

A secure framework for effective workload resource management

Dharuman Salangai Nayagi¹, Hosaagrahara Savalegowda Mohan²

¹Department of Computer and Science Engineering, New Horizon College of Engineering, Visvesvaraya Technological University, Belagavi, India

²Department of Computer and Science Engineering (Data Science), RNS Institute of Technology, Visvesvaraya Technological University, Belagavi-590018, India

Article Info

Article history:

Received Nov 21, 2023

Revised Dec 29, 2023

Accepted Jan 3, 2024

Keywords:

Cybershake

Data management

Internet of things

Montage

Workload

ABSTRACT

An efficient and dynamic role-based access-control (RBAC) model is presented in this work which utilizes access-control for internet of things (IoT) nodes while minimizing storage and computational overhead. Also, for the identification of the malicious packets at the gateway server, a machine learning method has been presented. In addition, a framework for data management techniques in the IoT environment is designed to ensure efficient and secure storage, management, and processing of IoT data. The results have been evaluated by using the Montage and Cybershake workload in terms of energy consumption, processing time, detection accuracy and misclassification rate. The results show that the proposed secure framework for effective workload resource management (SFE-WRM) attains better performance in comparison to the reliable and energy-efficient route selection (REERS) and FTA-WRM method. Also, by using the security method, the proposed method provides better security to the IoT nodes during the data aggregation and processing of the workload. The ultimate aim of this work is to provide a solution for the development of a secure and efficient IoT environment that can address critical security challenges and enable the widespread adoption of IoT devices and services.

This is an open access article under the [CC BY-SA](https://creativecommons.org/licenses/by-sa/4.0/) license.



Corresponding Author:

Dharuman Salangai Nayagi

Department of Computer and Science Engineering, New Horizon College of Engineering

Visvesvaraya Technological University

Belagavi-590018, Karnataka, India

Email: dsalangainayagiresearch@gmail.com

1. INTRODUCTION

The cloud workflow resource management environment typically involves the exchange and processing of sensitive data [1]. This data could be confidential business information, financial records, personal data of customers, or other types of sensitive data that need to be protected from unauthorized access and misuse. Since cloud management systems are susceptible to data leakage, it is essential that the data be secured against any possible intrusions [2]. One way to achieve this is by implementing a robust access-control mechanism which only grants the users to access the data necessary for performing their tasks [3]. By controlling access to data, the workflow management system can prevent unauthorized access or misuse of data, ensuring that only those with legitimate reasons can access the sensitive information [4]. This approach helps to ensure data integrity and protect against potential security breaches that could result in data loss or leakage. In addition, monitoring and tracking the data accessed by employees or users can provide valuable insights into how the data is being used, making it easier to detect any anomalies or signs of

misuse [5]. This can help prevent data breaches by identifying and mitigating security risks before they become more significant issues. In summary, implementing a secure and robust access-control mechanism for cloud workflow management systems is crucial to protect sensitive data and ensure the integrity of the system [6].

By controlling access to data and monitoring data usage, organizations can minimize the risk of data breaches and ensure the safety of their data. Combining edge-computing and cloud in an internet of things (IoT) environment is growing as an effective way to address the challenges of managing and processing the substantial volumes of data generated by the IoT devices [7]. Furthermore, in this environment, while data storage and other services are provided by the cloud, processing occurs at the network's edge, near the point of data generation. This approach offers several benefits, including reduced latency, improved response time, and enhanced scalability. However, this architecture also poses significant security challenges, such as unauthorized access [8], data breaches, and cyber-attacks [9]. One of the key challenges in securing the cloud-edge IoT environment is the need to ensure end-to-end security. Since data is being processed locally before being sent to the cloud, it is vulnerable to interception, modification, and theft. Additionally, the distributed nature of the cloud-edge IoT environment introduces complexities in access-control and authentication [10]. Traditional security mechanisms are often not suitable for this environment, and new approaches are required to address these challenges. Moreover, the diversity of devices, protocols, and interfaces in the cloud-edge IoT environment presents additional challenges for ensuring security [11], [12]. The heterogeneity of devices and protocols increases the complexity of the system, making it challenging to manage and monitor security risks effectively. Therefore, there is a need to develop new security mechanisms that can address the unique challenges of the cloud-edge IoT environment and provide end-to-end security without compromising performance and scalability.

In light of these challenges, the motivation for this work is to provide an efficient and dynamic role-based access-control (RBAC) model for different users/stakeholders with minimal storage and computational overhead. The RBAC model will enable fine-grained access-control for IoT devices and services, and adapt to changes in the IoT environment dynamically. Additionally, the work will design a framework for data management techniques in the IoT environment, to ensure efficient and secure storage, management, and processing of IoT data. The ultimate goal is to provide a secure and efficient IoT-environment that can address critical security challenges and enable the widespread adoption of IoT devices and services. The contribution of the proposed work is to provide a dynamic and efficient RBAC model for different users/stakeholders with minimal storage and computational overhead. The RBAC model in this work is designed to give the best access-control for the IoT devices, IoT data and IoT services. Also, the RBAC can adapt to the dynamic changes in the IoT-environment. This will ensure that only authorized IoT nodes have access to sensitive data and resources, while minimizing the risk of unauthorized access and data breaches. Additionally, in this work provides a complete framework for the data management technique within the IoT-environment. The framework will address the challenges of managing and storing massive volumes of generated data by IoT devices, while ensuring security. Overall, this work provides an efficient and secure IoT-environment by addressing critical challenges in access-control and data management. The RBAC model and data management framework will be designed to be scalable, adaptable, and resilient to ensure long-term viability, security and effectiveness in the rapidly evolving IoT environment.

The manuscript has been organized in the following way. In the second section, different existing reliable route selection methods, resource as well as scheduling management methods for the IoT-environment and secure resource provisioning methods have been discussed. In third section, the proposed model which consists of a dynamic access-control in IoT environment using reputation-based model, enhancing IoT security through machine learning-based malicious packet detection at gateway servers and a secure framework for effective workload resource management (SFE-WRM) has been presented. In fourth section, the results for the proposed model have been compared and discussed. In the fifth section, the results attained by the proposed SFE-WRM have been compared with the existing REERS and FTA-WRM method. Finally in section 5, the conclusion and future work have been discussed.

2. LITERATURE SURVEY

Lenka *et al.* [13], presented a model for the wireless sensor-network (WSN) aided IoT environment called as cluster-based routing protocol with static hub (CRPSH) for reducing the traffic between the sensors to provide better reliability. They have presented a multi-path approach to provide better network reliability. They have evaluated their model in term of packet-delivery ration (PDR), energy-consumption, end-to-end delay (EED) and network-lifetime. They have compared their results with two models, passive cluster-based multipath routing protocol (PCMRP) and reliable and energy-efficient data collection (REDCL) and the simulations show better performance. The presented method has hotspot issues where devices near the hub drain their energy faster than those farther away. Ilyas *et al.* [14], a three-layer WSN clustering technique

called as TBEERP has been proposed which incorporates energy harvesting to extend network lifespan and improve throughput. Each cluster in this technique is equipped with cluster-nodes to detect malicious attacks. Sensor-nodes handles the majority of processing tasks without resource limitations. Extensive simulations were conducted using NS3-simulator for evaluating the efficiency of the TBEERP technique. The results demonstrated its superiority over other techniques n energy aware multi-hop routing (EAMR), artificial bee colony-SD (ABC-SD), fuzzy logic-based unequal clustering and ant colony optimization (ACO)-based routing hybrid (FUCARH) and enhanced three-layer hybrid clustering mechanism (ETLHCM) in terms of network throughput and lifetime, average energy-consumption, network stability and packet-latency.

Joshi and Raghuvanshi [15], introduced an approach aimed at optimizing cluster-head and route-path selection in WSNs. The approach considers multiple objectives, including distance, node energy, and delay. When compared to CRMOGA, the proposed method reduced energy consumption by 27.2% and enhanced network lifetime. The efficient route path selection also leads to increased throughput and PDR. Moreover, the average EED of the network decreases by over 40%, making it faster and suitable for applications such as surveillance and healthcare. Kumar and Zaveri [16], propose a resource-scheduling algorithm specifically designed for post-disaster management. In this work, first they have formulated the problem into a mathematical model and then used queuing-theory based method for solving the problem of resource-scheduling that a user may face during disaster management. They have proposed two algorithms for improving the performance of resource-scheduling. The results have been evaluated in terms of resource-utilization. Parida *et al.* [17], presented a binary self-adaptive salp-swarm-optimization for handling the dynamic load balancing in cloud computing. Results show better response time, makespan and has increase the resource-utilization. Mohapatra [18], discussed about the various issues and challenges faced in smart cities regarding the security of data.

Rahul and Bhardwaj [19], discussed the various existing scheduling techniques such as round-robin, min-min and first come first serve (FCFS). In this work they have analyzed all the parameters utilized in the previous works and then presented a hybrid algorithm to improve the performance. The results were evaluated in terms of processing time, as well as makespan. The results show better performance in comparison to the existing state-of-art works. Yu [20], for solving the issue of providing resources for scheduling in the cloud-environment, a fuzzy algorithm has been proposed. A trust-sensitive mechanism prevents malicious attacks and dishonest recommendations. Cloud task scheduling categorizes resources based on performance and calculates trust sensitivity coefficients to select suitable tasks for users. The proposed fuzzy algorithm in this study minimizes the cost of the user by selecting a cloud-service provider during resource scheduling. Hu *et al.* [21], explain a cloud workflow-scheduling method has been proposed which utilizes an intelligent algorithm. The study focuses on three intelligent algorithms, GA, ACO and PSO and enhances them for optimization. The results demonstrate notable variation in optimal values across different algorithms and test cases, while the overall trend of the optimal solution curve aligns with the mean curve. Lakhan *et al.* [22], explain a MSDSC framework is introduced in this research, emphasizing mobility-aware security in healthcare workflows. Through the utilization of restricted and serverless Boltzmann-machine technique, the framework enhances security measures. A deep neural-network is employed to train models for various aspects, including task-sequencing, service-composition, scheduling and security. The experimentations demonstrate the superiority of these innovative methods over traditional approaches, leading to a remarkable 25% improvement in safety and a significant 35% reduction in application costs.

3. MODEL

IoT devices are equipped with various sensors that rely on battery power to carry out sensing operations. These devices are randomly placed throughout the sensing area which will be continuously transmitting the collected data towards the edge devices, which will further aid the gateway servers as well as the for the cloud-computing environment. For reducing the energy consumption in the IoT-environment, the proposed model utilizes a cluster-based communication technique. Additionally, a multi-path-based communication technique is employed to improve reliability. A basic architecture of the edge-cloud IoT environment consisting of IoT nodes or devices, IoT gateway server and cloud computational environment has been given in Figure 1. In this work, the IoT gateway server removes the node with higher reputation fluctuation with lesser reputation put together that are lesser than reputation threshold from the IoT network. The eliminated nodes are reconfigured by the system administrator and again introduced into the network to take part in communication.

This existing work of Nayagi *et al.* [23] uses a multipath based data transmission network. The previous work mainly focused to transmit the data in the heterogenous environment consuming less energy and increasing lifetime performance of the IoT nodes. Further, the data which has been transmitted has to be stored and processed. Hence, the Nayagi *et al.* [24] presented an FTA-WRM algorithm for real-time

workload in heterogeneous computing environment. Nevertheless, both these models [23], [24] have reduced the energy consumption, yet, failed to provide the security to the IoT nodes. Moreover, the proposed model has not provided any secure framework for the data management in the heterogenous environment. The security is provided using a reputation-based access-control mechanism which has been presented in the next section.

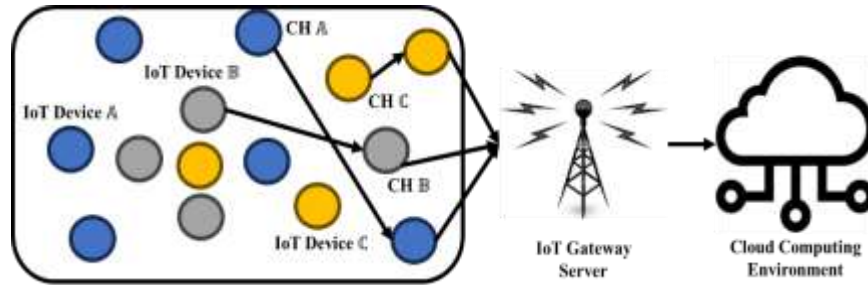


Figure 1. Architecture of edge-cloud IoT environment

3.1. Dynamic access-control in IoT environment using reputation-based model

We present a reputation-based access-control method which will provide security to the IoT nodes. To provide security using the reputation-based access-control method, initially, we have to considered the future reputation of the node. Consider IoT node x and IoT node y , which are connected with other IoT nodes. Assume, a parameter α which will define the relationship between the IoT node x and IoT node y . Assume, the parameter u which will be used for defining the time interval for the execution of the IoT tasks. Moreover, the parameter α defines the number of associations with respect to time u . Thus, the reputation value depends on number of times the node interacted with other nodes considering time u . From this, the future reputation of the node is represented as $F_o^u(x, y)$. The future reputation of the IoT node uses the information of the past reputation and the present reputation of both the IoT nodes, x and y . The future reputation $F_o^u(x, y)$ is estimated by utilizing the given (1).

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

Where, $C_o^u(x, y)$ is the present reputation, $L_o^u(x, y)$ is the past reputation of the IoT nodes and α is used for denoting how the reputation for a IoT node can be attained using the past reputation. The $C_o^u(x, y)$, $L_o^u(x, y)$ and α have been evaluated using [25].

Further, as the IoT nodes are moving and are not stationary at a single place, there may be a chance that the IoT node might get attacked using various kinds of attacks or using other malicious IoT nodes, hence, the oscillating reputation has to be evaluated for the IoT nodes. To address the issue of oscillating reputation, access-control policies can be designed to take into account the history of reputational levels assigned to a node, rather than relying solely on the current reputation level. Consider $\mathbb{D}_o^u(x, y)$ which has been defined to represent the oscillating reputation. Hence, the $\mathbb{D}_o^u(x, y)$ can be described using (2).

$$\mathbb{D}_o^u(x, y) = \begin{cases} \mathbb{D}_{o-1}^u(x, y) + \frac{C_o^u(x, y) - L_o^u(x, y)}{\rho}, & \text{if } C_o^u(x, y) - L_o^u(x, y) > \tau \\ \mathbb{D}_{o-1}^u(x, y) + L_o^u(x, y) - C_o^u(x, y), & \text{if } C_o^u(x, y) - L_o^u(x, y) > -\tau \\ \mathbb{D}_{o-1}^u(x, y), & \text{otherwise,} \end{cases} \quad (2)$$

where, τ has been used to define the tolerance parameter which will optimize the two IoT nodes reliability. In (2) tolerance parameter and penalty function is used to ensure fair reputation assignment. The parameter allows application specific optimization in providing secure workflow execution. Further, to bound the oscillating reputation, a penalty parameter has to be defined. The ρ ($\rho > 1$) in this work has been used for defining the penalty parameter. By using (2), the oscillating reputation can be evaluated by using the given (3).

$$\bar{\mathbb{D}}_o^u(x, y) = \begin{cases} 0, & \text{if } \mathbb{D}_o^u(x, y) > \mathbb{D} \\ \cos\left(\frac{\pi}{2} * \frac{\mathbb{D}_o^u(x, y)}{\max \mathbb{D}_o^u(x, y)}\right), & \text{otherwise,} \end{cases} \quad (3)$$

By using the (1) and (3), the reputation-based access-control level providing security parameter for the IoT-cloud environment can be provided using (4).

$$\mathcal{F}_0^u(x, y) = F_0^u(x, y) * \bar{\mathbb{D}}_0^u(x, y) \quad (4)$$

Where, $F_0^u(x, y)$ is the future reputation and $\bar{\mathbb{D}}_0^u(x, y)$ is the oscillating reputation.

Both these reputational parameters define the weight to provide security to the IoT nodes. Using (1), it can be evaluated that the IoT nodes having better future reputational weight will provide better security, but by using low oscillating weights, the total reputation of the IoT nodes will fall. Also, the reputation value assignment is done by the IoT gateway server; the IoT gateway server maintains a table to keep track of reputation metrics and to enhanced performance efficiency the older reputation value is discarded. For the preventing the proposed weighted average approach for access control inadvertently penalizing nodes that have recovered from past security incidents, this work computes the reputation value in term of logarithm terms to keep the value low and avoid significant fluctuation. This way it ensures that the proposed weighted average approach removes the node which is below the reputation threshold metrics. The IoT gateway server periodically collects and updates the reputation value. Hence, slight overhead is caused; however, the communication failures is reduced significantly improves the workflow execution performance with enhanced secureness.

Moreover, the IoT nodes that intentionally switch states among the biased weights will also have a reduced trust parameter due to the former's tendency to fluctuate. In order for a node within the IoTs to possess a high cumulative reputational parameter, it must first exhibit no significant fluctuations in that parameter and secondly operate in a systematic manner. Hence, to achieve an effective security solution for present heterogeneous IoT systems, a node is going to employ (1) to choose a node having a high trustable parameter. The reputation-based access control mechanism is very effective in detecting distributed denial-of-service (DDOS) and on-off attacks. A higher reputation value can assure effective communication and lower value indicates the system is being impacted severe attacks; thus, data collected is not of that good quality. The reputation metrics requires a certain number of interactions i.e., minimum of 5 interactions to establish the behavior of all the nodes. Further, the model uses the tolerance value to identify node that shows biased behavior in comparison with their anticipated reputation. These, nodes are removed and workflow execution process are initialized. Further, for identifying the malicious packet in the IoT environment, a machine learning model has been proposed in the next section.

3.2. Enhancing IoT security through machine learning-based malicious packet detection at gateway servers

Here for eliminating malicious packet machine learning model is presented. The extreme gradient boosting (XGBoost) method is an algorithm that is used for regression and classification regression tasks, and it can be used for identifying malicious packets at a gateway server in an IoT environment. Further, the XGBoost algorithm is a type of gradient boosting algorithm that builds a series of decision trees, where each new tree is built to correct the errors of the previous tree [26]. This approach allows XGBoost to achieve high accuracy in classification tasks, making it suitable for identifying malicious packets in an IoT environment. The objective function of the XGBoost model is minimized using (5).

$$\text{Obj} = -\frac{1}{2} \sum_{j=1}^t \frac{G_j^2}{H_j + \lambda} + \gamma t \quad (5)$$

Where, G and H are used for representing the total cost function of the first as well as the second-order gradients. t is used for representing the leaves present in the DT. λ and γ are used for denoting the penalty coefficients. As the XGBoost model is constructed by using the outcomes of the DT iterations, all the DT have to be accumulated for attaining high accuracy.

As a result, poor classification accuracy is achieved using standard XGBoost algorithm, in addressing this work presents a modified XGBoost algorithm by identifying features that impact detection accuracy. The feature identification is done through effective cross validation mechanism. In the context of XGBoost, cross-validation is used to determine the optimal hyperparameters of the model. This process helps to identify the best hyperparameters that result in the highest performance on average across all partitions. In addition, cross-validation helps to reduce the variance of the model, which can help to improve its generalization ability. The CV model is constructed by utilizing the different groups of K – folds. For the evaluation of an individual K – fold which has CV, the given (6) is utilized.

$$CV(\sigma) = \frac{1}{M} \sum_{k=1}^K \sum_{j \in G_{-k}} P \left(b_j, \hat{g}_{\sigma}^{-k(j)}(y_j, \sigma) \right) \quad (6)$$

By evaluating of an individual K – fold which has CV, the model fails to attain higher accuracy as the dataset may have imbalanced values. To decrease the error during the CV [27], has presented a CV which has two layers. These two layers consist of important features attained from the dataset as well as the important features which have been chosen by utilizing the previous layer. Both the layers are utilized for the construction of the predictive model. The two-layer CV is done using (7).

$$CV(\sigma) = \frac{1}{SM} \sum_{s=1}^S \sum_{k=1}^K \sum_{j \in G_{-k}} P \left(b_j, \hat{g}_{\sigma}^{-k(j)}(y_j, \sigma) \right) \quad (7)$$

Using the (7), to optimize the parameters of the CV and to select the best value for the parameters of CV, the (8) is used

$$\hat{\sigma} = \underset{\sigma \in \{\sigma_1, \dots, \sigma_l\}}{\text{arg min}} CV_s(\sigma) \quad (8)$$

In (3), the parameter for the gradient loss is represented using $P(\cdot)$. The size of training is represented using M . $\hat{g}_{\sigma}^{-k(j)}(\cdot)$ is utilized for the evaluation of the coefficients. By utilizing the standard XGBoost model and CV model, one can attain better results. For providing security during the processing of the task or the workload, a secure workload resource management (SWRM) has been proposed which has been discussed in the next section.

3.3. A secure framework for effective workload resource management

The secure framework for effective workload resource (SFE-WRM) has been proposed in this work to provide security as well as to reduce the energy during the processing of the task. This is provided using (9).

$$\text{Max} \gamma_l \triangleq \sum_{s=1}^N \gamma_{T_c}(s) + \sum_{s=1}^N \gamma_{M_c}(s) + \sum_{s=1}^N \gamma_{F_c}(s) + \sum_{s=1}^N \gamma_{F_y}(s) \quad (9)$$

Where, $\gamma_{T_c}(s)$ has been used to define the total energy used for processing the task of the IoT node, $\gamma_{M_c}(s)$ is used for defining the energy which has been induced during the communication of the tasks from one IoT node to another IoT nod by considering quality of service (QoS) constraint I_t [24], $\gamma_{F_c}(s)$ has been used for defining the overall reconfiguration cost and γ_{F_y} has been used for defining the service level agreement (SLA) constraints. Hence, in this proposed work, the QoS and SLA constraints have been optimized to attain the best workload execution resource management performance. The next section presents experimental evidence that the SWRM can guarantee excellent performance within the energy constraint requirements of data-intensive workloads.

4. RESULTS AND DISCUSSION

In this section, we discuss the results obtained from the presented SFE-WRM model. The proposed method is studied through simulation study using two different data intensive workflow application. The parameters like detection accuracy and misclassification rate. A higher value indicates better performance. The experimental studies were conducted in a system environment consisting of a Windows 10 operating system, a quad-core processor of Pentium I-7 class, and 16 GB of RAM. For the experimental study, the Sensoria simulator was utilized. To evaluate the performance of SFE-WRM model, a comparison was made with the existing workflow optimization strategy (MOWOS) model [28] in terms of energy consumption, processing time and detection accuracy. The Montage and Cybershake workload has been considered for the processing of the tasks. More information about the Montage and Cybershake workload can be obtained from [29]. The work is tested considering two major attacks like DDOS and on-off attacks. In this work, we provide security to the IoT nodes during the processing of the aggregated information. Initially all the nodes are assumed to be good. i.e. the reputation of all the nodes is kept to 1. In this work, the reputation value is greater and equal to 0.5 is considered as good and any value below 0.5 is considered as bad. Then, workflow application communication is initialized, and the attack rate is at 20%. The attacks are introduced into the network after 10 seconds of workflow application initialization. Then, according to their communication association between different nodes the reputation value is updated. Further, the base station maintains a buffer to keep the past and present reputation value of all the IoT devices. In similar manner to [25], the work uses a local i.e., direct association reputation and global i.e., indirect association reputation and compare the local and global reputation to assure accuracy and reliability by eliminating IoT device that provide wrong

reputation for personal workflow execution benefit. In this work malicious activities are introduced into the network by creating attacks like DDOS and on-off attacks using NSL-KDD dataset [30] on certain IoT device in random manner. In simulation the attack rate is kept at 20%; thus, for 1,000 nodes considering 20% attack rate, 200 nodes will turn malicious, and 800 nodes will behave as normal. Using (4) the nodes that are below reputation threshold i.e., 0.3 will assumed as illegitimate and anything higher are legitimate node.

4.1. Network lifetime performance

In this section, the network lifetime performance been given. The REERS model demonstrates significant improvements in lifetime performance compared to low-energy adaptive clustering hierarchy (LEACH) and energy-efficient and reliable routing (E2R2) models across different numbers of IoT devices. When considering 500 IoT devices, 1,000 IoT devices, 1,500 IoT devices, and 2,000 IoT devices, REERS achieves lifetime performance improvements of 71.64%, 74.90%, 84.76%, and 89.66% over LEACH, respectively. Similarly, REERS shows lifetime performance improvements of 57.27%, 66.87%, 74.167%, and 78.41% over E2R2 for the same number of IoT devices. On average, REERS achieves lifetime performance improvements of 80.24% over LEACH and 69.17% over E2R2. As depicted in Figure 2, the lifetime performance of LEACH and E2R2 decreases as the size of IoT devices increases, whereas REERS remains stable regardless of the IoT device size.

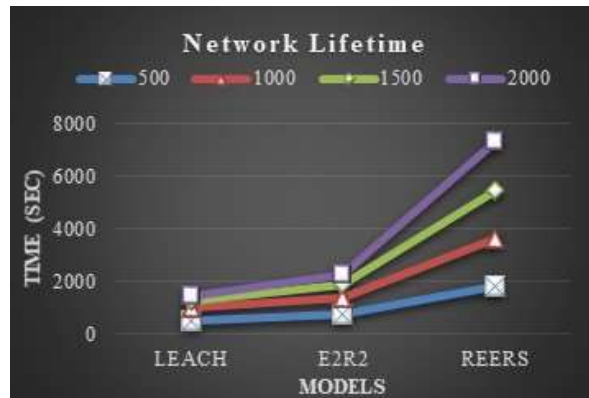


Figure 2. Network lifetime performance

4.2. Processing time

In this section, the processing time for executing varied tasks of Montage and Cybershake has been given. The SFE-WRM model demonstrates significant improvements in processing time for executing varied tasks of Montage and Cybershake when compared with the MOWOS. In Figure 3, the processing time for executing varied tasks of Montage have been given. Similarly in Figure 4, the processing time for executing varied tasks of Cybershake have been given. The results show that the SFE-WRM has improved the average processing time for executing the Montage and Cybershake workload by 79.41% and 76.71% when compared with the MOWOS model.



Figure 3. Processing time for executing varied tasks of Montage

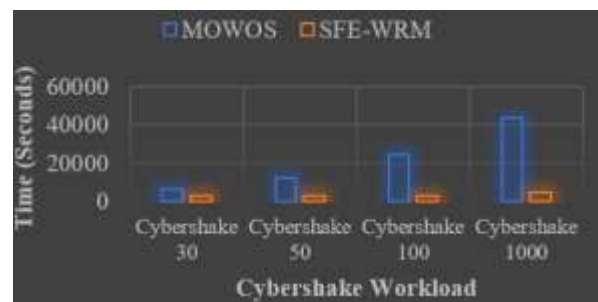


Figure 4. Processing time for executing varied tasks of Cybershake

4.3. Energy consumption

In this section, the energy consumption consumed for executing varied tasks of Montage and Cybershake has been given. The SFE-WRM model demonstrates significant improvements in energy consumed for executing varied tasks of Montage and Cybershake when compared with the MOWOS. In Figure 5, the energy consumption consumed for executing varied tasks of Montage have been given. Similarly in Figure 6, the energy consumption consumed for executing varied tasks of Cybershake have been given. The results show that the SFE-WRM has improved the average energy consumed for executing the Montage and Cybershake workload by 87.48% and 83.77% when compared with the MOWOS model.



Figure 5. Energy consumed for executing varied tasks of Montage

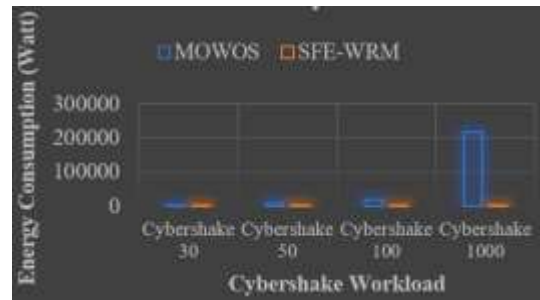


Figure 6. Energy consumed for executing varied tasks of Cybershake

4.4. Detection accuracy

In this section, the detection accuracy attained while executing varied tasks of Montage and Cybershake has been given. The SFE-WRM model demonstrates significant improvements in detection accuracy for executing varied tasks of Montage and Cybershake when compared with the MOWOS. In Figure 7, the detection accuracy attained for executing varied tasks of montage have been given. Similarly, in Figure 8, the detection accuracy attained for executing varied tasks of Cybershake have been given. The results show that the SFE-WRM has improved the average detection accuracy for executing the Montage and Cybershake workload by 7.64% and 9.49% when compared with the MOWOS model.



Figure 7. Detection accuracy for varied tasks of Montage

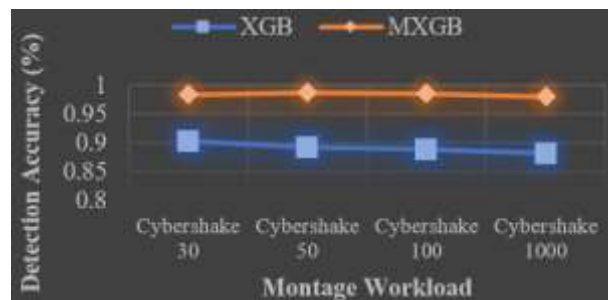


Figure 8. Detection accuracy for varied tasks of Cybershake

4.5. Misclassification rate

In this section, the misclassification rate attained while executing varied tasks of Montage and Cybershake has been given. The SFE-WRM model demonstrates significant improvements in misclassification rate attained while executing varied tasks of Montage and Cybershake when compared with the MOWOS. In Figure 9, the misclassification rate attained while executing varied tasks of montage have been given. Similarly, in Figure 10, the misclassification rate attained while executing varied tasks of Cybershake have been given. The results show that the SFE-WRM has improved the average misclassification rate for executing the Montage and Cybershake workload by 4.37% and 6.22% when compared with the MOWOS model.



Figure 9. Misclassification rate for varied tasks of Cybershake

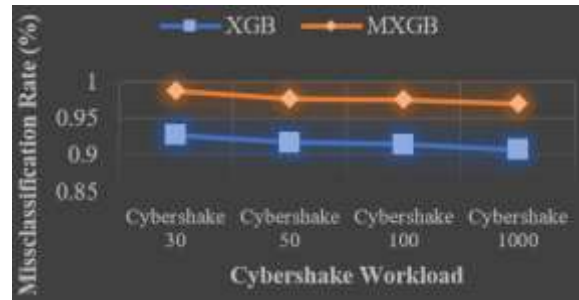


Figure 10. Misclassification rate for varied tasks of Cybershake

5. CONCLUSION

The proposed work aims to address the challenges related to secure resource provisioning, access-control, and workload resource-management in the IoT environment. This work introduced the proposed model, which incorporates a dynamic access-control mechanism that uses reputation-based models, a machine learning-based approach for detecting malicious packets at gateway servers, and a SFE-WRM. The work is tested considering different kinds of nodes size varying between 50 nodes to 1,000 nodes. Considering all the cases the proposed reputation security model is scalable. The proposed is capable of working for larger size due to adoption of centralized reputation computation scheme. The SFE-WRM was compared with the existing REERS and FTA-WRM methods and the results showed that the proposed method outperforms the existing methods in terms of resource utilization and energy consumption. In conclusion, the proposed model provides a comprehensive solution to address the security and management challenges in the IoT environment. Only approved devices and users are granted access to the IoT's resources using the dynamic access-control mechanism. The machine learning-based approach for detecting malicious packets at gateway servers helps to identify and mitigate security threats in real-time. Finally, the SFE-WRM enables efficient workload resource management by dynamically allocating resources based on workload demands. Overall, the proposed model provides a robust and scalable solution for managing the IoT environment while ensuring security, efficiency, and optimal resource utilization. The overall system is implemented through simulation on complex workflow application. However, for future work, the proposed reputation can work under more diverse attack must be studied, also, can the proposed work can explore the integration of blockchain-based approaches to enhance security and trust in the IoT environment.





REFERENCES

- [1] M. B. Paul and U. Sharma, "Security in cloud computing for sensitive data: challenges and propositions," in *International Conference on Innovative Computing and Communications*, 2021, pp. 905–918, doi: 10.1007/978-981-15-5113-0_76.
- [2] J. C. John, A. Gupta, and S. Sural, "Data leakage free ABAC policy construction in multi-cloud collaboration," in *2022 IEEE 15th International Conference on Cloud Computing (CLOUD)*, Jul. 2022, pp. 315–320, doi: 10.1109/CLOUD55607.2022.00054.
- [3] M. S. Rahaman, S. N. Tisha, E. Song, and T. Cerny, "Access control design practice and solutions in cloud-native architecture: a systematic mapping study," *Sensors*, vol. 23, no. 7, p. 3413, Mar. 2023, doi: 10.3390/s23073413.
- [4] N. Alharbe, A. Aljohani, M. A. Rakrouki, and M. Khayyat, "An access control model based on system security risk for dynamic sensitive data storage in the cloud," *Applied Sciences*, vol. 13, no. 5, p. 3187, Mar. 2023, doi: 10.3390/app13053187.
- [5] Z. Wang and X. Chen, "Intrusion detection-data security protection scheme based on particle swarm-BP network algorithm in cloud computing environment," *Journal of Electrical and Computer Engineering*, vol. 2023, p. e1128545, Mar. 2023, doi: 10.1155/2023/1128545.
- [6] G. Zhao, Y. Wang, and J. Wang, "Lightweight intrusion detection model of the internet of things with hybrid cloud-fog computing," *Security and Communication Networks*, vol. 2023, p. e7107663, Jan. 2023, doi: 10.1155/2023/7107663.
- [7] J. Almutairi and M. Aldossary, "A novel approach for IoT tasks offloading in edge-cloud environments," *Journal of Cloud Computing*, vol. 10, no. 1, p. 28, Apr. 2021, doi: 10.1186/s13677-021-00243-9.
- [8] X. Liu, L. Huan, R. Sun, and J. Wang, "Lightweight fine-grained multiowner search over encrypted data in cloud-edge computing," *Security and Communication Networks*, vol. 2023, pp. 1–15, Jan. 2023, doi: 10.1155/2023/1701874.
- [9] W. Ahmad, A. Rasool, A. R. Javed, T. Baker, and Z. Jalil, "Cyber security in IoT-based cloud computing: a comprehensive survey," *Electronics*, vol. 11, no. 1, p. 16, Dec. 2021, doi: 10.3390/electronics11010016.
- [10] L. Zhang, B. Li, H. Fang, G. Zhang, and C. Liu, "An internet of things access control scheme based on permissioned blockchain and edge computing," *Applied Sciences*, vol. 13, no. 7, p. 4167, Mar. 2023, doi: 10.3390/app13074167.
- [11] G. Nebbione and M. C. Calzarossa, "Security of IoT application layer protocols: challenges and findings," *Future Internet*, vol. 12, no. 3, p. 55, Mar. 2020, doi: 10.3390/fi12030055.
- [12] P. K. Sadhu, V. P. Yanambaka, and A. Abdelgawad, "Internet of things: security and solutions survey," *Sensors*, vol. 22, no. 19, p. 7433, Sep. 2022, doi: 10.3390/s22197433.





- [13] R. K. Lenka, M. Kolhar, H. Mohapatra, F. Al-Turjman, and C. Altrjman, "Cluster-based routing protocol with static hub (CRPSH) for WSN-assisted IoT networks," *Sustainability*, vol. 14, no. 12, p. 7304, Jun. 2022, doi: 10.3390/su14127304.
- [14] M. Ilyas *et al.*, "Trust-based energy-efficient routing protocol for Internet of things-based sensor networks," *International Journal of Distributed Sensor Networks*, vol. 16, no. 10, p. 155014772096435, Oct. 2020, doi: 10.1177/1550147720964358.
- [15] P. Joshi and A. S. Raghuvanshi, "A multi-objective metaheuristic approach based adaptive clustering and path selection in iot enabled wireless sensor networks," *International Journal of Computer Networks and Applications*, vol. 8, no. 5, p. 566, Oct. 2021, doi: 10.22247/ijcna/2021/209988.
- [16] J. S. Kumar and M. A. Zaveri, "Resource scheduling for postdisaster management in IoT environment," *Wireless Communications and Mobile Computing*, vol. 2019, pp. 1–19, Mar. 2019, doi: 10.1155/2019/7802843.
- [17] B. R. Parida, A. K. Rath, and H. Mohapatra, "Binary self-adaptive salp swarm optimization-based dynamic load balancing in cloud computing," *International Journal of Information Technology and Web Engineering*, vol. 17, no. 1, pp. 1–25, May 2022, doi: 10.4018/IJITWE.295964.
- [18] H. Mohapatra, "Socio-technical challenges in the implementation of smart city," in *2021 International Conference on Innovation and Intelligence for Informatics, Computing, and Technologies (3ICT)*, Sep. 2021, pp. 57–62, doi: 10.1109/3ICT53449.2021.9581905.
- [19] S. Rahul and V. Bhardwaj, "Optimization of resource scheduling and allocation algorithms," in *2022 Second International Conference on Interdisciplinary Cyber Physical Systems (ICPS)*, May 2022, pp. 141–145, doi: 10.1109/ICPS55917.2022.00034.
- [20] J. Yu, "Qualitative simulation algorithm for resource scheduling in enterprise management cloud mode," *Complexity*, vol. 2021, pp. 1–12, Feb. 2021, doi: 10.1155/2021/6676908.
- [21] Y. Hu, H. Wang, and W. Ma, "Intelligent cloud workflow management and scheduling method for big data applications," *Journal of Cloud Computing*, vol. 9, no. 1, p. 39, Dec. 2020, doi: 10.1186/s13677-020-00177-8.
- [22] A. Lakhan *et al.*, "Restricted boltzmann machine assisted secure serverless edge system for internet of medical things," *IEEE Journal of Biomedical and Health Informatics*, vol. 27, no. 2, pp. 673–683, Feb. 2023, doi: 10.1109/JBHI.2022.3178660.
- [23] D. S. Nayagi, S. G. G. V. Ravi, V. K. R., and S. Sennan, "REERS: Reliable and energy-efficient route selection algorithm for heterogeneous Internet of things applications," *International Journal of Communication Systems*, vol. 34, no. 13, Sep. 2021, doi: 10.1002/dac.4900.
- [24] D. S. Nayagi, G. G. Sivasankari, V. Ravi, K. R. Venugopal, and S. Sankar, "Fault tolerance aware workload resource management technique for real-time workload in heterogeneous computing environment," *Transactions on Emerging Telecommunications Technologies*, vol. 34, no. 3, Mar. 2023, doi: 10.1002/ett.4703.
- [25] V. Desai and D. Hagare Annappaiah, "Reputation-based security model for detecting biased attacks in BigData," *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 29, no. 3, p. 1567, Mar. 2023, doi: 10.11591/ijeecs.v29.i3.pp1567-1576.
- [26] K. Chandrashekar and A. T. Narayanreddy, "An ensemble feature optimization for an effective heart disease prediction model," *International Journal of Intelligent Engineering and Systems*, vol. 16, no. 2, pp. 517–525, Feb. 2023, doi: 10.22266/ijies2023.0430.42.
- [27] A. Shahapurkar and S. F. Rodd, "Efficient feature aware machine learning model for detecting fraudulent transaction in streaming environment," *International Journal on Information Technologies and Security*, vol. 14, no. 3, pp. 3–14, 2022.
- [28] J. K. Konjaang and L. Xu, "Multi-objective workflow optimization strategy (MOWOS) for cloud computing," *Journal of Cloud Computing*, vol. 10, no. 1, 2021, doi: 10.1186/s13677-020-00219-1.
- [29] "Workflow gallery," *pegasus.isi.edu*. https://pegasus.isi.edu/workflow_gallery/ (accessed Oct. 31, 2023).
- [30] "NSL-KDD dataset," *Canadian Institute for Cybersecurity*. <https://www.unb.ca/cic/datasets/nsl.html> (accessed Oct. 31, 2023).

BIOGRAPHIES OF AUTHORS



Dharuman Salangai Nayagi     is a Senior Assistant Professor in the Department of Computer Science and Engineering at New Horizon College of Engineering, Bangalore, India. She received her B.Tech. degree in Information Technology from Anna University, Chennai, India. M. Tech degree in Information Technology from Dr. MGR University, Chennai, India. She is currently pursuing Ph.D. degree in the area of Internet of Things from Visveswaraya Technological University, Karnataka, India. She has published 2 SCI, 1 international and 4 national conferences /journal papers. Her research interest is in the area of internet of things, information security and big data analytics, machine learning. She can be contacted at email: nayagisalangai@gmail.com.



Hosaagrahara Savalegowda Mohan     is currently working as a Professor and Head in the Department of CSE-Data Science at RNS Institute of Technology Bangalore. He is having total 24 years of teaching experience. He received his Bachelor's degree in Computer Science and Engineering from Malnad College of Engineering, Hassan and M.Tech. in Computer Science and Engineering from Jawaharlal Nehru National College of Engineering, Shimoga and Ph.D. in Computer Science and Engineering from Dr. MGR University, Chennai during the year 2012. His area of interests are cryptography and networks security, image processing, cloud computing, data structures, computer graphics, finite automata and formal languages, compiler design. He has Awarded Dr. Abdul Kalam Life Time Achievement for his excellence teaching and research during the year 2017. He can be contacted at email: mohan_kit@yahoo.com.