SECURE EFFICIENT TASK COMMUNICATION MECHANISMS FOR BIG DATA ENVIRONMENT

*Vinod Desai (1) *, Dr. Dinesha Hagare Annappaiah (2)*

(1) Department of Computer Science and Engineering (Artificial Intelligence and Machine Learning), BLDEA's V P Dr. PG Halakatti College of Engineering & Technology, Vijayapura, India
(2) Department of Computer Science and Engineering, Shridevi Institute of Engineering and Technology, Tumkur, Founder and Director, Cybersena (R&D) India Private Limited, Shreenagar, Belagavi, 590016
India

* Corresponding Author, e-mail: desaivinod2021@gmail.com

Abstract: In this paper, a Secure Efficient Task Communication (SETC) Mechanism for Bigdata environment has been proposed. The SETC mechanism detects the oscillating device efficiently (detects the good and bad behavior of the node). The results have been compared with the current reliability-based security methods. The SETC method has achieved very good detection rate, reduced the detection failure rate, and provided high reliability in comparison to the current reliability-based security methods. It has been seen that the current reliability-based security methods fail to address the issue of the dynamic behavior of the sensor nodes and feedback-reliability. In addition, in comparison to the conventional cryptography-based authentication method, the reputation-based security system is far more effective at determining the behavior of the user.

Key words: Heterogeneous BigData environment, Multi-objective parameter, Trust management mechanism, Secure communication, Reliability, Reputation evaluation system.

1. INTRODUCTION

The main issue of handling Bigdata includes data storage and management, integrity, confidentiality, privacy, and security. Security issues for Bigdata and IoT have been also been considered open research issues. Security in Bigdata is difficult because it must account for both online and offline attacks. Data maintained online could be stolen, malware can encrypt files, and attacks caused due to the Distributed

Denial-of-Service (DDoS) can bring down the entire site. This problem could be problematic for businesses in which the information that is being held is private or perhaps even confidential, like information about a user's contact information, credit card information, or even details regarding the user's financial transactions. Such attacks result in significant losses for the organization, which may lead to financial difficulties. The information can be protected in a variety of different ways by utilizing the Bigdata security procedures in a variety of different ways. In addition, there is a wide variety of attacks that are currently utilized to obtain information from the Bigdata server. As a result of these problems, this is of extreme significance to provide security for the Bigdata workflows when the tasks are being executed or are transferred from one node to another node. In this paper, a secure and efficient task communication mechanism is presented for the execution data intensive workflows in the Bigdata environment encompassing IoT, edge, and cloud platforms. In addressing the research limitation in the next section a brief literature survey about the existing system has been given. The proposed Secure Efficient Task Communication (SETC) method has reduced the detection failure-rate and attains a high attack-detection rate in comparison to the existing reputation-based security methods. The SETC method increases the throughput and reduces the consumption of energy in comparison to the existing reputation-based security methods. The SETC method provides more reliability by providing better security and QoS.

2. LITERATURE SURVEY

In this section, various security methods have been used for the execution of the workflow in the Bigdata environment. A trustworthy and light weight trust method for Internet of Things edge devices has been presented in [1], and it is based on the fusion of information from several sources of feedback. In the initial stage of this method, they used global-trust evaluation. Hence, this makes their trust evaluation method more dependable. After this, they used a light-weight trust evaluation method for providing cooperation among the IoT-edge devices. This approach is well-suited for large-scale IoT-edge computing devices. In [2], a blockchain-based-trust method for helping the Mobile-Edge-Computing (MEC) has been proposed which deals with selfish edge assaults and faked service record attacks. By using the trust assignment technique, the edge-trust method selects the miner of a given blockchain, which applies two consensus protocols for appending the trust of the new service to the Mobile-Edge-Computing blockchain. To further enhance the performance of the computation, they have used a reinforcement-learning-based on-edge CPU allocation method. In [3], they have proposed a blockchain-based SD-CPS architecture to provide security during the offloading of the task to edge computing [4]. Moreover, they have created a resource management strategy for lowering the latency of the system and to provide the adaptability of cooperation to adaptively apply a control strategy and offloading strategy while assuring data security. With the help of deep-reinforcement learning, they have optimized the

allocation of resources, reduced the latency, and ensured data security by formulating the combined computation, communication, and consensus issues as a Markov-Decision-process.

A trust-based clustering approach has been proposed in [5], which enables clusters to identify a trustworthy cluster-head. The proposed approach has several innovative features, one of which is a trust-based cluster head selection process that takes into account the reputation, experience, and knowledge of the node. Additionally, a backup-head is established by conducting a trusted analysis on each node that makes up a cluster. In [6], they have proposed three distinct layers of security using a multi-tier trust-management method for dealing with the problem of malicious automobiles in a vehicle ad-hoc-network. A value of the trust has been allotted to each vehicle in the vehicle ad-hoc-network by the first tier. This value is determined by a variety of factors, including the time required for processing, packet loss, and information on the previous vehicle. In [7], a clustering technique was developed to ensure quality and safety during cluster creation using previously determined Quality-of-Service (QoS) criteria. For solving the problem of managing the trust between edges and the difficulty in distinguishing malicious from safe nodes that are initiating weak attacks, in [8], the researchers present a method of preventing attacks during the transmission of reputation at the network's boundary. Additionally, a solution for good intrusion network security has indeed been developed to alleviate the adverse impacts of attacks on customer interaction and boost the overall reputation performance and process integrity of edge intelligent systems. In [9], the authors attempted to decrease the network latencies of edge devices linked with Cyber-Physical-System (CPS) even though concurrently taking into consideration the criteria for security and dependability. Though the existing reputation-based method has achieved good security performance; however, these models have failed to detect biased attacks [10] where the device keeps changing its behavior state from normal to malicious and vice versa; further, failed to consider load balancing as a result of performance if degraded. In [11], they have proposed an energy-efficient data-transmission method for the IoT environment but have failed to address the security during task communication. In addressing the research limitation in the next section secure and efficient task communication mechanism is presented.

The contribution of Secure Task Communication Mechanisms for the BigData environment method has been given as follows.

- The SETC method has reduced the rate of detection failure and attains a high rate of attack-detection in comparison to the existing reputation-based security methods.
- The SETC method increases the throughput and reduces the consumption of energy in comparison to the existing reputation-based security methods.
- The SETC method provides more reliability by providing better security and QoS.

3. SECURE AND EFFICIENT TASK COMMUNICATION MECHANISM FOR BIG DATA ENVIRONMENT

3.1. System Model

This section presents a system model for data-intensive workflow execution under Bigdata computational platform encompassing IoT devices, edge-server, and the cloud environment as shown in Figure 1. The IoT devices communicate the workflows through intermediate IoT devices towards the edge server for executing workflows. The edge servers either execute the workflows or offload them to the cloud server to execute the workflows. The frequent offloading of data from IoT devices to edge-server and cloud environments and the wireless nature of IoT and edge-server environments lead to possible intermediate data attacks. Existing methodologies have adopted cryptography methods to mitigate intermediate data attacks; however, the limited battery and computational capability of IoT devices limit the usage of such methods. On the other side reputation-based provides an effective mechanism to provide security in the Bigdata environment. Nonetheless, the existing method fails to detect the biased attack, and poor load-balancing further impact the workflow execution performance. In addressing research problems, a Secure and Efficient Task Communication (SETC) mechanism for Bigdata environment employing effective reputation metrics and load-balancing modelling is presented.

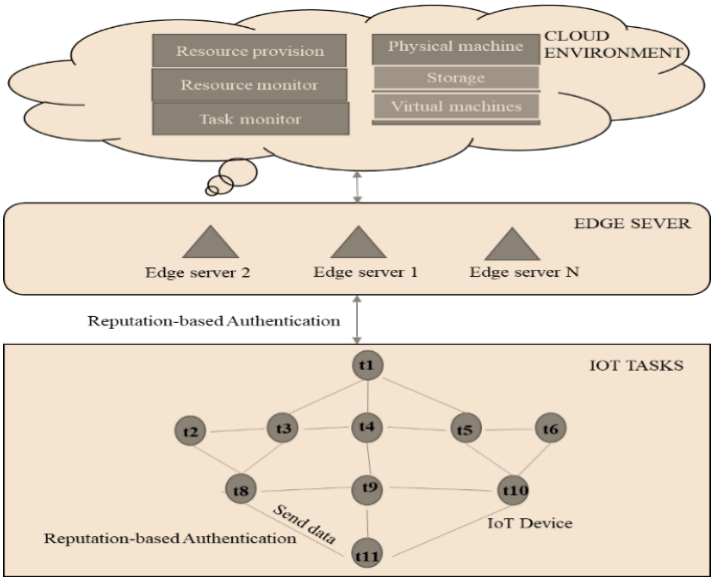

Figure. 1. Architecture for Secure and Efficient Task Communication Mechanism for Big Data environment.

3.2. Reputation Metric

The reputation metrics have been taken from the previous work [12]. In this proposed work first, we compute the explicit reputation metric $\mathbb{L}_o^u(x,y)$ between any two communicating devices i.e., x and y within one-hop neighbour considering u^{th} session instance using the following equation

$$\mathbb{L}_o^u(x,y) = Sec_o^u(x,y). \tag{1}$$

The parameter $Sec_o^u(x,y)$ defines reputation given by device x on device y and vice versa (i.e., positive reward and negative reward for the good and bad experience, respectively). Then implicit reputation metrics $\mathbb{G}_o^u(x,y)$ is computed for obtaining the global trust of different devices with respect to each other for minimizing selfish behavior using the following equation

$$\mathbb{G}_o^u(x,y) = \begin{cases} \dfrac{\sum_{p\in Z-\{x\}} \mathbb{F}_o^u(x,p) * \mathbb{L}_o^u(x,y)}{\sum_{p\in Z-\{x\}} \mathbb{F}_o^u(x,p)}, & if\ |Z-\{x\}| > 0, \\ 0, & if\ |Z-\{x\}| = 0. \end{cases} \tag{2}$$

where $\mathbb{F}_o^u(x,p)$ defines reputation trustworthiness given by a device x on p, $Z = \mathbb{S}(y)$ signifies IoT device set that has associated with IoT device y. The current reputation metrics $\mathbb{C}_o^u(x,y)$ is used for measuring the current security level of devices and is computed using the following equation

$$\mathbb{C}_o^u(x,y) = \delta * \mathbb{L}_o^u(x,y) + (1-\delta) * \mathbb{G}_o^u(x,y) \tag{3}$$

Where δ represents the weights to optimize the recent reputation metric

The past reputation metric $\mathbb{i}_o^u(x,y)$ is used for measuring the past behavior of devices and is measured using the following equation

$$\mathbb{i}_o^u(x,y) = \frac{\varphi * \mathbb{i}_{o-1}^u(x,y) + \mathbb{C}_{o-1}^u(x,y)}{2}, \tag{4}$$

where $\mathbb{i}_0^0(x,y) = 0$ as well as $\varphi(0 \le \varphi \le 1)$ represents the rewarding parameter and to reduce storage overhead exponential mean update mechanism is employed. The anticipated reputation metric $F_o^u(x,y)$ is used for measuring how secure a device will be in the future and is computed using the following equation

$$F_o^u(x,y) = \begin{cases} 0, if\ neither\ \mathbb{i}\ or\ \mathbb{C}\ is\ available \\ \alpha\mathbb{C}_o^u(x,y) + (1-\alpha)\mathbb{i}_o^u(x,y)\ if\ either\ \mathbb{i}\ or\ \mathbb{C}\ is\ available \end{cases} \tag{5}$$

In the above equation, the parameter α is defined for dynamically optimizing a device to come out of experience reputation. However, in a big data setting, the risk of a malicious node turning good should not be underestimated, since this could have a negative impact on the efficiency with which workflows are executed, hence the α should be always high. In removing biased attacks unfair and oscillating reputation metrics $\mathbb{D}_o^u(x,y)$ is computed using the following equation

$$\mathbb{D}_o^u(x,y) = \begin{cases} \mathbb{D}_{o-1}^u(x,y) + \frac{\mathbb{C}_o^u(x,y) - \mathbb{L}_o^u(x,y)}{\rho},\ if \mathbb{C}_o^u(x,y) - \mathbb{L}_o^u(x,y) > \tau \\ \mathbb{D}_{o-1}^u(x,y) + \mathbb{L}_o^u(x,y) - \mathbb{C}_o^u(x,y),\ if \mathbb{C}_o^u(x,y) - \mathbb{L}_o^u(x,y) > -\tau \\ \mathbb{D}_{o-1}^u(x,y),\ otherwise, \end{cases} \tag{6}$$

where τ represents the parameter for tolerance which is used to optimize the reliability and $\rho(\rho > 1)$ represents the penalty-factor which helps for bounding the oscillation. Then, the biased attack is computed through the following equation

$$\bar{\bar{\mathbb{D}}}_{o}^{u}(x,y) = \begin{cases} 0, & \text{if } \mathbb{D}_{o}^{u}(x,y) > \mathbb{D} \\ \cos\left(\frac{\pi}{2} * \frac{\mathbb{D}_{o}^{u}(x,y)}{\max \mathbb{D}_{o}^{u}(x,y)}\right), & \text{otherwise,} \end{cases} \quad (7)$$

Algorithm 1. Choosing the node (x, T) for communication
Input. Computing node x and nodes set replying to a communication request T
Output. Communication provider node y
Start
$\forall\ p \in T$ **do**
  estimate Reputation(x, p)
  if Reputation$(x, p) > \mathcal{T}$ **then**
    $H \leftarrow H \cup \{p\}$
  Else
    $V \leftarrow V \cup \{p\}$
  End if
End $\forall$
If $h \neq \emptyset$ **then**
  $\forall\ p \in H$ do
    Estimate load $O(x, p)$
  End $\forall$
  sort H in ascending order with respect to traffic O
  Get node y with the least traffic O
Else
  Total_Reputation$\leftarrow$ 0
  $\forall\ p \in V$ do
    Total_Reputation$\leftarrow$Total_Reputation + Reputation(x, p)
  End $\forall$
  If Total_Reputation$>$ 0 **then**
    $\forall\ p \in V$ do
      Estimate $\mathcal{P}(x, p)$
    End $\forall$
    Get node y with probabilities $\mathcal{P}(x, y)$
  Else
    Get randomly any node y
  End if
End if
Stop

3.3. Secure and Efficient Load Balancing Mechanism

The algorithm to execute the given workflow securely and assure efficiency through load balancing is given in Algorithm 1. The process of secure and efficient

task communication mechanism is given in Algorithm 1. Using Eq. (5) and (7) the final security metrics $\mathcal{F}_o^u(x,y)$ is defined through the following equation

$$\mathcal{F}_o^u(x,y) = F_o^u(x,y) * \mathbb{D}_o^u(x,y). \quad (8)$$

Using the above equation, the device with a higher $\mathcal{F}_o^u(x,y)$ is chosen for communication as defined below

$$max \sum_{p \in Z-\{x\}} \mathcal{F}_o^u(x,y) \quad (9)$$

However, always sending the information through a secure device will cause performance issues; in addressing an effective load balancing mechanism is introduced by analyzing the traffic of each IoT device using the following equation

$$\mathcal{T}^{\mathrm{u}}(\mathrm{x},\mathrm{y}) = \mathbb{T}^{\mathrm{u}}(\mathrm{x},\mathrm{y}) + \sum_{\mathrm{p} \in \mathrm{Z}-\{\mathrm{x}\}} \mathbb{F}_{\mathrm{o}}^{\mathrm{u}}(\mathrm{x},\mathrm{p}) * \mathbb{T}^{\mathrm{u}}(\mathrm{p},\mathrm{y}) \quad (10)$$

where $\mathbb{T}^u(x,y)$ defines the number of associations between IoT devices x and y. Then, the IoT device is selected using the following equation

$$\min \sum_{\mathrm{p} \in \mathrm{Z}-\{\mathrm{x}\}} \mathcal{T}^{\mathrm{u}}(\mathrm{x},\mathrm{p}) \quad (11)$$

If an IoT device is added to the workflow execution environment; in such case, the IoT device will not have any reputation value; considering the scenario, the node is chosen in an arbitrary manner using the following equation

$$\mathcal{P}^u(x,y) = \begin{cases} \dfrac{\mathcal{F}_o^u(x,y)}{\sum_{p \in V} \mathcal{F}_o^u(x,p)}, & if \sum_{p \in V} \mathcal{F}_o^u(x,p) \neq 0, \\ arbitrarly\ choose\ any\ sensor\ device, & else. \end{cases} \quad (12)$$

From Equation (12), the communication starts from the IoT nodes to the V, where the IoT device has the maximum value and nodes have 0 trust, due to which it randomly chooses the node and starts the communication. The proposed SETC method reduces the rate of failure for the attack-detections when evaluated with the existing reputation-based methods which have been discussed in the next section.

4. SIMULATION RESULT AND ANALYSIS

In this section, the results have been simulated and compared with the other current reputation-based security methods [9], [10]. For simulation, the SENSORIA tool has been used as well as CloudSim [13] has been used to integrate the cloud layer. The Cybershake real-time simulated workflows are used for experiment analysis. More detail on the workflows used is given in [14]. For evaluation of the model, the rate of attack-detection, rate of failure for attack detection, throughput, and ROC curve have been plotted. The area for the simulation area to gather the information was set to 100m×100m, there are a total of 4 edge servers, and there are 1000 IoT devices. The attack rate ranges from 10% to 40%, the Internet of Things devices communicate using IEEE 802.11b MAC, the range for communication was made to 6 metres, the range for sensing range was made to 3 metres, the IoT devices' initial energy ranges from 0.05 to 0.2 Joules (j), the bandwidth is set to 10000 bit/s.

The length of a data-packet was set to 2000 bits, and the length of a control packet is 248 bits. Sensing happens every 0.1 seconds, and the amount of energy used for idle and amplification is set to 50 nJ/bit and 100 pJ/bit/m2, respectively

4.1. Attack detection rate vs attack rate

The rate for attack-detection vs attack-rate has been evaluated by comparing the results with the ERS [9], and ERCAD [10] methods with our proposed SETC method which has been given in Figure 2. The SETC method increases the rate for detection by 13.33% when compared with ERS method and the detection-rate for the ERCAD and SETC are the same for the 10% attack rate. The SETC has a better detection-rate of 25.37% when compared with the ERS method and when compared with the ERCAD method, it shows a better detection-rate of 3% for 20% of the attack rate. Further, for the 30% of the attack rate, the SETC attained an 18.03% better attack detection rate when compared with the ERS and a 3% better detection-rate when compared with the ERCAD method. The SETC method attained better results for the 40% of attack rate having a 17.105% of better detection rate when compared with the ERS method and the ERCAD model attained a 1% better attack detection rate. Based on these outcomes, it is clear that the suggested SETC method outperforms the state-of-the-art approaches to reputation-based security.

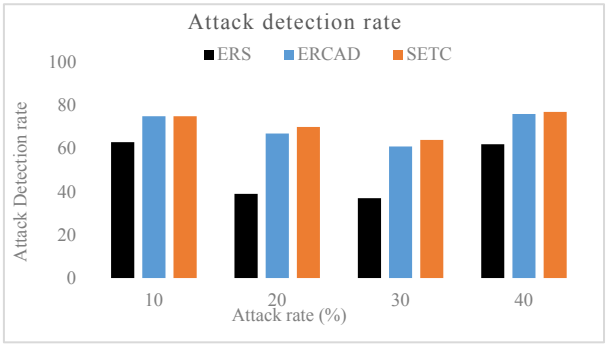

Figure 2. Rate of Attack detection rate vs rate of attack (%).

4.2. Rate of failure for Attack detection vs varied rate of attack

The rate of failure for attack detection vs varied rate of attack has been evaluated by comparing the results with the ERS [9], ERCAD [10] methods with our proposed SETC method which has been given in Figure 3. The SETC method increases the rate of failure for attack detection by 28.57% when compared with ERS method and the rate of failure for attack detection for the ERCAD and SETC is the same for the 10% attack rate. The SETC has a better rate of failure for attack detection of 34.0% in comparison to the ERS method and when compared with the ERCAD method, it shows a better attack-detection failure-rate of 3% for 20% of attack rate. Further, for the 30% of the attack rate, the SETC attained a 22.0% better rate of failure for attack detection in comparison to the ERS and a 3% better rate of failure for attack detection

in comparison to the ERCAD method. The SETC method attained better results for the 40% of attack rate having a 51.02% of better rate of failure for attack detection in comparison to the ERS method and the ERCAD model which attained a 1% better attack-detection failure-rate. Based on these outcomes, it is clear that the suggested SET method outperforms the state-of-the-art approaches to reputation-based security.

4.3. Throughput performance vs attack rate

The throughput has been evaluated by comparing the results with the ERS [9], ERCAD [10] methods with our proposed SETC method which has been shown in Figure 4. The SETC method achieves a throughput of 0.555 whereas the ERS method attains 0.4662 and the throughput for the ERCAD and SETC are the same for the 10% attack rate. The SETC has attained a throughput of 0.371 when compared with the ERS method, it attained a throughput of 0.2067 and when compared with the ERCAD method, it shows attained throughput of 0.3685 for 20% of attack rate. Further, for the 30% of the attack rate, the SETC attained 0.2816 throughputs whereas the ERS attained a throughput of 0.1628 and 0.2501 throughputs was attained by the method. The SETC method attained better results for the 40% of attack rate having 0.1848 throughput, whereas for the ERS method, it attained a throughput of 0.1488 and for the ERCAD model it attained a throughput of 0.1672. Based on these outcomes, it is clear that the suggested SETC method outperforms the state-of-the-art approaches to reputation-based security.

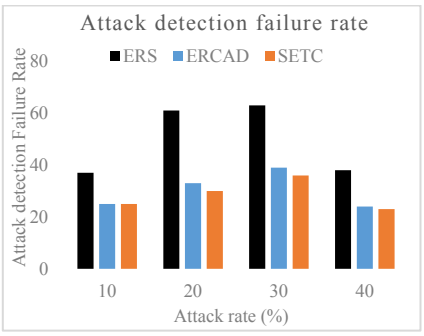

Figure 3. Attack detection failure rate vs attack rate (%).

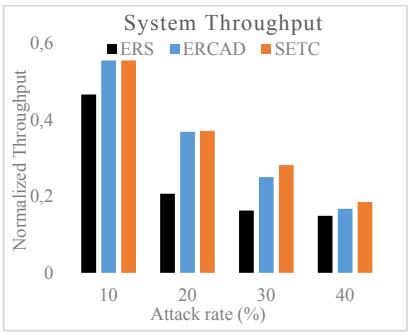

Figure 4. Throughput vs attack rate.

4.4. ROC Curve

In this section, the ROC curve for the current ERS [9] (ES) method and the SETC (PS) method have been given. The simulation for the attack has been done by varying the 10% to 40%, having an interval of 10% for the ROC Curve. In Figure 5, Figure 6, Figure 7, and Figure 8, the ROC curve for the 10% attack rate, 20% attack rate, 30% attack rate, and 40% attack rate has been given. From all the ROC curves it can be seen that the ROC curve attains better results for the proposed SETC method

while the ERS method fails to attain better performance for 10% attack rate, 20% attack rate, 30% attack rate, and 40% attack rate.

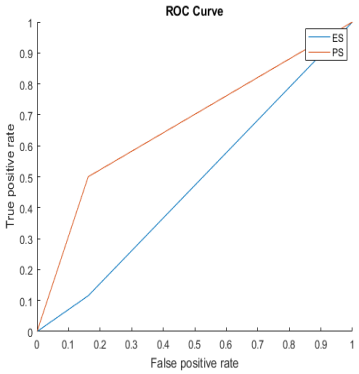

Figure 5. ROC curve for 10% of attack rate.

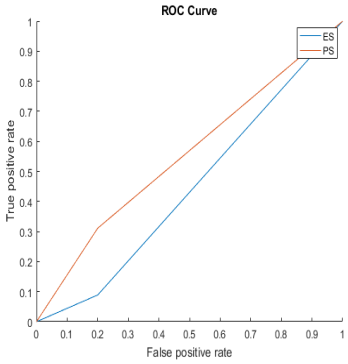

Figure 6. ROC curve for 20% of attack rate.

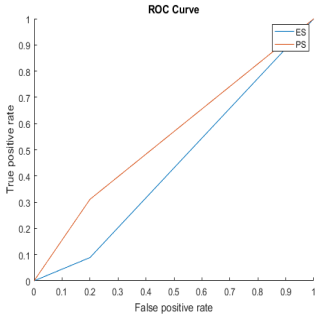

Figure 7. ROC curve for 30% of attack rate.

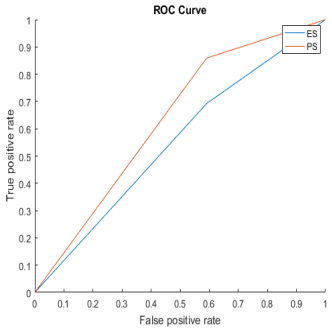

Figure 8. ROC curve for 40% of attack rate.

5. CONCLUSION

The current reputation-based security methods do not provide good performance in terms of feedback reliability, dynamic behavior and provide very less reliability. Nevertheless, the SETC method provides better performance for the detection of the oscillating device (detects the good and bad behavior of the node). The results have been compared with the current reputation-based security method. The SETC model attains good accuracy for the detection, reduced false classification and higher throughput. The SETC increases the rate of detection by 22.04%, minimizes the failure detection by 33.89% and attains higher throughput of 22.4% when compared with the ERS method. Hence, the SETC method provides better reliability when compared with the existing models. Future work would focus on designing efficient resource allocation design for edge cloud-platform to reduce the cost of service provisioning. Further, improve security with balanced cost-based resource

offloading design for an edge-cloud platform for real-time execution of big data workflows

REFERENCES

[1] J. Yuan and X. Li. A Reliable and lightweight trust vomputing mechanism for IoT edge devices based on multi-source feedback information fusion. *IEEE Access*, vol. 6, 2019, pp: 23626-23638. doi: 10.1109/ACCESS.2018.2831898.

[2] L. Xiao et al. A Reinforcement learning and blockchain-based trust mechanism for edge networks. *IEEE Transactions on Communications*, vol. 68, no. 9, 2020, pp : 5460-5470. doi: 10.1109/TCOMM.2020.2995371.

[3] D. Wang, N. Zhao, B. Song, P. Lin and F. R. Yu. Resource management for secure computation offloading in softwarized cyber–physical systems. *IEEE Internet of Things Journal*, vol. 8, no. 11, 2021, pp. 9294-9304. doi: 10.1109/JIOT.2021.3057594.

[4] M. Kong, J. Zhao, X. Sun and Y. Nie. Secure and efficient computing resource management in blockchain-based vehicular fog computing. *China Communications*, vol. 18, no. 4, 2021, pp. 115-125. doi: 10.23919/JCC.2021.04.009.

[5] Awan, Kamran Ahmad & Ud Din, Ikram & Al-Mogren, A.s & Guizani, Mohsen & Khan, Sonia. StabTrust - A stable and centralized trust-based clustering mechanism for IoT enabled vehicular ad-hoc networks. *IEEE Access*, 2020, pp: 1-1. 10.1109/ACCESS.2020.2968948.

[6] Akwirry, B.; Bessis, N.; Malik, H.; McHale, S. A multi-tier trust-based security mechanism for vehicular ad-hoc network communications. *Sensors*, vol. 22, 2022, pp. 8285. https://doi.org/10.3390/s22218285.

[7] Awan, K.A.; Din, I.U.; Almogren, A. A blockchain-assisted trusted clustering mechanism for IoT-enabled smart transportation system. *Sustainability,* vol. 14, 2022, pp 14889. https://doi.org/10.3390/su142214889.

[8] Boran Yang, Dapeng Wu, Ruyan Wang, Zhigang Yang, Yu Yang, A fine-grained intrusion protection system for inter-edge trust transfer. *Digital Communications and Networks*, 2022, https://doi.org/10.1016/j.dcan.2022.11.007.

[9] Dan Wang, Bin Song, Yingjie Liu, Mingjun Wang. Secure and reliable computation offloading in blockchain-assisted cyber-physical IoT systems. *Digital Communications and Networks*, vo. 8, no. 5, 2022, pp: 625-635. https://doi.org/10.1016/j.dcan.2022.05.025.

[10] Desai V, Dinesh HA. Efficient reputation-based cyber attack detection mechanism for Big Data environment. *Indian Journal of Science and Technology*, vol. 15, no. 13, 2022, pp:592-602. https://doi.org/10.17485/IJST/v15i13.2102.

[11] Naveen Kumar, D. Annapurna. Energy efficient data transmission model for Internet of Things application, *International Journal on Information Technologies and Security*, vol. 14, No. 2, 2022, pp. 3-14.

[12] Desai V, Dinesh HA. Efficient reputation-based cyber attack detection mechanism for Big Data environment. *Indian Journal of Science and Technology*. vol. 15, no. 13, 2022, pp:592-602. https://doi.org/10.17485/IJST/v15i13.2102

[13] Le, D.-N., Pal, S. and Pattnaik, P.K. Cloudsim: A simulator for cloud computing environment. *Cloud Computing Solutions*, 2022. https://doi.org/10.1002/9781119682318.ch16

[14] A Yajie Lee, A Christine Goulet, A Zhenghui Hu, A Ronald T. Eguchi T. Impact of CyberShake on risk assessments for distributed infrastructure systems. *B Lifelines*, 2022, pp: 869-879, doi:10.1061/9780784484432.077.

Information about the authors:

Vinod Desai is presently working as Assistant Professor in Dept. Of Computer Science and Engineering (Artificial Intelligence and Machine Learning) in B.L.D.E. A's V.P. Dr.P.G.Halakatti College of Engineering and Technology Vijayapura. He is pursuing his Ph.D in Cyber Security and Machine Learning under Visvesvaraya Technological University Belagavi in Computer Science and Engineering.

Dr. Dinesha Hagare Annappaiah is an M. Tech, Ph.D, and Professor in Department of Computer Science and Engineering, Shridevi Institute of Engineering and Technology. He is the Founder and Chief Executive Director of Cybersena (R&D) India Private Limited, India in the domain of Cybersecurity and forensic investigations.

Manuscript received on 16 December 2022
Revised paper received on 2 February 2023