International Journal of Computer and Engineering Optimization (IJCEO)
Volume 1, Issue 1, September – October (2023)

RESEARCH ARTICLE

INTRUSION DETECTION ARCHITECTURE (IDA) IN IOT BASED SECURITY SYSTEM

M. Amanullakhan[1, *], M. Usha[2] and S. Ramesh[3]

[1] Department of Electronics and Communication Engineering, Mohamed Sathak Engineering College, Kilakarai, India.
[2] Department of Masters in Computer Application, MEASI Institute of Information Technology, Tamilnadu, India.
[3] Department of Computer Science Engineering, Krishnasamy College of Engineering Technology, Anand Nagar, Kumarapuram, Cuddalore, India

[*]*Corresponding e-mail: amanulla82@gmail.com*

Abstract – Through the use of billions of data points, the internet of things (IOT) links billions of objects to the internet, all of which require security. A major issue for cyber security is the expanded attack surface of IOT. To overcome these challenges, Intrusion Detection Architecture (IDA) has been proposed in this paper, which helps to trace the Intrusion Data in IOT. The proposed Intrusion Detection Architecture (IDA) is performed in three stages namely, Data Collection, Pre-processing in Data encoding and Classification block. Initially, the request from the IOT devices is sent to the Data collection (DC) and pre-processing stage there it could find the amount of data. The collected data traces and filter through the Normalization Technique (NT). Then the filtered data goes to the data encoding block. After the encoded data goes to classification block here it classifies the data by Ghost Net technique and finally the attack can be classified and detected. The effectiveness of the suggested IDA strategy has been assessed using assessment measures such as configuration latency, detection rate, accuracy, precision, recall rate, false detection rate. The proposed method reduces the communication overhead of 75%, 50% and 38% than SSTS, ANT and FPDS existing techniques.

Keywords *– IoT, Intrusion detection, Cyber security, Data encoding, Ghost Net technique.*

1. INTRODUCTION

An increasing number of sectors are utilising the Internet of Things [1]. Everybody's life is changing as a result of the Internet of Things (IoT), that provides services like monitoring and managing linked smart gadgets. Smart cities [2], homes [3], cars [4], industrial [5], digital health care smart control system [6], commuting [6], wearables [7], farming [8], and many more areas are among the numerous uses for the Internet of Things. The Internet of Things (IoT) is a growingly well-liked technology that allows actual objects, such as cars and home appliances, to interact and even communicate with one another [9]. Autonomous and semi-autonomous smart automobiles make up the Internet of Vehicles (IOV), which may be defined as an Internet of Things (IoT) system having incorporated sensing as well as management capabilities for computerized navigation and enhanced safety [10].

In recent years, IoT technologies and platforms have expanded rapidly. IoT is a relatively new technology, yet it does not always imply that it is simpler than the current system. Otherwise, interactions between the real world and the internet actually make IoT platforms and systems more complex [11]. The Internet of Things (IoT) most crucial characteristic is how widely it is used and how easily it can be adapted to computer networks [12]. Large amounts of data are generated by IoT device sensors, which call for authentication, security, and privacy [13].

Yet, because to the variety, decentralization and due to the IoT network's complexity, certain IoT problems with relation to cyber physical security are emphasized [14]. Cybersecurity is currently the top priority for the Internet of Things (IoT) as one of its core topics. By utilizing solutions like block chain, intelligent logistics, and smart home management, IoT cyber security reduces cyber security risk for individuals and enterprises [15]. It has been observed that IoT devices are vulnerable to numerous cyber dangers when seen as sensors that can be connected to a computer network.

Cyber-physical systems (CPSs) are integrated technologies that include IoT for smart cities, industry, and healthcare [16]. Securing the topology to which the devices are connected as soon as possible against potential cyberattacks is one of the most crucial factors to take into consideration in the IoT [17]. IoT application on the critical infrastructure has called for an explosion of cyber security challenges on the grid [18]. To overcome these challenges, Intrusion Detection Architecture (IDA) has been proposed in this paper, which helps to trace the Intrusion Data in IOT. The following list summarizes the primary contributions of the suggested IDA approach.

- The proposed Intrusion Detection Architecture (IDA) is performed in three stages namely, Data Collection, Pre-processing, Data encoding and Classification block.
- Initially, the request from the IOT devices is sent to the Data collection (DC) stage there it could

find the amount of data in pre-processing technique.

- The collected data traces and filter through the Normalization Technique (NT) by Data cleaning in Deep Learning (DL). Then the filtered data goes to the data encoding block.
- After the encoded data goes to classification block here it classifies the data by Ghost Net technique and finally the attack can be classified and detected.
- Using assessment criteria including configuration delay, detection rate, accuracy, precision, recall rate, and false detection rate, the effectiveness of the suggested IDA technique has been assessed.

This essay's remaining sections are organized as follows: Part II covers the review of the literature. It serves as a stand-in for the method that Section III suggests. Section IV contains the results and discussions. Section V covers the conclusion and future initiatives.

2. LITERATURE SURVEY

Data privacy in IoT network is concerned, especially for IoT devices which used in moreover sensitive industries, such as healthcare and finance. Many studies have been conducted to solve this problem. Among those, some of the techniques have been reviewed in this section.

In 2020, Yan Zhang, B., et al., [19] aimed a security conscious authentication convention for the multiple server CE Internet of Thing (IoT) system by merging PUFs and the block-chain method. An official oracle model and security and privacy features are used to prove the protocol's security. This protocol's formal proof is based on the random predicted theory and the automated verification tool, which provide semantic security.

In 2020, Waseem Iqbal, H., et al.,[20] put forward the idea to risks, security requirement, troubles to assault vectors relevant in IoT networking system. Through Software Defined Networking (SDN) the IOT architecture deployed attention base networks. The main barriers are unified to the entire IoT participants in single platform, which issues are highlighted by the core. And some findings, emphases to IOT paradigm on a network supported security solution.

In 2021, Kwok-Yan Lam,[21] proposed an ActivityNetwork Things (ANT) with three systems those are device, internet and semantic of architectural perspectives in studying IoT systems, these architectures are based by centric security reference of architecture. The approach helps for security risks manager which was focused the critical activities happened in other micro perimeters with an IoT network system.

In 2021, Shikhar Verma, [22] had suggested the RAW mechanism to evaluate the IoT and inspect the output which was on the basis of on mathematical model. By reducing the risk in the final analysis in for every single device towards an optimal scan rate which was to optimize the tradeoff. The admin cannot control the network parameters by this approach which considers the perspective. Thus, the network was unable to utilize successfully for security enhancement.

In 2021, Wei Zhou, C., et al., [23] had proposed the inspecting Internet of Things security through logical flaws in IOT devices and platforms. It provides information on newly found logic defects specific to IOT systems and platforms. The lessons that can be drawn from these kinds of bugs were covered. The approach in IOT systems and platforms will be focused on newly found logic problems.

In 2021, Jun Zhang, Y., et al., [24] approached a smart transportation security system (STSSs). For the security concern the STSS architecture was proposed. Because there were many smart transportation innovations are facing this problem. For the purposes of examining its feasible and applicability the socio technical was assembled. These assemble approach requires legitimate of socio technical and social interventions.

In 2021, Jiyoon kim [25] had put forward a technique to enable safe mobile terminal transitions between hubs by Mobile Terminal Handover (MTH) security protocol. The issue with the current protocols was resolved by utilizing a brand-new entity known as the Backhaul Management Function (BMF). These protocols can safeguard and protect data between the terminals. the exchangeable messages and then it moves across the hub.

In 2021, Fei Zhu, X., et al., [26] had proposed the integrity and source authentication protecting requirements which was satisfied by the first identification based on RSS and chosen exposure controls healthcare data or information sharing ways in IoT. Which provide possible strategy on the side of a beholder to prevent further reduction or random reduction from corrupt signature have been keep.

In 2021, Shuodi Hui, Z., et al., [27] had offered a method that quantifies a large amount of mobile network traffic data sets that include 46.651 Internet of Things devices in order to prevent IoT privacy breaches. It blends empirical measures with methodical analysis. Additionally, there is a greater degree of privacy leaking to users and platforms are present in IOT devices and also does different daily pattern in privacy leakage to follow their working ways.

In 2022, Hua Deng, Z., et al., [28] had proposed IOT cloud-assisted scheme for the Flexible Privacy preserving Data Sharing (FPDS). By this way, users in IOT could share the data's which was outsourced by the cloud FPDS manner. It protects privacy outsourced data in privacy and with identify-based encryption, and it introduced a fine-grained delegation to the flexible data. And for more importantly, to the owners FPDS provides a flexible data sharing mechanism.

From these literature studies, the authors are used IOT to make the work secured and privacy. The Internet of Thing (IOT) security technique that involves protecting data as it is starts transfers from the local devices in order to the clouded one. Here some techniques are used for the security, the granular methodology, a mathematical model are used to evaluate and identify risks, and 5G modeling

based the indications for making key judgments include station coverage and the metro convenience index.

3. IDA TECHNIQUES IN IOT

The Intrusion Detection Architecture (IDA) is proposed in this section is performed in three stages namely, Data Collection, Pre-processing and Data encoding, and Classification block. The request from the IOT devices is sent to the Data collection (DC) way there it could find the amount of data in pre-processing technique. The collected data traces and filter through the Normalization Technique (NT) by data cleaning in Deep Learning (DL). Then the filtered data goes to the data encoding block. After the encoded data goes to classification block there it classifies the data by Ghost Net technique and finally the attack can be classified and detected. The efficiency of the proposed IDA approach has been determined using the evaluation metrics such as configuration latency, detection rate, accuracy, precision, recall rate, false detection rate. Overall proposed system method has shown and detailed in Figure.1.

3.1 Data collection

In data collection it collects all IOT requested data such as, Protocol, IP address, Frame length, File type, Host post, Frame number, etc. The collected data are the traces of Pre-processing. The Internet of Things device filters packets, chooses features from a range of network features, including the duration and frame number, gives them labels, and stores these details in a database. The gathered data are then taken as traces. The traces from the IOT devices are then pre-processed with data cleaning in Deep Learning (DL) process.

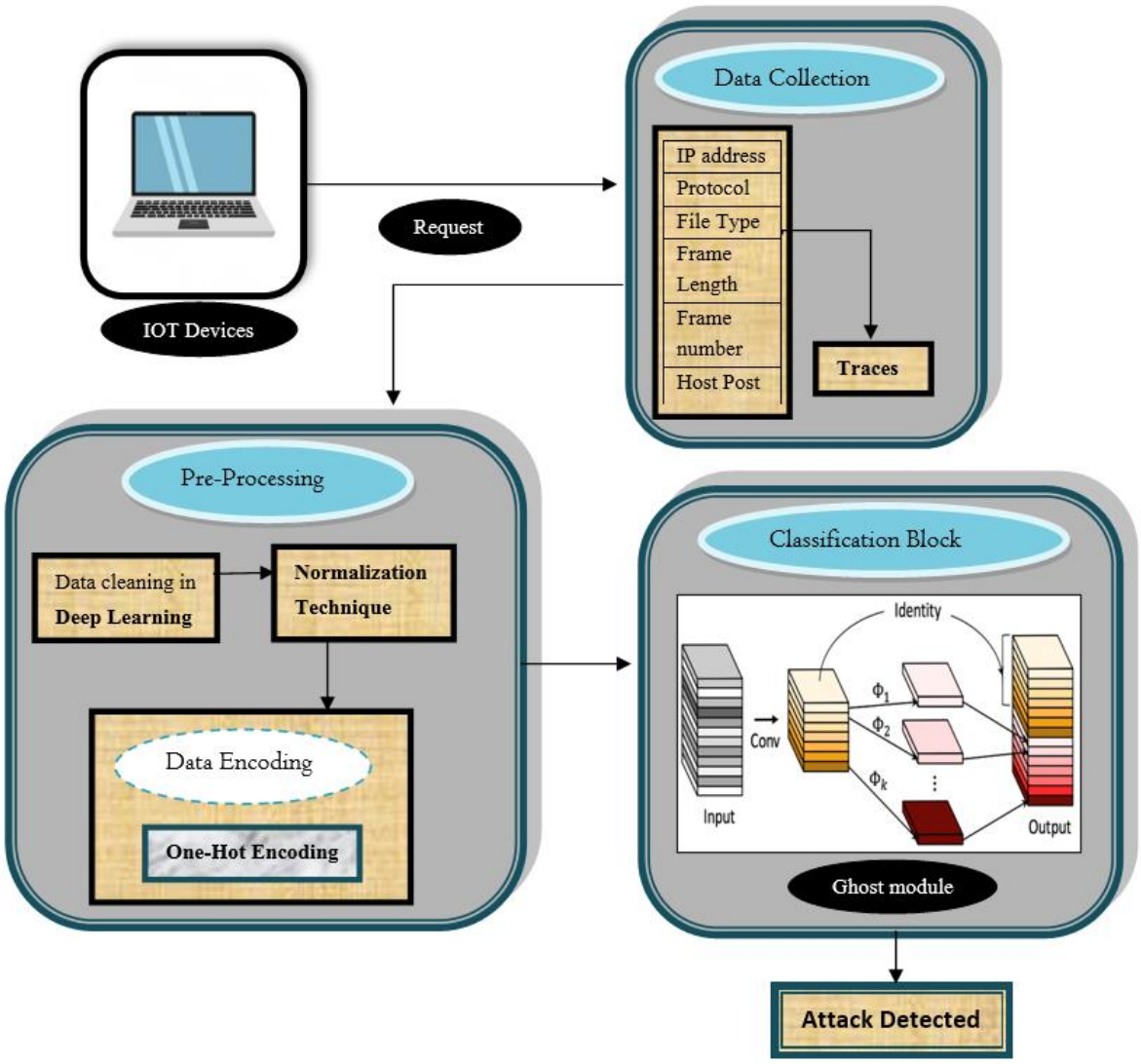

Figure 1. Proposed method

3.2 Pre-processing

The act of transforming unprocessed data into a format that a deep learning (DL) network can use is known as pre-processing. It is the most important and initial step in creating a deep learning model. Finding clean, prepared data is not always the case while working on a Deep Learning project. Before using data, users must also clean and prepare it. Therefore, to do this, we employ a data pre-processing method.

3.2.1 Data cleaning

Data cleaning is the process of fixing or deleting erroneous, corrupted, misleading, duplicate, or insufficient information from a dataset. The following Figure 2 shows the data cleaning steps

Steps involved in data cleaning

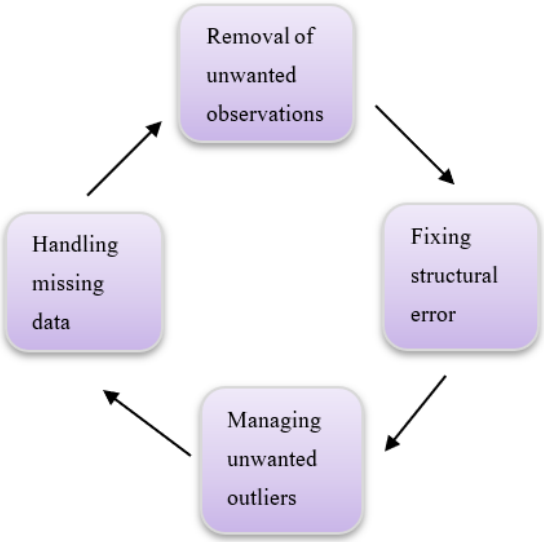

Figure 2. Data cleaning steps

3.2.2. Normalization

Data cleaning is the process of fixing or deleting erroneous, corrupted, misleading, duplicate, or insufficient information from a dataset for Deep Learning (DL). A set of data is transformed to be on a similar scale through normalization. Depending on the data itself, the purpose of machine learning models is typically to recenter and rescale our data so that it is between 0 and 1 or -1 and 1.

3.3 Data encoding

Data encoding is one of the tasks that is seen to be essential. In general, DL models carry out mathematical operations that can be carried out with a wide range of tools and methods. The process of encoding IOT data involves turning categorical data into integer format so that the models may use the converted data to produce and enhance predictions. In this proposed data cleaning technique method use one-hot encoding, it given brief as follows.

3.3.1 One-hot encoding

By one-hot encoding method the IOT data pre-processed, for textual data, the Deep Learning (DL) process is not suitable directly. Data has to be numeric. Hence, in this study for data pre-processing, One-hot vectors were used to encode the IOT text data. A basic way for representing strings with a finite set of values is one-hot encoding, which employs a sparse vector with one member set to 1 and all other elements set to 0. Neural networks frequently employ one-hot encoding because their activation functions call for input to fall within the discrete range of [0, 1] or [-1, 1].

A 1* N matrix (vector) that has 0s in every cell except for one that is used to uniquely identify a word is called a one-hot vector. Categorical data can be represented more expressively using one hot encoding. Three of these encodings [0, 0, 1] would each represent a word range of [good, good, bad]. For the experimental flow Figure 3 is shown as follows.

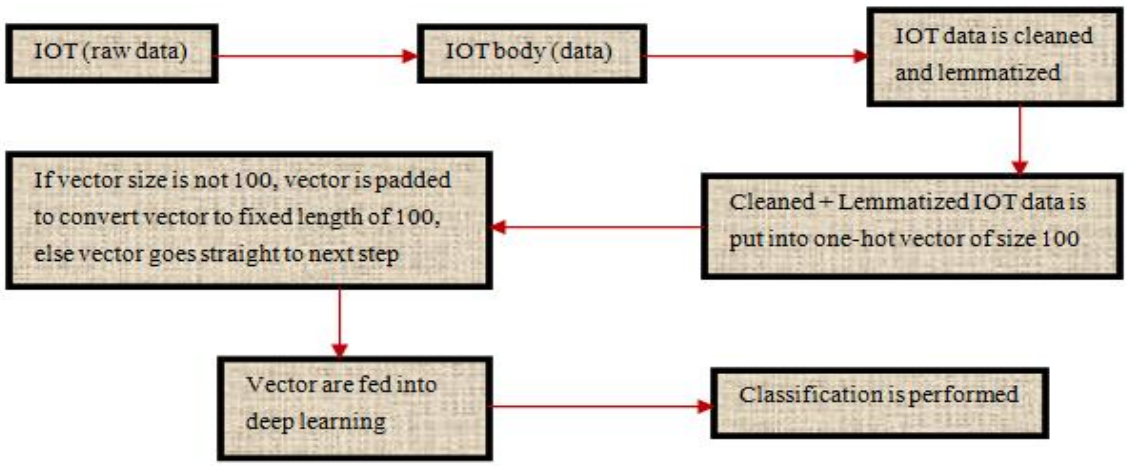

Figure 3. Experimental flow in IOT data

The IOT data utilized in this research was cleaned, lemmatized, and represented as one-hot encoded vectors Lemmatization combines a word's several spellings into one so they can be studied as a single entity. As a result, 100 was chosen as the study's arbitrary length, and padding was applied to all vectors to make them all the same length. These matrices were fed into a neural network or deep learner, and the vectors in these networks were then translated into a low dimensional space. This low dimensional space is represented in the neural network by a hidden layer, where the vocabulary size is smaller than the number of words.

3.4 Ghost Net

Ghost net is used for making decision to access or deny the user request based on the trust value and data owner attributes. The quantity of inference computation is minimized by the ghost net by using linear operations rather

than partial convolution. Convolutional Neural Networks (CNN) were created specifically for decision-making and identification in the ghost net. Rather of employing fully linked layers, which are excessively large to handle large amounts of data, CNNs create a local receptive field for every hidden layer neuron. In order to decrease the network's capacity, enhance the usefulness of its features, and extract multi-scale bottom-level features, a ghost module is induced in the CNN network, as shown in Figure. 4.

3.4.1. Ghost module Architecture

Within a convolutional layer's narrow local window, each neuron receives an input, as does the layer above it. The groups of weights connected to a particular receptive field define a filter. This network maintains the association between the pixels while identifying various characteristics of the inputs, including edges and embosses, using initialised random distributions.. By screening the resulting feature maps, the data is processed in this fashion. As a result, different filters produce different feature maps. The collection of kernels applied during the convolutional phases the same as the output depth in the convolutional layer.

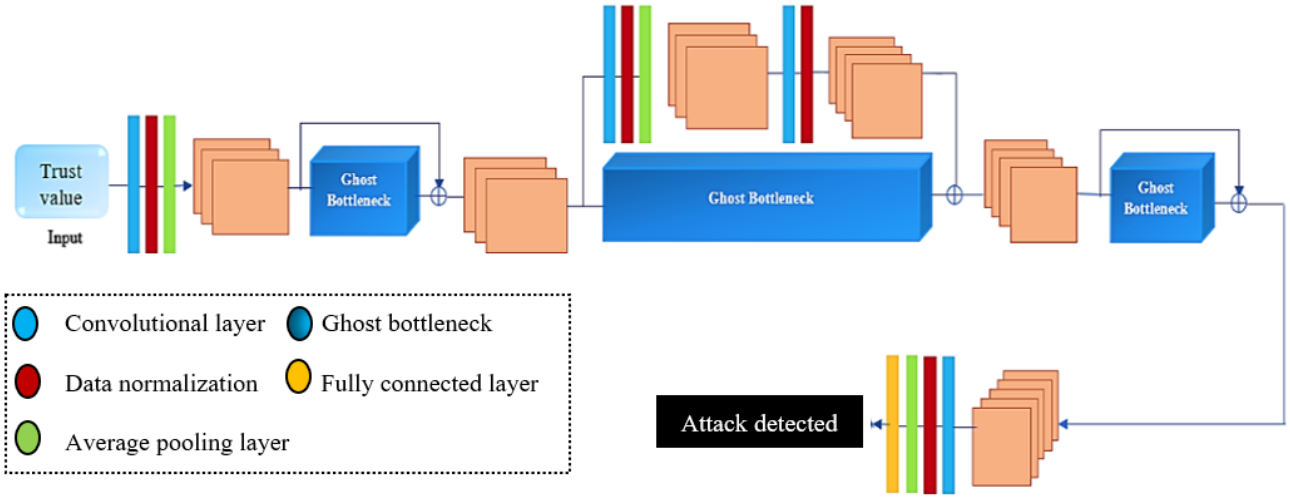

Figure 4. Architecture of Ghost module process

In particular, convolutional layer is considered$G_l \epsilon \mathbb{R}^{w_l * w_l * d_{l-1} * d_l}$, is the definition of the number of weights, where w_l stands for the spatial width and height of the filter, d_{l-1} for the data channels input, and d_l for the number of kernels. $S_{l-1} \epsilon \mathbb{R}^{N_{l-1} * N_{l-1} * K_{l-1}}$, which relates to the bias vector is included, is the representation of the l^{th}convolution process in this framework. It is the linear function obtained in equation (1) that multiplies the equivalent number of weights and the input volume of the layer. As a result, an arbitrary feature map $Z_l \epsilon \mathbb{R}^{N_l * N_l * K_l}$ is obtained, accurately locating identified features within the input data.

$$Z_l = G_l * S_{l-1} + bias_l \quad (1)$$

Equation (2) states that the local receptive field receives the element-wise product of each input element and filter weight when convolutional kernels are applied to the input data. Here, since $\hat{s_i}$and $s_i$are the spectral indices as well as $a, b, \hat{a}$ and $\hat{b}$ are the indexes across the spatial ratios for the input or output data and the weights, $a = \hat{a} - [N_{l-1}/2]$ and $b = \hat{b} - [N_{l-1}/2]$ are interpreted by the recentered spatial indexes.

$$Z_l^{a,b,s_i} = \sum_{\hat{a}\hat{b}\hat{s_i}} G_l^{\hat{a},\hat{b},\hat{s_i}} * S_{l-1}^{a+\hat{a},b+\hat{b},\hat{s_i}} + bias_l^{s_i} \quad (2)$$

As a result, the final output feature maps are obtained by learning the nonlinearities of the data using a non-linear activation function H( ). as $S_l \epsilon \mathbb{R}^{N_l * N_l * K_l}$,

$$S_l = \mathcal{H}(Z_l) \quad (3)$$

Where, $\mathcal{H}$ is applied as Fully Connected (FC) layer, It is typically employed in methods for back propagation. reducing the number of convolutional kernels developed and the number of superfluous feature maps in order to lower the amount of computing storage needed for CNN. Ghost Bottleneck is a reusable module that reduces model size and its structure is similar to the simple residual block in CNN, which is made up of two stacked Ghost modules as shown in Figure 5. A stride of 2 is a depth wise convolution that links two Ghost modules.

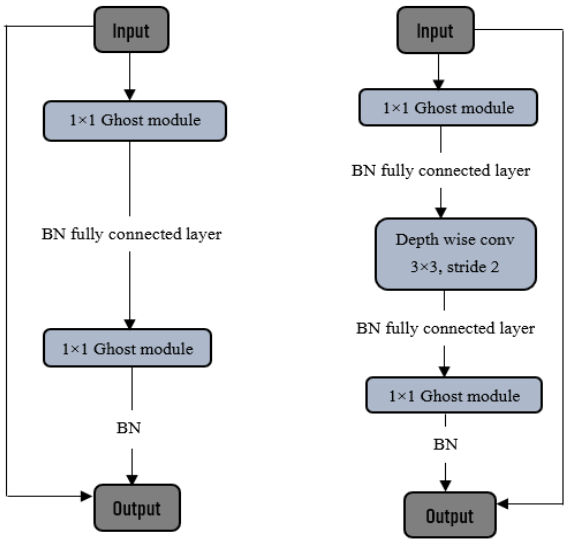

Figure 5. Ghost Bottleneck structure

From each input, a ghost component retrieves intrinsic feature maps, and every single channel of the intrinsic feature maps is given a linear kernel by the paired convolutional layer. The intrinsic feature maps $\tilde{S}_l$ may be easily updated in several simple ways, and the output feature maps S_l are generated as Ghosts. The group known as $S_l \epsilon\ \mathbb{R}^{N_l * N_l * \tilde{K}_l}$ for these intrinsic feature maps is generated by a main convolution from equation (1); the number of kernels is determined by $G_l \epsilon\ \mathbb{R}^{w_l * w_l * d_{l-1} * \tilde{D}_l}$ applied to the input layer data, where $\tilde{D}_l < d_l$

Consequently, a variety of discounted linear techniques are used to each intrinsic feature of $\tilde{S}_l$ in order to construct M ghost features, which are stated in equation (4), in order to obtain the genuine w_l feature maps.

$$S_l^{s_i,q} = \varphi_{s_i,q}\left(\tilde{S}_l^{s_i}\right),\ \forall t = 1, \ldots . \tilde{D}_l, \forall q = 1, \ldots . \tilde{w}_l \qquad (4)$$

The intended $d_l = w * \tilde{D}_l$ feature maps are therefore produced. The resultant volume of the paired layer is combined with the resultant volume of the point-wise layer and moved to the next block. Once the first bottleneck has been eliminated, the second bottleneck needs several convolutions in the shortcut relation to regulate the size of its input feature maps. Furthermore, each feature is combined and optimized by the pooling module, which then provides the outcomes to the two Fully Connected Layers (FC) for use as classifiers in deciding whether to approve or reject user requests.

4. RESULTS AND DISCUSSIONS

Simulations have been performing to evaluate the IDA scheme in IOT security system. Here, the Matlab is used to simulate the Intrusion Detection Architecture (IDA). The detection in IOT intrusion system is maintained by Attack Detection Set or Thread Detection Set with the Network Intrusion Detection System (NIDS) which perform as a detector in IOT system.

The UNSW-NB15 dataset is used to monitor the network problem or system activity problem for malicious or anomalous behavior in the IOT security system applications. The UNSW-NB15 dataset's NetFlow-based format, referred to as NF-UNSW-NB15, has been created and labelled with the appropriate attack categories. There are 1,623,118 data flows in total, of which 1,550,712 (95.54%) are benign and 72,406 (4.46%) are attack samples. So, that here for the IDA it dedicates NIDS to detect the IOT intrusion which detects easily when compared to other.

4.1 Performance metrics

This section presents the simulation results of proposed IDA performance metrics namely Communication overhead, Throughput, Attack graph index, Delay analysis, Signaling Overhead, Attack detection rate with malicious node, Communication cost and Energy consumption. The amount of time it takes a node to process a packet is referred to as computational overhead. The time between the packet being fully received and the node completing its processing should be considered.

After this period, the node might eventually have another packet prepared for transmission.

4.1.1 Communication overhead

Communication overhead factor for the authentication schemes (shown in Figure 6), neglecting protocol overhead. When compared to other methods, the IDA has a larger overhead. Proposed an Intrusion Detection Architecture (IDA) it is built on the device, internet, and semantic architectural views for understanding IoT systems.

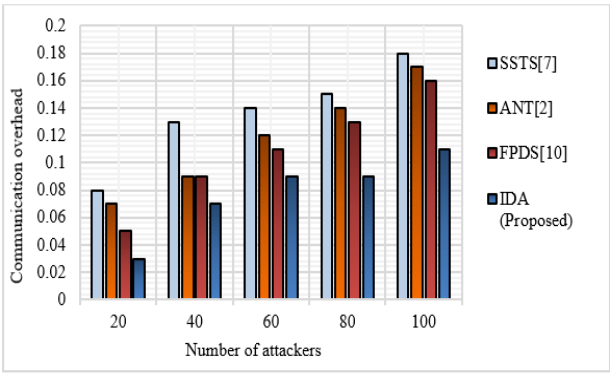

Figure 6. Communication overhead

In Figure 6 the communication overhead factors for authentication scheme compared with some existing techniques which are, Smart Security Transportation System (SSTS) [7], Activity Network Things (ANT) [2], Flexible Privacy-preserving Data Sharing (FPDS) [10] and proposed Intrusion Detection Architecture (IDA). The number of attackers takes within 100 of size, when compared to other three existing technique the IDA proposed is low, -75%, -50% and -38% of SSTS, ANT and FPDS is reduced in communication overhead when compared with proposed IDA as shown in graph Figure 6.

4.1.2 Throughput

The throughput in IOT security is refers to how much the IOT data is actually transfers during a particular period of time. The throughput figure is shown as follows Figure 7.

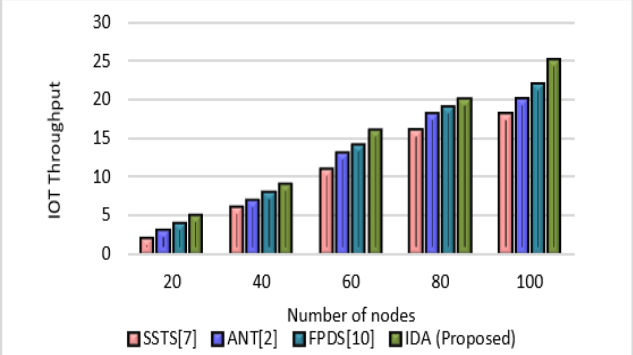

Figure 7. IOT throughput with number of nodes

The IOT throughput with average time is compared with existing three techniques which are, Smart Security Transportation System (SSTS) [7], Activity Network Things (ANT) [2], Flexible Privacy-preserving Data Sharing (FPDS) [10] and proposed Intrusion Detection Architecture (IDA). The number of nodes taken in n=10

<100. Compared with other three existing technique the proposed IDA is high in throughput, 33%, 20%, 13% of SSTS, ANT, FPDS is increased in throughput compared with proposed IDA is shown in Figure 7.

4.1.3 Attack graph

IOT's attack graph plays an important role in this process. IOT security graphs can be used to create multi-stage attack routes, each of which reflects a series of vulnerabilities that an attacker could use to break into a network. The attack graph index is shown below in Figure 8.

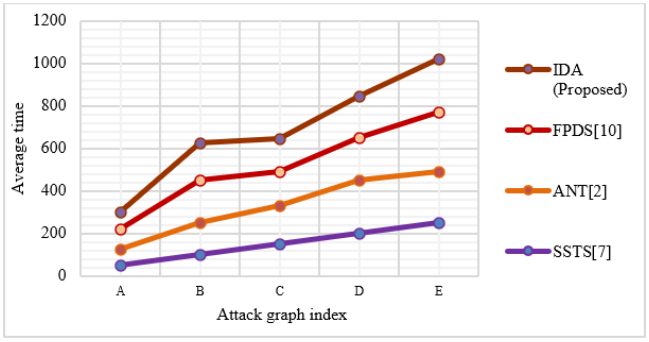

Figure 8. Attack graph index

The attack graph index with average time is compared with existing three techniques which are, Smart Security Transportation System (SSTS) [7], Activity Network Things (ANT) [2], Flexible Privacy-preserving Data Sharing (FPDS) [10] and proposed Intrusion Detection Architecture (IDA). Compared with other existing techniques the proposed IDA is high which shown in Figure 8.

4.1.4. Delay analysis

To determine the percentage of the IOT data delay is attributed to each party (contractor, owner, or neither), delay analysis includes estimating the delay and working backwards from it, delay analysis graph is shown in Figure 9.

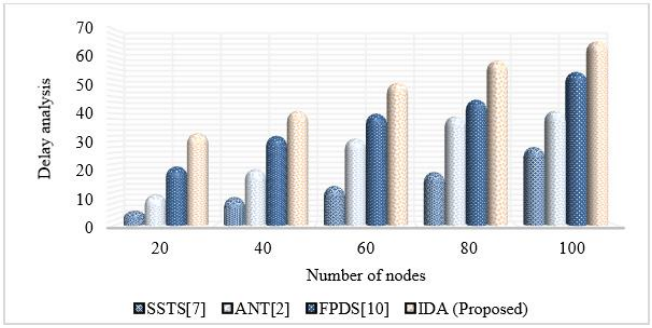

Figure 9. Resultant Graph of the Proposed System

The Delay analysis with number of nodes is compared with existing three techniques which are, Smart Security Transportation System (SSTS) [7], Activity Network Things (ANT) [2], Flexible Privacy-preserving Data Sharing (FPDS) [10] and proposed Intrusion Detection Architecture (IDA) in this graph Figure 9. Compared with other existing techniques the proposed IDA is high.

4.1.5. Signaling overhead

Signaling overhead which contains addition information to enhance performance of the wireless networks in IOT data. The signaling overhead figure in given below in Figure 10.

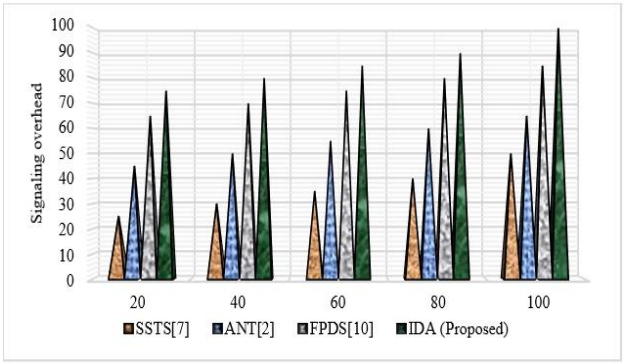

Figure 10. signaling overhead

The signaling overhead is compared with existing three techniques which are, Smart Security Transportation System (SSTS) [7], Activity Network Things (ANT) [2], Flexible Privacy-preserving Data Sharing (FPDS) [10] and proposed Intrusion Detection Architecture (IDA). In signaling overhead, compared with other existing techniques the proposed IDA is high which shown in Figure 10.

4.1.6. Attack detection

A technology called attack detection is used to track IOT data flow and identify any unauthorized entry or activity in the database environment. The attack detection graph is shown in Figure 11.

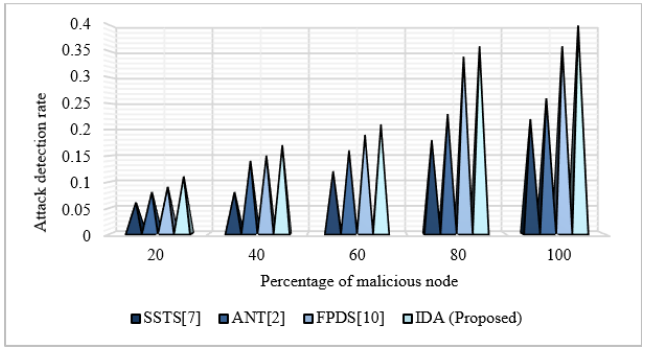

Figure 11. Attack detection rate vs malicious percentage node

The attack detection rate with malicious percentage node is compared with existing three techniques which are, Smart Security Transportation System (SSTS) [7], Activity Network Things (ANT) [2], Flexible Privacy-preserving Data Sharing (FPDS) [10] and proposed Intrusion Detection Architecture (IDA). The number of nodes is taken in between 10<100 of size. Compared with other existing techniques the proposed IDA is high which shown in Fig.11.

4.1.7. Communication cost

Communication cost of the IOT data is depends up on the size and complexity of undertaking data. Here, the communication cost is compared with others is shown in Figure.12

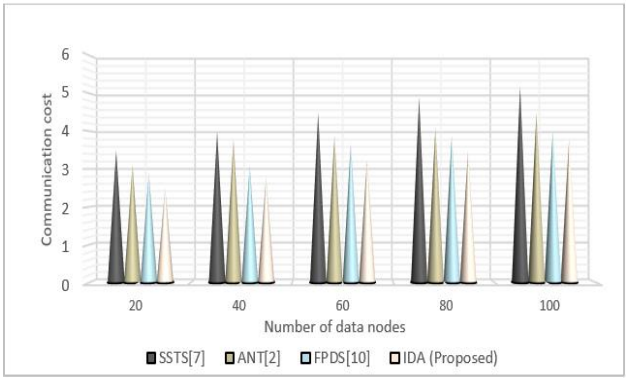

Figure 12. Communication cost with number of data nodes

The communication cost with number of nodes in data are compared with existing three techniques which are, Smart Security Transportation System (SSTS) [7], Activity Network Things (ANT) [2], Flexible Privacy-preserving Data Sharing (FPDS) [10] and proposed Intrusion Detection Architecture (IDA). Number of data nodes are taken in between 10<100 of size. Compared with other existing techniques the proposed IDA communication cost is low, -67%, -33%, -33% of SSTS, ANT, FPDS is reduced in communication cost when compared with proposed IDA. which is shown in Figure.12.

4.1.8. Energy consumption

IoT data enables a smart grid system to control power flow or substantially reduce energy consumption. The energy consumption is shown in graph Figure.13.

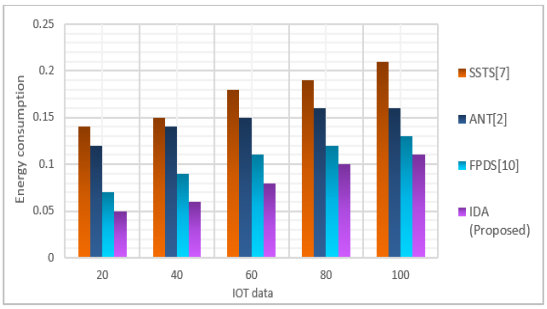

Figure.13. Energy consumption in IOT data

The energy consumption in IOT data is compared with other existing three techniques which are, Smart Security Transportation System (SSTS) [7], Activity Network Things (ANT) [2], Flexible Privacy-preserving Data Sharing (FPDS) [10] and proposed Intrusion Detection Architecture (IDA). Compared with other existing techniques the proposed IDA energy consumption is low which is shown in Figure 13.

5. CONCLUSION

Intrusion Detection Architecture (IDA) has been proposed in this paper, which helps to trace the Intrusion Data in IOT. The proposed Intrusion Detection Architecture (IDA) is performed in three stages namely, Data Collection, Pre-processing in Data encoding and Classification block. The efficiency of the proposed IDA approach has been determined using the evaluation metrics such as configuration latency, detection rate, accuracy, precision, recall rate, false detection rate. The Matlab is used to simulate the Intrusion Detection Architecture (IDA). The detection in IOT intrusion system is maintained by Attack Detection Set or Thread Detection Set with the Network Intrusion Detection System (NIDS) which perform as a detector in IOT system. The proposed method has been evaluated in terms of Communication overhead, Throughput, Attack graph index, Delay analysis, Signaling Overhead, Attack detection rate with malicious node, Communication cost and Energy consumption. The proposed method reduces the communication overhead of 75%, 50% and 38% than SSTS, ANT and FPDS existing techniques. In order to deliver dependable and secure IoT services that will be taken into consideration in the future, backup security solutions must be created and integrated with the DL-based security schemes.

CONFLICTS OF INTEREST

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper**.**

FUNDING STATEMENT

No funding was received to assist with the preparation of this manuscript.

ACKNOWLEDGEMENTS

The authors would like to thank the reviewers for all of their careful, constructive and insightful comments in relation to this work**.**

REFERENCES

[1] R. Ding, H. Zhong, J. Ma, X. Liu, and J. Ning, "Lightweight privacy-preserving identity-based verifiable IoT-based health storage system", *IEEE Internet of Things Journal*, vol. 6, no. 5, pp.8393-8405, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[2] R. Sharma, and R. Arya, "Security threats and measures in the Internet of Things for smart city infrastructure: A state of art", *Transactions on Emerging Telecommunications Technologies*, pp.4571, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[3] L. Nemec Zlatolas, N. Feher, and M. Hölbl, "Security perception of IoT devices in smart homes", *Journal of Cybersecurity and Privacy*, vol. 2, no.1, pp.65-73, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[4] M.Y. ISMAIL, M.S. Beg, M.F. Jamlos, W.H. Azmi, N.H. Badrulhisam, and O.I. Awad, Potential and Limitation of Internet of Things (IOT) Application in the Automotive Industry: An Overview", *International Journal of Automotive and Mechanical Engineering*, vol. 19, no. 3, pp.9939-9949, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[5] S.S. Kute, A.K. Tyagi, and S.U. Aswathy, Security, "privacy and trust issues in internet of things and machine learning based e-healthcare", *Intelligent Interactive Multimedia Systems for e-Healthcare Applications*, pp.291-317, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[6] Y. Wu, H.N. Dai, H. Wang, Z. Xiong, and S. Guo, "A survey of intelligent network slicing management for industrial IoT: integrated approaches for smart transportation, smart energy, and smart factory", *IEEE Communications Surveys & Tutorials*, vol. 24, no. 2, pp.1175-1211, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[7] H. Uddin, M. Gibson, G.A. Safdar, T. Kalsoom, N. Ramzan, M. Ur-Rehman, and M.A. Imran, "IoT for 5G/B5G applications in smart homes, smart cities, wearables and connected cars", In *2019 IEEE 24th International Workshop on Computer Aided Modeling and Design of Communication Links and Networks (CAMAD)*, pp. 1-5, 2019. IEEE. [CrossRef] [Google Scholar] [Publisher Link]

[8] K. Demestichas, N. Peppes, and T. Alexakis, "Survey on security threats in agricultural IoT and smart farming", *Sensors*, vol.20, no.22, pp.6458, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[9] P. Ratta, A. Kaur, S. Sharma, M. Shabaz, and G. Dhiman, "Application of blockchain and internet of things in healthcare and medical sector: applications, challenges, and future perspectives", *Journal of Food Quality*, pp.1-20, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[10] E.S. Ali, M.K. Hasan, R. Hassan, R.A. Saeed, M.B. Hassan, S. Islam, N.S. Nafi, and S. Bevinakoppa, "Machine learning technologies for secure vehicular communication in internet of vehicles: recent advances and applications", *Security and Communication Networks*, 2021, pp.1-23, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[11] W.D. Lin, and M.Y. Low, "Concept design of a system architecture for a manufacturing cyber-physical digital twin system", In *2020 IEEE International Conference on Industrial Engineering and Engineering Management (IEEM)*, pp. 1320-1324, 2020. IEEE. [CrossRef] [Google Scholar] [Publisher Link]

[12] K.O.M. Salih, T.A. Rashid, D. Radovanovic, and N. Bacanin, "A comprehensive survey on the Internet of Things with the industrial marketplace", *Sensors*, vol. 22, no. 3, pp.730, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[13] A. Kumari, S. Tanwar, S. Tyagi, and N. Kumar, Verification and validation techniques for streaming big data analytics in internet of things environment. *IET Networks*, vol. 8, no. 3, pp.155-163, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[14] A. Attkan, and V. Ranga, "Cyber-physical security for IoT networks: a comprehensive review on traditional, blockchain and artificial intelligence-based key-security", *Complex & Intelligent Systems*, vol. 8, no. 4, pp.3559-3591, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[15] B. Alotaibi, "Utilizing blockchain to overcome cyber security concerns in the internet of things: A review", *IEEE Sensors Journal*, vol. 19, no. 23, pp.10953-10971, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[16] J. Franco, A. Aris, B. Canberk, and A.S. Uluagac, "A survey of honeypots and honeynets for internet of things, industrial internet of things, and cyber-physical systems", *IEEE Communications Surveys & Tutorials*, vol. 23, no. 4, pp.2351-2383, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[17] I. Vaccari, E. Cambiaso, and M. Aiello, "Evaluating security of low-power internet of things networks", *International Journal of Computing and Digital Systems*, vol. 8, no. 02, pp.101-114, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[18] H.M. Akwetey, P. Danquah, and I. Asampana, "Critical infrastructure cybersecurity challenges: Iot in perspective", *arXiv preprint arXiv:2202.12970*. 2022. [CrossRef] [Google Scholar] [Publisher Link]

[19] Y. Zhang, B. Li, B. Liu, Y. Hu, and H. Zheng, "A privacy-aware PUFs-based multiserver authentication protocol in cloud-edge IoT systems using blockchain", IEEE Internet of Things Journal, vol. 8, no. 18, pp.13958-13974, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[20] W. Iqbal, H. Abbas, M. Daneshmand, B. Rauf, and Y.A. Bangash, "An in-depth analysis of IoT security requirements, challenges, and their countermeasures via software-defined security", *IEEE Internet of Things Journal*, vol. 7, no. 10, pp.10250-10276, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[21] K.Y. Lam, S. Mitra, F. Gondesen, and X. Yi, "ANT-centric IoT security reference architecture—Security-by-design for satellite-enabled smart cities", *IEEE Internet of Things Journal*, vol. 9, no. 8, pp.5895-5908, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[22] S. Verma, Y. Kawamoto, and N. Kato, "A network-aware Internet-wide scan for security maximization of IPV6-enabled WLAN IoT devices", *IEEE Internet of Things Journal*, vol. 8, no. 10, pp.8411-8422, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[23] W. Zhou, C. Cao, D. Huo, K. Cheng, L. Zhang, L. Guan, T. Liu, Y. Jia, Y. Zheng, Y. Zhang, and L. Sun, "Reviewing IoT security via logic bugs in IoT platforms and systems", *IEEE Internet of Things Journal*, 8(14), pp.11621-11639, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[24] J. Zhang, Y. Wang, S. Li, and S. Shi, "An architecture for IoT-enabled smart transportation security system: a geospatial approach", *IEEE Internet of Things Journal*, vol. 8, no. 8, pp.6205-6213, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[25] J. Kim, P.V. Astillo, V. Sharma, N. Guizani, and I. You, "MoTH: Mobile Terminal Handover Security Protocol for HUB Switching based on 5G and Beyond (5GB) P2MP Backhaul Environment", *IEEE Internet of Things Journal*, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[26] F. Zhu, X. Yi, A. Abuadbba, I. Khalil, S. Nepal, and X. Huang, "Cost-Effective Authenticated Data Redaction with Privacy Protection in IoT", *IEEE Internet of Things Journal*, vol. 8, no. 14, pp.11678-11689, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[27] S. Hui, Z. Wang, X., Hou, X. Wang, H. Wang, Y. Li, and D. Jin, "Systematically quantifying IoT privacy leakage in mobile networks. *IEEE Internet of Things Journal*, vol. 8, no. 9, pp.7115-7125, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[28] H. Deng, Z. Qin, L. Sha, and H. Yin, "A flexible privacy-preserving data sharing scheme in cloud-assisted IoT", *IEEE Internet of Things Journal*, vol. 7, no. 12, pp.11601-11611, 2020. [CrossRef] [Google Scholar] [Publisher Link]

AUTHORS

M. AmanullaKhan received M.E degree in applied electronics from Anna university in 2008, India working as an assistant professor in the department of Electronics and communication engineering at Mohammad Sathak Engineering college, India. His area of interest includes image processing, computer vision, Internet of things, pattern recognition bio metrics and gait recognition he presented various international conference events like IAEME, SCOPUS, and materials today, he has CSTA and ISTE membership. He has guided many computer vision projects and hands on programming MATLAB, PYTHON at various technical institutions around India**.**

M. Usha is currently working as an Associate Professor and HOD in MEASI Institute of Information Technology, Chennai. She has completed M.C.A. and M.Phil. in Computer Science from Bharathidasan University, Trichy. She has also done her M. Tech (CIT) and Ph.D. from Manonmaniam Sundaranar University, Tirunelveli. She has 20 years of teaching experience and she has published papers in Network Security in National and International journals and has presented in International Conferences and Seminars. Her area of interests includes Operating Systems, Artificial Intelligence, Machine Learning, Algorithms and ad-hoc networks especially FANET and Underwater Communication.

S. Ramesh received Ph.D. degree from Anna University, India. He received M.E degree from Anna University, India. He received B. Tech degree in Anna University, India. He is Working as an Associate Professor nearly 14 years still now in Department of Computer science Engineering, Krishnasamy college of Engineering & Technology, Anand Nagar, Kumarapuram, Cuddalore. He got Anna University Supervisor Recognition on 2021. His research interest includes Embedded system and Wireless sensor networks.

Arrived: 25.08.2023
Accepted: 25.10.2023