermore, the ERS models have more throughput with more energy consumption and are less reliable and have not provided any QoS requirement and proper security for their models. Hence, the ERCAD model achieves a very good attack detection rate of 22.04% with a minimum detection failure rate of 33.89% for a wide range of attacks in comparison with Existing Reputation-Based Security (ERS) models. Moreover, the ERCAD improves throughput by 22.40% and with a reduction of energy consumption of 40.032% in comparison with Existing Reputation-Based Security (ERS) models and also is highly reliable by assuring QoS and security together. **Novelty:** The ERS models have failed to attain a better attack detection rate when the device is in the dynamic behavior. Further, are not efficient in modeling feedback reliability. Hence, our ERCAD model provides a better attack detection rate when the device is in dynamic behavior and also provides a security framework for classifying the malicious IoT nodes.

Keywords: Reliability; Security; Detection; BigData Environment; QoS requirement

1 Introduction

IoT devices are ranging from tiny wearable devices to large industrial IoT-based Bigdata applications. The age of IoT with millions of associated gadgets has made a consistently bigger area for digital assailants to take advantage of, which has brought about the requirement for quick and precise identification of attacks[4]. Due to this, there is an increase in communication with no proper security to the IoT-based Bigdata applications. The advancements in smart devices, mass storage, communication, and mobile computing designs in the last 10 years have achieved the occurrence of Bigdata, which includes an extraordinary quantum of useful information created in different structures at a faster pace. The capacity to deal with these gigantic measures of information continuously utilizing the Bigdata analytic tool brings in significant advantages that could be used in cyber-attack detection frameworks. The intrusion detection system or cyberattack detection framework can extract useful information in real-time by utilizing large data gathered from cloud computing, computers, sensors, and networks framework. This data aids in detecting network/framework weaknesses and identifying attacks that getting more predominant and widespread and modeling security models under that[5]. BigData analysis frameworks will be an integral part of modern powerful cyber-threat detection mechanism because of the prerequisite of faster computation of huge volume and velocity of information collected through different means for establishing behavior, patterns, and anomalies as quick as conceivable to restrict system vulnerabilities/weakness and enhance its stability[1]. Even though numerous Bigdata analytical frameworks have been designed in the last decade, their use in the field of cyber-forensic certifications new methodologies considering numerous perspectives that include following such as data processing considering the resource-starved device, data aggregation, real-time analysis, and data sharing across intrusion detection system (IDS)[6].

In recent times a wide range of IoT-based applications have been emphasized and deployed considering many interconnected devices and generates an immense measure of information and push data towards cloud storage wirelessly. Thus, in IoT applications providing security, privacy, and trust plays a significant part in the wide adoption of IoT. Trust is a key feature that is used for establishing trustworthy communication between different devices to provide secure services. In[6], a Deep RL-based security model is presented for offloading execution. Here they considered both short and long-term interaction history into consideration. Trust computation is the basic foundation that has been adopted in different distributed computing services such as Cloud computing wireless sensor networks[2], P2P communication[7], Adhoc communication, and IoT edge computing[8]. Unlike standard authentication schemes such as cryptography mechanisms, the trust (i.e., reputation)-based computing scheme uses dynamic behavior pattern of user/service provider for establishing malicious service provider concerning the authenticated service provider. The existing trust-based security methodology offers a good access control mechanism by comparing QoS and helps in providing reliability by guaranteeing that all communicating devices are trustable during service provisioning[9]. Recently, in the Bigdata environment different attacks and security threats have been introduced such as communication attacks and physical attacks; for example, reply attacks, message tampering, message forging, and distributed denial of service (DDoS) attacks[9]. The current problems prompt the absence of trust among IoT gadgets, which has delayed the general acknowledgment of IoT edge computing service providers (IoT-ECSP) for outsourcing computing services. In this manner, IoT-ECSP must assure trust to mitigate the worries of various end clients[10]. To guarantee the nature of cooperative assistance practices and support to set up trust among IoT edge gadgets, the trust component is utilized, which is especially significant because gadgets in edge computing environments have different expertise levels and assorted capacities, and there is a chance of presence of malicious nodes who augment their advantages. In particular, IoT-ECSP is experiencing an assortment of malicious behavior like collusive cheating, badmouth attacks, and false feedback[9]. Furthermore, how to develop an efficient trust computational model for guarantying the effective execution of the given jobs, has become a hot research area of IoT-ECSP and Bigdata communication frameworks. Further, the major issues are how to compute the trust of IoT devices reliably in IoT-ECSP and Bigdata communication frameworks.

In addressing the aforementioned issues number of trust-based security models have been presented IoT-ECSP and Bigdata communication frameworks. In[10] presented a trust computation model for IoT device communication considering five trust parameters such as trust propagation, trust architecture, trust algorithm, trust source, and trust metrics. In[11] presented a blockchain-based trust computation model with help of mobile edge computing (MEC) to identify selfish edge attacks. Here the selfish attacks are identified through reinforcement learning (RL) and then it's broadcasted among neighboring mobile and edge devices. To further improve detection accuracies modeled deep RL. In[12], presented a multi-party authentication scheme employing a blockchain mechanism for providing security and preserving privacy. Here timestamp information is used for building trust and every party must be sent correct information within the stipulated time. Employed game theory (GT) for guaranteeing fairness. Furthermore, the trust computation method is presented for the selection of trustable cluster head (CH) and backup cluster head for eliminating malicious nodes and sharing valid information across the Bigdata collection framework. In[13] presented a decentralized trust-based security model that guarantees SLA and privacy requirements. Here trust is computed based on past interaction among public fog nodes to provision service to end-users. In[14], employed blockchain-based decentralized trust management technique. Here the data is transmitted to the node with the highest trustable parameter. In[15] presented a probability-based trust computation model for the execution of a task with a privacy guarantee. However, these models fail to assure the reliability requirement of application QoS and security prerequisites[3]. Further, existing models have some important limitations. In[16], they have given six methods to process and analyze the large Bigdata datasets.

First, very little work has been modeled considering Bigdata application under IoT edge computing environment focusing on reliability issues employing a trust-based security model. Second, most of the existing trust-based security models neglect collusion issues using feedback-based mechanisms; thus, the reliability of the model is reduced. Third, existing trust-based security models lack the flexibility of global trust aggregation computation; thus, may result in an error in computing trust value especially when IoT devices exhibit dynamic behavior such as sometimes behaving well and sometimes behaving badly. Detection and removing such kinds of a device from the network are very difficult. Further, the user may give biased, unfair, and selfish feedback for their benefit; Thus, affecting the reliability of communication. Lastly, existing reputation-based frameworks are mainly designed considering a high resource availability environment; thus, when adopted to a resource-starved environment induce significant overhead; as result affects network performance. For overcoming the research issues this paper presents an efficient reputation-based cyber-attack detection mechanism for the Bigdata environment. Different reputation metrics are modeled based on device interaction. Finally, secure communication metrics are presented to achieve high reliability.

The contribution of an efficient reputation-based cyber-attack detection model is given below.

- The ERCAD model achieves a very good attack detection rate with minimal detection failure rate wide range of attacks in comparison with the standard reputation-based security mechanism.
- The ERCAD improves throughput with minimal energy consumption in comparison with the standard reputation-based security mechanism.
- ERCAD is highly reliable by assuring QoS and security together.

2 Efficient Reputation-based Cyber Attack detection Method For BigData Environment

This section presents an efficient reputation-based cyber-attack detection mechanism for the BigData environment. First is the system model of a secure Bigdata collection environment through thousands of interconnected IoT devices. Then, we have presented various reputation metrics for building an efficient reputation-based cyber-attack detection mechanism. Finally, the objective parameter is modeled for achieving reliable communication.

2.1 System model

This work presents the system model for securely collecting a large amount of data from thousands of interconnected IoT devices toward gateway/edge servers and storing collected information into a cloud storage environment for provisioning Bigdata applications (i.e., further processing). The architecture of the secure data collection model for provisioning the Bigdata application is shown in Figure 1. These IoT devices are powered through batteries; thus, preserving batteries are of utmost importance. Further, are composed of different sensors for collecting various sensory information through time or event-driven, and are wireless with limited coverage. Thus, these IoT devices communicate through the intermediate device to reach the destination. If one device is compromised (i.e., it is being attacked or turned malicious), then it affects the overall communication of the network. One way of protecting information is to employ a cryptography mechanism; however, the cryptography mechanism induces high computation overhead; thus, is not suitable considering battery constrained nature of IoT devices which is deployed in a hazardous location where the replacement of batteries is nearly impossible. Recently, a reputation-based security framework offers significant benefits considering such an environment. However, the standard reputation-based security model cannot guarantee feedback reliability and are not efficient in detecting unfair and oscillating behavior pattern of IoT devices; as a result, achieves poor detection accuracies and thus affects the overall performance of the BigData collection network. To address this work present Efficient Reputation-based Cyber Attack Detection (ERCAD) Mechanism for BigData environment.

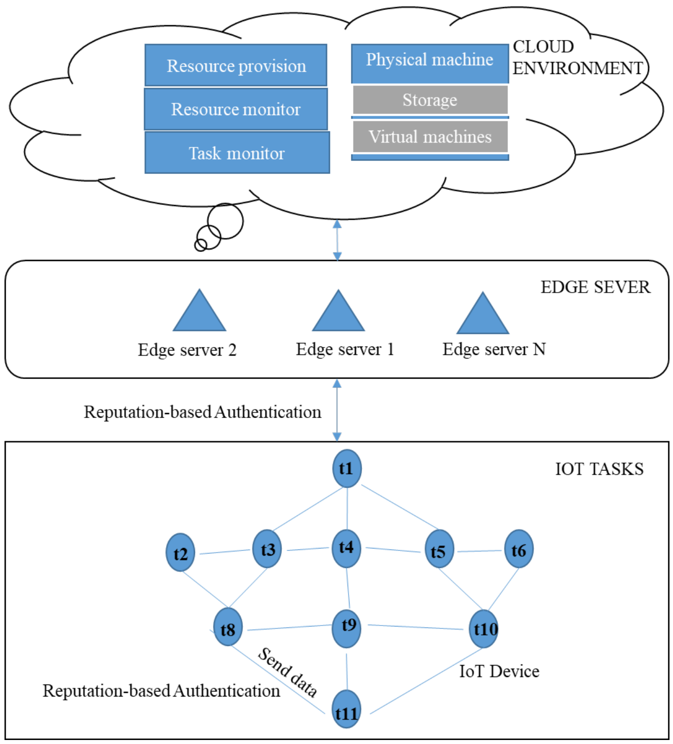

Fig 1. The architecture of secure data collection model for provisioning Bigdata application.

2.2 Feedback-reliability reputation metric:

In this section, feedback-reliability reputation metrics are modeled for the Bigdata environment. Let consider $Sec_o^u(x,y)$ as a parameter defining the total trust of IoT node x for IoT node y for carrying out certain tasks considering o association in u^{th} time interval is measured through the following equation

$$Sec_o^u(x,y) = \gamma * Sec_{rec}(x,y) + (1-\gamma) * Sec_{o-1}^u(x,y). \tag{1}$$

where parameter γ is adjusted based on recent failures $\mu_o^u(x,y)$ and its associated variance $\beta_o^u(x,y)$, Sec_{rec} defines recent association trust experienced with respect to other IoT nodes. The feedback variance among IoT nodes x and y is collected through mutual IoT nodes of x and y as follows

$$V_o^u(x,y) = \sqrt{\frac{\sum_{p \in H} \left(Sec_o^u(x,p) - Sec_o^u(y,p)\right)^2}{(H(x,y)|}} \tag{2}$$

where p defines the mutual IoT node, $H(x,y)$ defines mutual IoT nodes with whom IoT nodes x and y have associated. In order to obtain a relationship among IoT node x and$(R_o^u(x,y))$, IoT node x initially relates $V_o^u(x,y)$ with the connection difference H and optimize it in the below equation

$$\mathbb{R}_o^u(x,y) = \begin{cases} \mathbb{R}_{o-1}^u(x,y) + \dfrac{1-\mathbb{R}_{o-1}^u(x,y)}{X}, & \text{if } \mathbb{V}_o^u(x,y) < \mathscr{H} \\ \mathbb{R}_{o-1}^u(x,y) - \dfrac{1-\mathbb{R}_{o-1}^u(x,y)}{Y}, & \text{else} \end{cases} \tag{3}$$

where X and Y define reward and penalty parameters, respectively which can be optimized dynamically as per application secureness prerequisite.

The above equation assures a certain level of security when all nodes behave good or bad all the time; however when nodes keep changing their behavior state with high randomness the existing reputation-based security model provides poor results. In addressing this work present improved reliability metrics. In this work higher weights are given to highly reliable devices and lesser weights are given to nodes with less reliability. Let $F_o^u(x,y)$ represent reliability parameter of IoT node y from IoT node $x's$ viewpoint as follow

$$\mathbb{F}_o^u(x,y) = \begin{cases} 1 - \dfrac{\log\left(\mathrm{Sec}_o^u(x,y)\right)}{\log\theta}, & \text{if } \mathbb{R}_o^u(x,y) > \theta \\ 0, & \text{else} \end{cases} \tag{4}$$

where $log\theta$ defines the least value of likenesses tolerance.

2.3 Explicit reputation metric

Here explicit trust $L_o^u(x,y)$ among IoT nodes x and y within one-hop neighbor with minimum o association considering u^{th} time interval is measured as follows

$$L_o^u(x,y) = Sec_o^u(x,y). \tag{5}$$

the above equation the IoT node x is given positive trust if IoT node y experiences a very good outcome considering $x's$ viewpoint.

2.4 Implicit reputation metric

Here implicit trust $G_o^u(x,y)$ among IoT nodes for all adjacent IoT devices greater than one-hop range. Here IoT nodes collect feedback from all neighboring nodes of the respective node with whom it wants to communicate securely. Later, the IoT nodes cumulate this collected feedback for establishing an explicit reputation as follows

$$\mathbb{G}_o^u(x,y) = \begin{cases} \dfrac{\sum_{p\in Z-\{x\}} \mathbb{F}_o^u(x,p) * \mathbb{L}_o^u(x,y)}{\sum_{p\in Z-\{x\}} \mathbb{F}_o^u(x,p)}, & \text{if } |Z-\{x\}| > 0 \\ 0, & \text{if } |Z-\{x\}| = 0 \end{cases} \tag{6}$$

where, $Z = S(y)$ defines the set of IoT nodes that have communicated with IoT node y.

2.5 Current reputation metrics

Using both implicit and explicit reputation metrics the current reputation metric $C_o^u(x,y)$ among IoT node x has on IoT node y is computed as follows

$$C_o^u(x,y) = \delta * L_o^u(x,y) + (1-\delta) * G_o^u(x,y) \tag{7}$$

where δ defines weights for optimizing current reputation metrics.

2.6 Past experience reputation metric

The current reputation metric will turn old after certain interactions; these parameters are kept by each IoT device through an exponential mean update for reducing storage overhead. Therefore, the past experience $L_o^u(x,y)$ reputation that IoT node x on IoT node y is computed as follows

$$L_o^u(x,y) = \frac{\varphi * L_{o-1}^u(x,y) + C_{o-1}^u(x,y)}{2}, \tag{8}$$

where $L_0^0(x,y) = 0$ and $\varphi\,(0 \le \varphi \le 1)$ defines the parameter used for rewarding.

2.7 Anticipated reputation metric

In order to measure the anticipated reputation $F_o^u(x,y)$ of IoT node y from IoT node $x's$ viewpoint, this work uses both current and past experience reputation metrics as follows

$$F_o^u(x,y) = \begin{cases} 0, \text{ if neither } \mathbb{L} \text{ or } \mathbb{C} \text{ is available} \\ \alpha\mathbb{C}_o^u(x,y) + (1-\alpha)\mathbb{L}_o^u(x,y) \text{ if either } \mathbb{L} \text{ or } \mathbb{C} \text{ is available} \end{cases} \tag{9}$$

where α defines how an IoT device can come out of past experience reputation. In this work initially, the α is set to zero, nonetheless, it can be optimized dynamically as per application need. Note the value of α should not be set very low as some malicious nodes can become good and impact performance.

2.8 Unfair and oscillating trust evaluation

Using current reputation and future reputation metrics with tolerance factor the unfair and oscillating reputation metrics $D_o^u(x,y)$ is computed as follows

$$\mathbb{D}_o^u(x,y) = \begin{cases} \mathbb{D}_{o-1}^u(x,y) + \dfrac{\mathbb{C}_o^u(x,y) - \mathbb{L}_o^u(x,y),}{\rho}, & \text{if } \mathbb{C}_o^u(x,y) - \mathbb{L}_o^u(x,y) > \tau \\ \mathbb{D}_{o-1}^u(x,y) + \mathbb{L}_o^u(x,y) - \mathbb{C}_o^u(x,y), & \text{if } \mathbb{C}_o^u(x,y) - \mathbb{L}_o^u(x,y) > -\tau \\ \mathbb{D}_{o-1}^u(x,y), & \text{otherwise} \end{cases} \tag{10}$$

where τ defines the tolerance parameter for optimizing reliabilities and ρ $(\rho > 1)$ defines penalty facto for bounding oscillation factor.

2.9 Reputation metric for classifying malicious IoT nodes

Using anticipated and unfair and oscillation reputation metric the final reputation metric for cyber-attack detection metric $F_o^u(x,y)$ is obtained as follows

$$F_o^u(x,y) = F_o^u(x,y) * D_o^u(x,y)\,. \tag{11}$$

The above equation assures the node will communicate with the device that is expected to be good in the future and as well as it will not change its state. The adoption of such a metric is very suitable for attaining efficient security methods for modern BigData applications.

2.10 Efficient reputation cyber-attack detection communication metric for BigData environment

This section presents an efficient reputation-based cyber-attack detection communication model for the BigData environment. Using Eq. (11), the malicious IoT nodes are eliminated from the network. Further, for improving efficiency and reliability the IoT device with maximum trust are chosen for communication as follows

$$max \textstyle\sum_{p \in Z - \{x\}} F_o^u(x,y) \tag{12}$$

The newly added device will not have any reputation parameters. In such circumstances, the nodes are chosen in a probabilistic manner as follows

$$\mathscr{P}^u(x,y) = \begin{cases} \dfrac{\mathscr{F}_o^u(x,y)}{\sum_{p\in V} \mathscr{F}_o^u(x,p)}, & \text{if } \sum\limits_{p\in V} \mathscr{F}_o^u(x,p) \neq 0 \\ \text{arbitrarily choose any sensor device}, & \text{else} \end{cases} \tag{13}$$

Using Eq. (13) the IoT nodes from V will start communicating with the node having the highest trust value and nodes with zero trust randomly selects a new node and communicate. The ERCAD model attains a much better attack detection rate with less attack detection failure rate when compared with the existing reputation-based security mechanism which is validated through an experiment in the below section.

3 Simulation Result and Analysis

In this section, simulation is conducted for studying the security effectiveness of ERCAD and the existing reputation-based security (ERS) mechanism[(1)],[(11)], and[(3)]. The SENSORIA is used for creating data collection and edge computing layer and CloudSim[(17)] is used for integrating the cloud layer. Sensoria was created with the goal of being simple to use while still giving sophisticated simulations. Sensoria makes the entire process simple and systematic, starting with the selection of input parameters and finishing with the graphic display of simulation outcomes. Sensoria has a visually appealing graphical interface (GUI).

The parameters used are as follows, the simulation area for collecting a large amount of data is set to$100m \times\ 100m$, a total of 4 edge servers used, IoT devices are set to 1000, the attack rate is varied from 10%-40%, the IoT device communicates using $IEEE$ $802.11b$ MAC, the communication range of IoT device is set to 6 meters, sensing range is set to 3 meters, initial energy of IoT devices varies from $0.05-0.2$ $Joules$ (j), the bandwidth is set to 10000 bit/s, data packet length is set to 2000 bits, control

Table 1. Parameters of the dataset used for SENSORIA simulation

Parameter	Values
Simulation Area	100m*100m
Total number of servers	4
IoT devices used	1000
Attack Rate	10%-40%
IoT device Communication Protocol	$IEEE$ 802.11b MAC
Communication Range of the IoT device	6 meters
Sensing Range of the IoT device	3 meters
Energy of the IoT device	$0.05 - 0.2$ $Joules$ (j)
Bandwidth of the IoT device	10000 bit/s
Data Packet Length	2000 bits
Control Packet Length	248 bits
Sensing of the IoT device	0.1 seconds
Amplification Energy of the IoT device	100 pJ/bit/m2
Idle Energy of the IoT device	50 nj/bit

packet length of 248 bits, sensing is done every 0.1 seconds, idle and amplification energy is set 50 nj/bit and 100 pJ/bit/m2, respectively. The following performance metrics such as attack detection rate, attack detection failure rate, throughput, energy consumption, and communication overhead have been analyzed using the SENSORIA simulation

3.1 Attack detection rate for varied attack rates

Here experiment is conducted by varying the attack rate from 10% to 40%, with an interval of 10%, and the attack detection rate achieved using ERCAD and ERS is graphically shown in Figure 2. The ERCAD improves the detection rate by 13.33% when the attack is set to 10% in comparison with ERS mechanism. The ERCAD improves the detection rate by 25.37% when the attack is set to 20% in comparison with ERS mechanism. The ERCAD improves the detection rate by 18.03% when the attack is set to 30% in comparison with ERS mechanism. Similarly, the ERCAD improves the detection rate by 17.105% when the attack is set to 40% in comparison with ERS mechanism. An average attack detection rate enhancement of 22.04% is achieved using ERCAD in comparison with ERS mechanism.

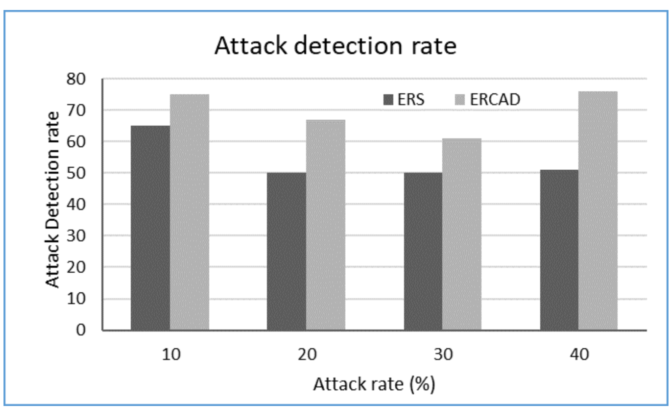

Fig 2. Attack detection ratevs attack rate (%)

3.2 Attack detection failure rate for varied attack rates:

Here experiment is conducted by varying the attack rate from 10% to 40%, with an interval of 10%, and the attack detection failure rate achieved using ERCAD and ERS is graphically shown in Figure 3. The ERCAD improves the attack detection failure rate by 28.57% when the attack is set to 10% in comparison with ERS mechanism. The ERCAD improves the attack detection failure rate by 34.0% when the attack is set to 20% in comparison with ERS mechanism. The ERCAD improves the attack detection failure rate by 22.0% when the attack is set to 30% in comparison with ERS mechanism. Similarly, the ERCAD improves the attack detection failure rate by 51.02% when an attack is set to 40% in comparison with ERS mechanism. An average attack detection failure rate enhancement of 33.89% is achieved using ERCAD in comparison with ERS mechanism.

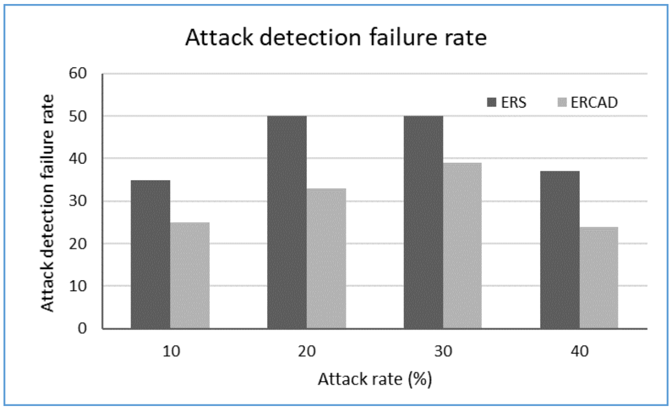

Fig 3. Attack detectionfailure rate vs attack rate (%)

3.3 Throughput performance for varied attack rates:

Here experiment is conducted by varying the attack rate from 10% to 40%, with an interval of 10% and throughput achieved using ERCAD and ERS is graphically shown in Figure 4. The ERS and ERCAD achieve a normalized throughput of 0.481 and 0.555, respectively when an attack is set to 10%. The ERS and ERCAD achieve a normalized throughput of 0.275 and 0.3685, respectively when an attack is set to 20%. The ERS and ERCAD achieve a normalized throughput of 0.205 and 0.2501, respectively when an attack is set to 30%. The ERS and ERCAD achieve a normalized throughput of 0.1326 and 0.1976, respectively when the attack is set to 40%. From Figure 4, it can be seen the ERCAD achieves an average throughput enhancement of 22.4% in comparison with ERS mechanism. As the IoT devices increase, the throughput of our model has better performance.

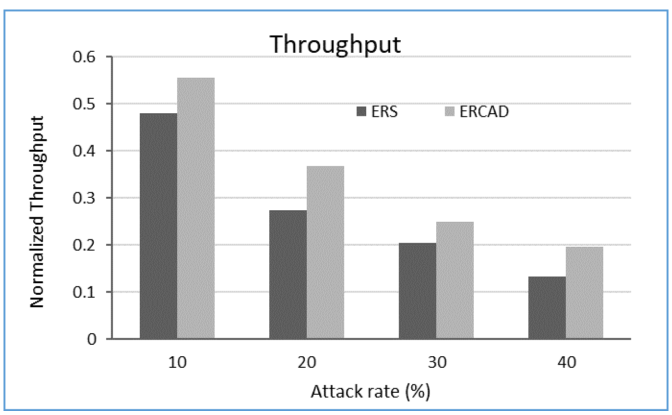

Fig 4. Throughput vs attackrate

3.4 Communication overhead for varied attack rates

Here experiment is conducted by varying the attack rate from 10% to 40%, with an interval of 10% and communication overhead achieved using ERCAD and ERS is graphically shown in Figure 5. The ERCAD reduces communication overhead by 22.51% when the attack is set to 10% in comparison with ERS mechanism. The ERCAD reduces communication overhead by 31.69%

when the attack is set to 20% in comparison with ERS mechanism. The ERCAD reduces communication overhead by 37.25% when the attack is set to 30% in comparison with ERS mechanism. Similarly, the ERCAD reduces communication overhead by 42.39% when the attack is set to 40% in comparison with ERS mechanism. An average reduces communication overhead reduction of 33.46% is achieved using ERCAD in comparison with ERS mechanism.

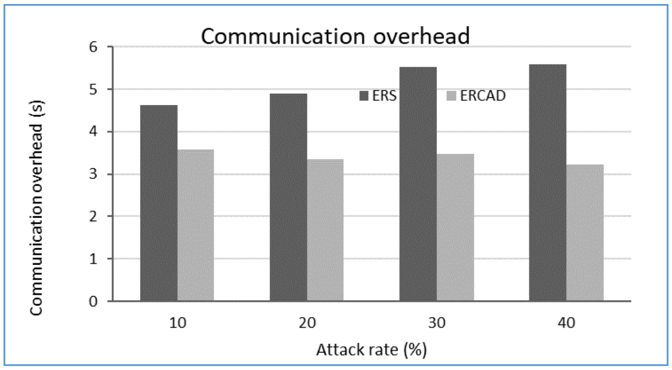

Fig 5. Communicationoverhead vs attack rate

3.5 Energy consumption for varied attack rates

Here experiment is conducted by varying the attack rate from 10% to 40%, with an interval of 10%, and the average energy consumption per packet induced using ERCAD and ERS is graphically shown in Figure 6. The ERCAD reduces average energy consumption per packet by 19.89% when the attack is set to 10% in comparison with ERS mechanism. The ERCAD reduces average energy consumption per packet by 45.32% when the attack is set to 20% in comparison with ERS mechanism. The ERCAD reduces average energy consumption per packet by 47.2% when the attack is set to 30% in comparison with ERS mechanism. Similarly, the ERCAD reduces average energy consumption per packet by 47.71% when the attack is set to 40% in comparison with ERS mechanism. An average energy consumption per packet reduction of 40.032% is achieved using ERCAD in comparison with ERS mechanism.

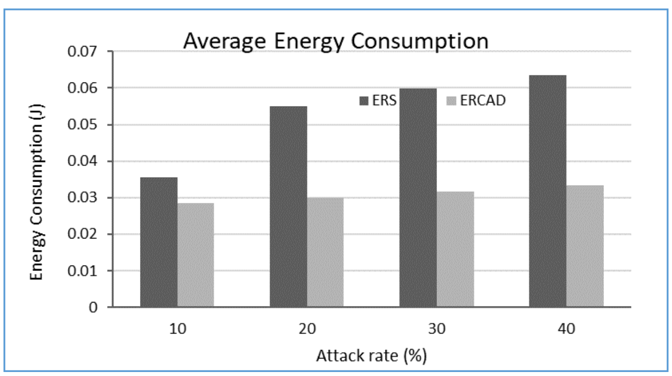

Fig 6. Energy consumption vsattack rate

3.6 Results and Discussions

From all the above results, it can be seen that our Efficient Reputation-based Cyber-Attack Detection (ERCAD) model presents better results when compared with the existing reputation-based security (ERS) models in terms of attack detection rate, attack detection failure rate, throughput performance, communication overhead, and energy consumption. As the ERS models are not efficient in the dynamic environment and cannot provide better performance in terms of feedback reliability, our model provides this by the detection of the attack using the oscillating device which exhibits whether the attack incoming is good or bad for the system. This reduces the failure rate of the model and increases the performance of the model. Moreover, the

ERCAD improves detection rate by 22.04% and reduces the detection failure by 33.89%, achieves better throughput by 22.4%, reduces communication overhead by 33.46%, and improves energy efficiency by 40.03% in comparison with ERS model; thus, ERCAD assures higher reliability in comparison with ERS models.

4 Conclusion

This work mainly focuses to provide a security model for the IoT devices which reduce the cyber-attacks in the IoT devices for the Big Data Environment. Hence, this paper presents an Efficient Reputation-Based Cyber-Attack Detection (ERCAD) mechanism for the Big Data Environment. In this paper, first, we have presented the various works and drawbacks of the Existing Reputation-Based Security (ERS) models. From the drawbacks, we have concluded that the existing system lacks a good attack detection rate and has no method to classify the malicious nodes that are incoming to the IoT nodes. Moreover, the ERS models have no proper means of security to reduce the attack detection failure rate. Moreover, the Existing Reputation-Based Security (ERS) models are not efficient when the device exhibits dynamic behavior and also are not efficient in modeling feedback reliability, and poor reliability. Hence, looking at all the drawback of the ERS models, we have presented a reputation model which reduces the attack detection failure rate and increase the attack detection rate. Moreover, to provide better security to the model, the ERCAD model provides a trust-based security model and a feedback-based model. Furthermore, our ERCAD model achieves a very good attack detection rate of 22.04% with a minimum detection failure rate of 33.89% for a wide range of attacks in comparison with Existing Reputation-Based Security (ERS) models. Moreover, the ERCAD improves throughput by 22.40% and with a reduction of energy consumption of 40.032% in comparison with Existing Reputation-Based Security (ERS) models and also is highly reliable by assuring QoS and security together. However, the ERCAD model is also efficient in detecting oscillating devices (i.e., exhibiting good and bad behavior together). Hence, our ERCAD mechanism achieves very good detection accuracy, less false classification, better throughput, less latencies, and high energy efficiency.

Future work would consider improving reputation metrics considering highly dynamic users. Furthermore, future work would be to present communication metrics that can reduce overhead among the good user and also maintain the reliability requirement of Bigdata applications.

References

1) Awan KA, Din IU, Almogren A, Guizani M, Khan S. StabTrust—A Stable and Centralized Trust-Based Clustering Mechanism for IoT Enabled Vehicular Ad-Hoc Networks. *IEEE Access*. 2020;8:21159–21177. Available from: https://dx.doi.org/10.1109/access.2020.2968948.
2) Kalkan K. SUTSEC: SDN Utilized trust based secure clustering in IoT. *Computer Networks*. 2020;178:107328–107328. doi:10.3390/fi13020048.
3) Yuan J, Li X. A Reliable and Lightweight Trust Computing Mechanism for IoT Edge Devices Based on Multi-Source Feedback Information Fusion. *IEEE Access*. 2018;6:23626–23638. Available from: https://dx.doi.org/10.1109/access.2018.2831898.
4) Jing X, Yan Z, Pedrycz W. Security Data Collection and Data Analytics in the Internet: A Survey. *IEEE Communications Surveys & Tutorials*. 2019;21(1):586–618. Available from: https://dx.doi.org/10.1109/comst.2018.2863942.
5) Du Y, Wang Z, Leung VCM. Blockchain-Enabled Edge Intelligence for IoT: Background, Emerging Trends and Open Issues. *Future Internet*. 2021;13(2):48–48. Available from: https://dx.doi.org/10.3390/fi13020048.
6) Nguyen DC, Pathirana PN, Ding M, Seneviratne A. Secure Computation Offloading in Blockchain Based IoT Networks With Deep Reinforcement Learning. *IEEE Transactions on Network Science and Engineering*. 2021;8(4):3192–3208. Available from: https://dx.doi.org/10.1109/tnse.2021.3106956.
7) Narayan BD, Vineetha P, Alluri BKR. Enhanced trust-based cluster head selection in wireless sensor networks. *Innovations in Computer Science and Engineering*;2019:263–275. doi:10.1007/978-981-13-7082-3_31.
8) Roman R, Lopez J, Mambo M. Mobile edge computing, Fog et al.: A survey and analysis of security threats and challenges. *Future Generation Computer Systems*. 2018;78:680–698. Available from: https://dx.doi.org/10.1016/j.future.2016.11.009.
9) Li W, Wu J, Cao J, Chen N, Zhang Q, Buyya R. Blockchain-based trust management in cloud computing systems: a taxonomy, review and future directions. *Journal of Cloud Computing*. 2021;10(1):1–34. Available from: https://dx.doi.org/10.1186/s13677-021-00247-5.
10) Najib W, Sulistyo S, Widyawan. Survey on Trust Calculation Methods in Internet of Things. *Procedia Computer Science*. 2019;161:1300–1307. Available from: https://dx.doi.org/10.1016/j.procs.2019.11.245.
11) Xiao L, Ding Y, Jiang D, Huang J, Wang D, Li J, et al. A Reinforcement Learning and Blockchain-Based Trust Mechanism for Edge Networks. *IEEE Transactions on Communications*. 2020;68(9):5460–5470. Available from: https://dx.doi.org/10.1109/tcomm.2020.2995371.
12) Gao H, Ma Z, Luo S, Wang Z. BFR-MPC: A Blockchain-Based Fair and Robust Multi-Party Computation Scheme. *IEEE Access*. 2019;7:110439–110450. Available from: https://dx.doi.org/10.1109/access.2019.2934147.
13) Debe M, Salah K, Rehman MHU, Svetinovic D. IoT Public Fog Nodes Reputation System: A Decentralized Solution Using Ethereum Blockchain. *IEEE Access*. 2019;7:178082–178093. Available from: https://dx.doi.org/10.1109/access.2019.2958355.
14) Liu H, Zhang P, Pu G, Yang T, Maharjan S, Zhang Y. Blockchain Empowered Cooperative Authentication With Data Traceability in Vehicular Edge Computing. *IEEE Transactions on Vehicular Technology*. 2020;69(4):4221–4232. Available from: https://dx.doi.org/10.1109/tvt.2020.2969722.
15) Zhang X, Lu R, Shao J, Zhu H, Ghorbani AA. Secure and Efficient Probabilistic Skyline Computation for Worker Selection in MCS. *IEEE Internet of Things Journal*. 2020;7(12):11524–11535. Available from: https://dx.doi.org/10.1109/jiot.2020.3019326.
16) Khan M. BigData Analytics Techniques to Obtain Valuable Knowledge. *Indian Journal of Science and Technology*. 2018;11(14):1–14. doi:10.17485/ijst/2018/v11i14/120977.

17) Priya B, Gnanasekaran T. Optimization of Cloud Data Center using CloudSim – A methodology. *2019 3rd International Conference on Computing and Communications Technologies (ICCCT)*. 2019;2019:307–310. doi:10.1109/ICCCT2.2019.8824950.