Energy Efficient Weighted Probability Model Integrated Cloud-IoT Network to Increase Lifetime of the Network with Layered Architecture

Adel Abdullah Basuliman*[1] , D.Kinslin[2] , Mr. Aishwary Awasthi[3] , Dr. R.Dinesh Kumar[4] , Dr.Juhi Juwairiyyah[5] , Mr. Rajesh Pandey[6]

Abstract: IoT-based wireless communication technology is an emerging technology involved in the provision of advanced communication for ubiquitous services. The drastic development of sensor devices leads to the effective realization of IoT technology based on the sensor environment. The IoT uses the cloud platform to process and manage a vast range of data. The integration of the cloud in the IoT platform leads to the acquisition of data, parallel processing, and dynamic resources. The implementation of the cloud in the IoT platform is subjected to a vast range of energy utilization. Hence, it is necessary to develop an appropriate scheme for secure communication in the IoT cloud environment. This paper proposed an LSTM-based cloud server IoT model for energy reduction in the IoT environment with the weighted probability estimation features. The proposed model is termed as the LSTMwpm for the estimation of the features in the IoT environment. Based on the computation of the energy level of the nodes the data transmission path is computed. Upon the estimated data transmission path the messages are transferred with the CH layer and base layer. The simulation analysis expressed that the proposed LSTMwpm model exhibits a higher alive node count of 1000 and a reduced dead node count. The estimated a number of a message transmitted in the layer expressed that base layer exhibits the value of 1000 messages in the network.

Keywords: *Internet of Things (IoT), Weighted Probability, Base layer, CH layer, Cloud Server, LSTM*

1. Introduction

Cloud computing technology comprises connected cloud servers to provide Information technology (IT) services by means of network devices, and servers [1]. The cloud computing platform uses the data center for the computation circumstance for the Quality of Service (QoS). The energy cost is higher for the cloud server for the cloud system with the higher performance with the Service Level Agreements (SLA) between the server and cloud for effective energy utilization [2]. The framework comprises accurate innovation with the implementation of the IoT system. The environment server demand storage, control, security, and time for the prerequisite clients. With the IoT with cloud environment to the development of various smart devices, actuators, and sensors that are capable of sensing ubiquitous data in real time [4]. Moreover, these small-sized, battery-powered, and internet-enabled devices have the ability to transmit data from remote locations in a matter of milliseconds with high efficacy [5]. Even though hardware and software specifications of these IoT devices vary from one another, but the overall objective of data acquisition, and transmission is analogous.

IoT has been a keen area of research over the past few years due to its high effectivity in provisioning time-sensitive results[6]. Moreover, the abrupt adoption of IoT in industrial organizations has made a global buzz about this innovative technology. As predicted by Cisco, number of IoT devices are expected to cross 50 billion by the year 2020 [7]. In fact, according to a survey report, more than 86% of industrial sectors around the world have been equipped with IoT technology, out of which 84% have depicted significant enhancements in delivering user-specific services [8]. As a result, over the past few years IoT technology has been considered as a pivotal area of modern era's research. Even though numerous definitions have been presented by researchers around the world.

The revolutionizing technology of cloud computing is around from sometimes. The world has transformed towards developing software for millions of users to consume-as-aservice rather than to purchase and execute on individual computers [9]. Extending from providing real-time computing power to online storage facility, cloud computing has been a pivotal division of research for researchers, and innovators. Moreover, with a well-established networking infrastructure representing cloud, both business organizations and individual users are able to access resources, platforms, and applications from anywhere in seamless manner. This paper proposed a LSTM based weighted probability model for the estimation of the energy level in the path of the network. The developed LSTMwpm estimates the distance

[1] *Research ScholarDepartment of Management Studies, NICHENoorul Islam Centre for Higher EducationThucklay, basuliman.a@gmail.com*
[2]*Professor, Department of Management Studies, NICHE Noorul Islam Centre for Higher EducationThucklay, dkinslin@gmail.com*
[3]*Research Scholar, Department of Mechanical Sanskriti University, Mathura, Uttar Pradesh, India, aishwary@sanskriti.edu.in*
[4]*Dept. of Electronics and communication Engineering, PERI Institute of technology, Chennai.*
[5]*Assistant Professor Computer Science Engineering Malla Reddy UniversityHyderabad drjuhi@mallareddyuniversity.ac.in*
[6]*Asst. Professor, Department of Computer Science Shobhit Institute of Engineering & Technology (Deemed to-be University) rajesh@shobhituniversity.ac.in*

between the nodes and perform the data transmission with the reduced energy consumption with the increased lifetime of the network. The defined model uses the CH layer and base layer for the security.

2. Related Works

In [10] developed Parkinson's disease classification using data based on IoT obtained from machine learning methods. There were three different classifiers used in the detection - DT, random forest, and NB. They were chosen by looking at their reliability and ability to enhance classification. The data was collected using an IoT node. It provided faster classification, which aided the decision-making process. Here, the data from the two different datasets, such as LSVT and CNAE-9, were preprocessed, and features from the preprocessed data were obtained using principal component analysis. Subsequently, eigenvalues were used for accomplishing feature reduction. The reduced features were given to classifiers. The patients with Parkinson's disease were monitored by transmitting the recorded voice of the patient to the IoT network using digital home virtual assistants. Moreover, the classifiers used in the IoT system also grouped the remaining types of traffic data present in the respective IoT node. Here, DT and random forest classifiers took more time in training the data.

In [11] presented a network ID model by means of single Convolutional Neural Networks (CNNs) and multi-CNN fusion models. The NSL-KDD dataset is considered as extensively used in network intrusion identification tests. This dataset was created in 2009. Subsequently, numeralization was used to transform features into 121-dimensional numerical features. Here, pre-processing of label data has delivered the value zero when the respective record belongs to the normal traffic; otherwise, it offers one during the binary classification. The one-hot encoding used pre-processed data during multiclass classification. The processed features so obtained were trainable and gave huge numerical differences in the records. This difference created an impact on the model's training effect and convergence speed. Hence, the dataset needed to be normalized in the range of [0, 1]. Additionally, data clustering was developed to minimize the effect of imposing correlation. The feature was separated into four portions based on the correlation among features. They are as follows: • Host • Content • Straightforward • Time This data clustering was used to understand higher-level relations among global features, which were avoided by other classification methods. After dividing the feature data into four parts, one-dimensional feature data was transformed into a grayscale graph. Here, CNN is used in the intrusion detection issue by utilizing the flow data visualization method. The performance analysis shows that the multi-CNN fusion model conveniently provided classification with less complexity and higher accuracy in the NSL-KDD dataset. However, this CNN-based intrusion detection didn't provide data protection over industrial-related IoT applications.

In [12] presented IPV6 based Routing Protocol for Low Power and Lossy Networks (RPL) to accomplish, a reliable data transmission over the resource-constrained Industrial Internet of Things (IIoT). The secure framework was based on genetic programming used to identify the existence of security threats in RPL 40 based IoT and IIoT networks. This security framework has the capacity for detecting various attacks. Here, the RPL Novel and Secure Framework (NSF) for IIoT is comprised of two essential functions. In this, DODAG was considered as a key element that confirmed loop-free communication in IIoT networks. In Directed Acyclic Graph (DAG), the nodes were linked in a tree-type structure. A high number of DAG that point towards the central node were created in the DODAG. In the attack detection, features that have huge probabilities were taken into consideration. For each attack, the in-order traversal of nodes was used to form the statement of the threshold. Initially, the possible features for all the nodes were extracted. Selected optimal features are chosen based on genetic programming. Here, the tournament selection method was used in the form of feature selection. In attack detection, the features which have higher possibilities played an important role. Child nodes in the IoT environment sent control packets towards upward nodes while generating the initial topology. After generating the communicational gateway among the participating nodes, data transmission was initialized in the RPL network. The features obtained from the child nodes were used to identify the attacks in the 2nd phase of RPL-NSF-IIoT. This RPL-NSF-IIoT easily detected the attacks in similar scenarios. But the detection of the attacks was difficult when RPL-NSF-IIoT was processed in different scenarios

In [13] presented an optimal feature extraction method to overcome the issues related to feature selection for cyber-attacks. This work used the BotIoT dataset for analyzing cyber-attack detection performances using ML methods. Initially, an optimal feature extraction method (i.e., CorrAUC) was used to handle feature selection of cyber-attack detection issues in the IoT network. Subsequently, Corrauc was designed, based on the CorrAUC, to detect Bot-IoT traffic since this Corrauc was a wrapper technique used for precise filtering of the features. The metric of the area under the 'roc' curve and correlation attributes evaluation were used to choose the features which provided adequate information for the ML method. These selected features were used for Bot-IoT cyber-attack identification. Furthermore, Shannon Entropy and TOPSIS were combined using the bijective soft set method for validating chosen features to detect malicious traffic in the network. The detection of the malicious traffic mainly depended on the selection of suitable attributes mean features set. The developed ML method precisely identified all the attacks but provided poor performance while detecting the KeylogingTheft attacks.

3. Weighted Probability model for energy reduction in cloud IoT

The emerging advancement with the IoT advancement leads to the processing of the vast range of the data through the cloud server. The data from the cloud server are processed with the cloud platform. This paper presented a LSTMwpm model for the medical healthcare data processing in the IoT environment using cloud. The weighted model uses the node energy level for the computation of the weights in the network to select cluster Head. The proposed LSTMwpm uses the SEP election model for the heterogeneity of the features at the two levels. The SEP protocol

model uses the two levels defined as the $level1$ and $level2$. Based on the assigned level in the IoT environment ,the energy levels are computed where the $level1$ has minimal energy than the other level $level2$. The probability estimation of the features in the levels are defined as the S^{level1} and S^{level2} with the optimization of the variables those are presented in equation (1) and (2)

$$S^{level1} = \frac{s^{opt}}{1+a\times m} \quad (1)$$

$$S^{level2} = \frac{s^{opt}\times(1+a\times m)}{1+a\times m} \quad (2)$$

The estimated threshold for the developed probability model for the estimation is presented in the equation (3) and (4)

$$T_s^{level1} = \begin{cases} \frac{S^{level1}}{1-S^{level1}\times\left(r\ mod\frac{1}{S^{level1}}\right)} & if\ s \in G^{level1} \\ 0 & otherwise \end{cases} \quad (3)$$

$$T_s^{level2} = \begin{cases} \frac{S^{level2}}{1-S^{level2}\times\left(r\ mod\frac{1}{S^{level2}}\right)} & if\ s \in G^{level2} \\ 0 & otherwise \end{cases} \quad (4)$$

Based on the consideration of the features for the energy T_s^{level1} and T_s^{level2} nodes with the transmission count of r with the computation of the transmission round. The cluster head optimal number is defined as S with the non-selected nodes are defined as $G^{level1}\ and\ G^{level2}$ respectively. The bridge layer comprises of the parameters key based on energy and distance efficiency represented as E_{ef} and D_{ef} defined as in equation (5) and equation (6)

$$E_{ef} = \frac{E_r}{E_{rav}} \quad (5)$$

$$D_{ef} = \frac{D_{sin}+D_{ch}}{2} \quad (6)$$

In the above equation (5) and (6) the node residual energy is computed as E_{rav} and the node distance function is measured as D_{sin} and D_{ch} for the sink node those are represented in equation (7) and equation (8)

$$D_{sin} = \frac{D_{sn}}{D_{sn_{av}}} \quad (7)$$

$$D_{ch} = \frac{D_{ch_{mean}}}{D_{ch_{mean_{av}}}} \quad (8)$$

The proposed LSTMwpm comprises of the node distance denoted as D_{sn} and the node average distance is presented as $D_{sn_{av}}$ for the sink nodes. The present cluster node distance is defined as $D_{ch_{mean}}$ for the average calculated value as $D_{ch_{mean_{av}}}$. With the selected CHs the algorithm computes the each node according with the equation (9)

$$Ch_{score} = E_{ef}\times\omega_1 + D_{ef}\times\omega_2 \quad (9)$$

In the above equation (9) the score weights are estimated with predefined value as ω_1 and ω_2. The selected node CH are sorted based on the score values based on the BN layer with the positive integer value of k% nodes. The developed model comprises o the setup phase for the every transmission those are directed for the selection of Cluster Head.

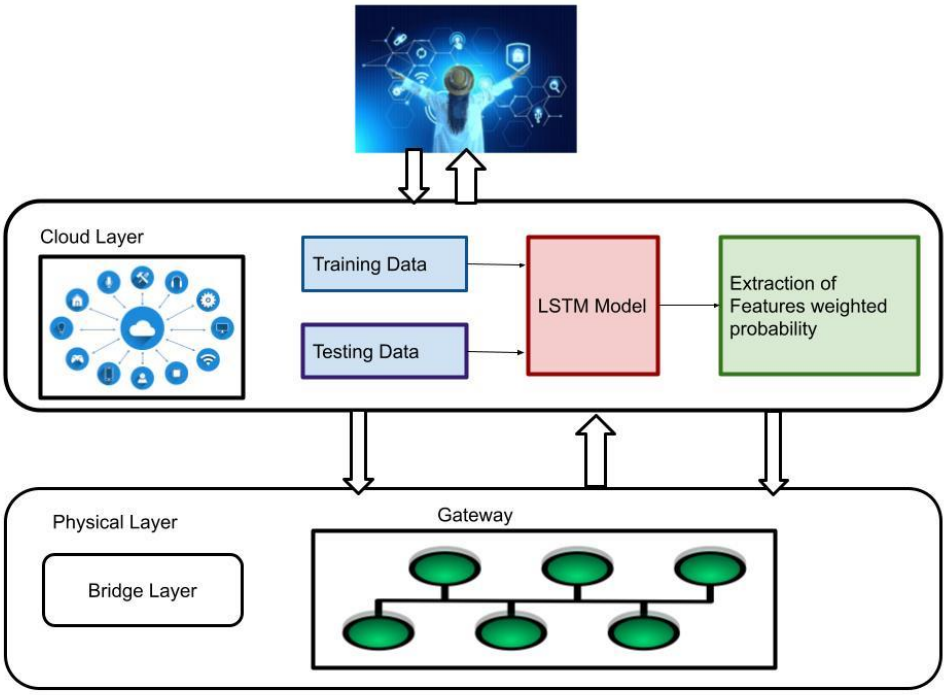

Figure 1: Architecture of the LSTMwpm

The figure 1 provides the architecture mode for the proposed LSTMwpm to estimates the data collected from the different sensor data. The processed information is evaluated with the LSTM network model for the weighted probability estimation feature models.

4. Experimental Analysis

The performance of the proposed LSTMwpm performance is evaluated based on the consideration of the lifetime of network. The evaluation of the proposed LSTMwpm model is examined with consideration of the three measures such as FND, HND and LND. The parameters considered for the analysis is presented as

follows:

First Node Dies (FND) – It determines the network period consistency

Half Node Dies (HND) - Determines the lifetime of network when 50% nodes are dead

Last Node Dies (LND) – Measures the lifetime of the complete network

The performance of the proposed LSTMwpm is evaluated based on the stability period of the network with the overall network lifetime of 112% gain which can be extended by 32%. In table 1 the computed lifetime of the network for the varying layers in the network are presented.

Table 1: Performance of Network Lifetime

Lifetime of Network	Layer CH	Bridge layer	Gain
FND	325	654	112
HND	1286	1278	03
LND	4268	5257	32

The performance of the proposed LSTMwdm is computed based on the consideration of the hyper parameters. The defined hyper paramters for the proposed model is presented in table 2.

Table 2: Hyper Parameter for analysis

Parameters	**Values**
Features	496
Hidden Units	246
Classes	8
Epochs	170
Threshold	2

The figure 2 – 4 performance of the proposed LSTMwpm for the alive nodes and number of nodes, dead nodes are presented. The simulation analysis stated that bridge layer exhibits the minimal performance for the cluster layer compared with the bridge layer. Moreover, with the bridge layer estimates the load balancing in the network for the CHs to minimize the energy consumption in the network based in the transmission distance.

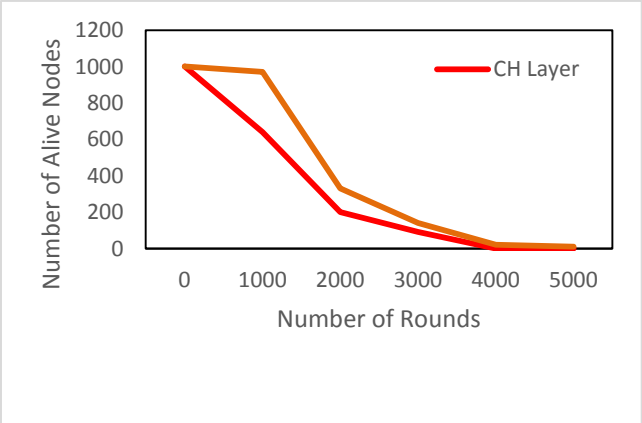

Figure 2: Number of Alive Nodes

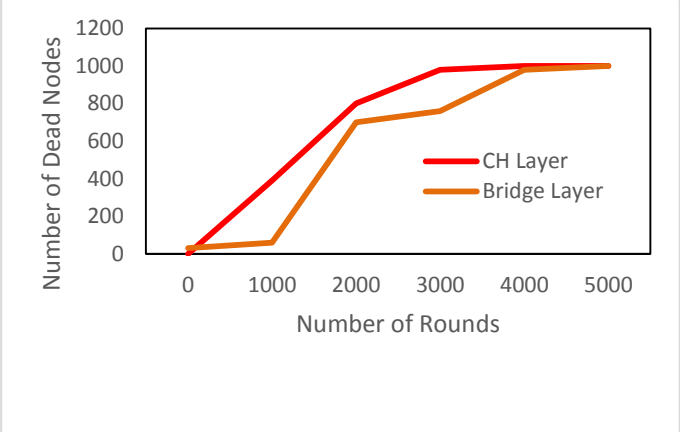

Figure 3: Comparison of Dead Nodes

The maximal number of alive nodes in the proposed LSTMwpm is maximal count of 1000 for the both CH and bridge layer in the network. The computed dead node sin the value is minimal for the rounds 1000. This implies that proposed LSTMwpm achieves the increased network lifetime compared with the other techniques. In figure 4 the energy consumption for the varying number of the rounds is presented.

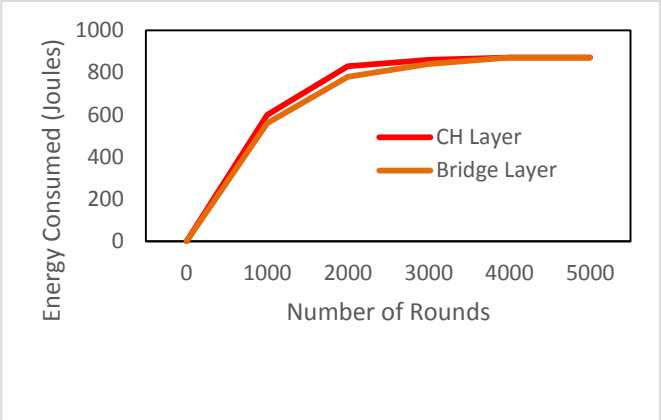

Figure 4: Estimation of Energy Consumed

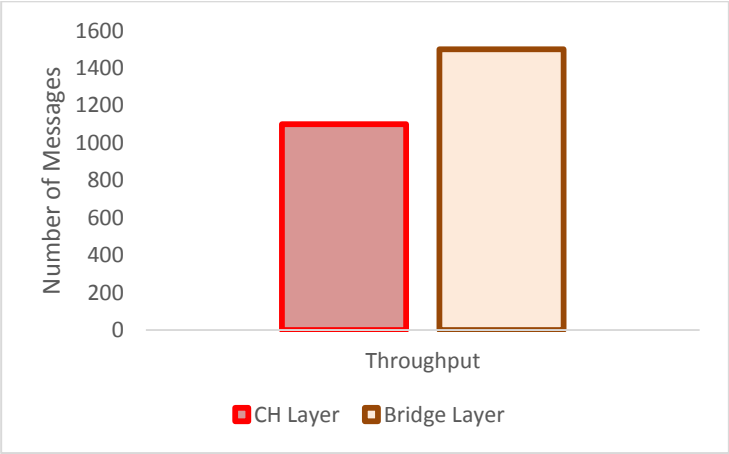

Figure 5: Comparison of the Messages

In the figure 4 the energy consumption is measured as 1000 joules for the both CH and bridge layer. The varying number of rounds the smooth curve is estimated for the varying rounds. The figure 5 provides the number of message transmitted over the network is presented for the CH and bridge layer. The number of

messages from the bridge layer is maximal than the CH layer.

5. Conclusion

In the IoT based cloud environment energy consumption is considered as the tremendous challenge. The incorporation of the physical layer increases the sensor node transmission for the long distance cloud environment which impacts positively on the higher energy sources. The energy consumption in the network are reduced with the implementation of the LSTMwpm with the incorporation of the intermediate layer between the cluster and sink layer. The proposed LSTMwpm aggregates the different cluster in the sink layer for the shortest distance between cluster and sink layer with the reduced energy utilization. The proposed LSTMwpm is comparatively examined for the CH layer and bridge layer in the network. The simulation analysis expressed that proposed model exhibist the higher number of alive nodes and reduced dead and energy consumption. The proposed LSTMwpm uses the 800Joules of energy consumption for the both CH and bridge layer. Also, the number of messages transferred is significantly reaches the maximal value of 100 for the both CH and bridge layers in the network.

References

[1] Alam, T. (2021). Cloud-based IoT applications and their roles in smart cities. *Smart Cities*, *4*(3), 1196-1219.

[2] Alshehri, M., Bhardwaj, A., Kumar, M., Mishra, S., & Gyani, J. (2021). Cloud and IoT based smart architecture for desalination water treatment. *Environmental research*, *195*, 110812.

[3] Chaudhry, S. A., Irshad, A., Yahya, K., Kumar, N., Alazab, M., & Zikria, Y. B. (2021). Rotating behind privacy: an improved lightweight authentication scheme for cloud-based IoT environment. *ACM Transactions on Internet Technology (TOIT)*, *21*(3), 1-19.

[4] Alsharif, M., & Rawat, D. B. (2021). Study of machine learning for cloud assisted iot security as a service. *Sensors*, *21*(4), 1034.

[5] Sadeeq, M. M., Abdulkareem, N. M., Zeebaree, S. R., Ahmed, D. M., Sami, A. S., & Zebari, R. R. (2021). IoT and Cloud computing issues, challenges and opportunities: A review. *Qubahan Academic Journal*, *1*(2), 1-7

[6] Lakshmi, G. J., Ghonge, M., & Obaid, A. J. (2021). Cloud based iot smart healthcare system for remote patient monitoring. *EAI Endorsed Transactions on Pervasive Health and Technology*, *7*(28), e4-e4.

[7] Shah, J. L., Bhat, H. F., & Khan, A. I. (2021). Integration of Cloud and IoT for smart e-healthcare. In *Healthcare Paradigms in the Internet of Things Ecosystem* (pp. 101-136). Academic Press.

[8] Zhang, Y., Li, B., Liu, B., Hu, Y., & Zheng, H. (2021). A privacy-aware PUFs-based multiserver authentication protocol in cloud-edge IoT systems using blockchain. *IEEE Internet of Things Journal*, *8*(18), 13958-13974.

[9] Juyal, S., Sharma, S., & Shukla, A. S. (2021). Smart skin health monitoring using AI-enabled cloud-based IoT. *Materials Today: Proceedings*, *46*, 10539-10545.

[10] Malarvizhi Kumar, P., Hong, C. S., Chandra Babu, G., Selvaraj, J., & Gandhi, U. D. (2021). Cloud-and IoT-based deep learning technique-incorporated secured health monitoring system for dead diseases. *Soft Computing*, *25*(18), 12159-12174.

[11] Deepika, J., Rajan, C., & Senthil, T. (2021). Security and privacy of cloud-and IoT-based medical image diagnosis using fuzzy convolutional neural network. *Computational Intelligence and Neuroscience*, *2021*.

[12] Deepika, J., Rajan, C., & Senthil, T. (2021). Security and privacy of cloud-and IoT-based medical image diagnosis using fuzzy convolutional neural network. *Computational Intelligence and Neuroscience*, *2021*.

[13] Ge, X., Yu, J., Chen, F., Kong, F., & Wang, H. (2021). Toward verifiable phrase search over encrypted cloud-based IoT data. *IEEE Internet of Things Journal*, *8*(16), 12902-12918.