Journal of ISMAC (2020)
Vol.02/ No.04
Pages: 190-199
http://irojournals.com/iroismac/
DOI: https://doi.org/10.36548/jismac.2020.4.002

Hybrid Intrusion Detection System for Internet of Things (IoT)

Dr. S. Smys,
Professor, Department of Computer Science and Engineering,
RVS Technical Campus,
Coimbatore, India.
Email: smys375@gmail.com

Dr. Abul Basar,
Professor, Prince Mohammad Bin Fahd University,
Kingdom of Saudi Arabia.
Email: abashar@pmu.edu.sa

Dr. Haoxiang Wang,
Department of Electrical and Computer Engineering,
Cornell University, Ithaca, USA.
Email: wanghaoxiang1102@hotmail.com

Abstract: - Internet of things (IoT) is a promising solution to connect and access every device through internet. Every day the device count increases with large diversity in shape, size, usage and complexity. Since IoT drive the world and changes people lives with its wide range of services and applications. However, IoT provides numerous services through applications, it faces severe security issues and vulnerable to attacks such as sinkhole attack, eaves dropping, denial of service attacks, etc., Intrusion detection system is used to detect such attacks when the network security is breached. This research work proposed an intrusion detection system for IoT network and detect different types of attacks based on hybrid convolutional neural network model. Proposed model is suitable for wide range of IoT applications. Proposed research work is validated and compared with conventional machine learning and deep learning model. Experimental result demonstrate that proposed hybrid model is more sensitive to attacks in the IoT network.

Keywords: - Intrusion detection system (IDS), Internet of Things (IoT), Network attacks

1. Introduction

Internet of Things (IoT) gain more attention in the recent time due to its novel applications and support to numerous domains such as industrial process, health care, automation, smart environment, etc., Though IoT provides wide range of services and application, it faces sever security issues as attacks. Since IoT is a heterogeneous environment and its interoperability mechanism is not supportive for conventional security methods. However, security in IoT is enhanced in other terms such as data authentication, confidentiality and access controls. These security measures are developed between the user and IoT but still if faces security issues. So it is essential to provide a separate module to ensure the IoT network security. Intrusion detection system (IDS) is such a concept which is already in use in wireless networks. Enhancing the wireless networks IDS features will help IoT to secure the network from attacks and other vulnerabilities.

In order to provide efficient and convenient environment to user, IoT used internet and real time applications. IoT is not specific for a single objective, it provides supports to achieve multiple objectives and it must meet its security requirements for large scale attacks. Before developing an intrusion detection system, it is essential to obtain prior knowledge about IoT environment and its security issues. Some of the major IoT security properties are summarized as follows.

ISSN: 2582-1369 (online)
Submitted: 29.08.2020
Accepted: 23.09.2020
Published: 30.09.2020

Journal of ISMAC (2020)
Vol.02/ No.04
Pages: 190-199
http://irojournals.com/iroismac/
DOI: https://doi.org/10.36548/jismac.2020.4.002

- Data Confidentiality - Fundamental IoT protection requirement Data alteration, modification in IoT appliances should not performed by authorized user. Data privacy is essential for industrial and individual applications and modification in health data will leads into severe issues. So data confidentiality is an important factor in the IoT environment.
- Data Integrity – Data Integrity in IoT environment is an essential factor. Since it works in an heterogeneous environment and data are moved from remote places to central unit. Trustworthiness and guaranteed service to transfer data from remote systems is essential in IoT. So it is necessary to define the data integrity by verifying the data source and identify the malicious attacks in an IoT module.
- Data Availability – The collected information in an IoT framework must be consistently accessible to the user and it an important process in an IoT module. Since without access to data the process is failure to user, so IoT must provide data access to user at any time at any place. But the devices used by the user may encounter vulnerabilities which leads into security issues to the network. So it is essential to provide safe data access to the user.
- Authentication – Generally verification process in IoT differs from one system to other and the objects are need to be classified at initial stage itself is an essential process. IoT requires a strong conformation process to provide authorization and access to the data along with better adaptability skills. This will increase the tradeoff between the IoT environment and data in the system.
- Authorization – The user privileges against data accessibility in an IoT environment is need to be defined with better authorization process. By measuring the appliances and the information confidentiality, the authorization process is need to be defined in a network.

Considering the security measures it is essential to develop a security mechanism for an IoT environment. Data oriented security mechanism is need to be focused to prevent unauthorized access of data source from malicious users. It is essential to focus the data confidentiality and integrity which mainly reduces the serious security threats in an IoT environment. Conventional security mechanisms are developed based on cryptography techniques and it is not widely adopted for IoT environment due to large volume of data. The threats must be identified with in a minimum time will reduce the issues in the network and conventional security models requires more time to process such large amount of data to identify the threats. Unauthorized access to data for short duration of time is sufficient for a malicious user to obtain confidential data and modification of such data leads into huge impact over the user. So it is essential to identify an intruder in an IoT network, Implementing IDS is necessary. Intrusion detection systems detects the intruders and secure the network and data by preventing access to the unauthorized users. But due to limitation of energy sources implementing IDS is a complex process. In order to reduce such complexity a central intrusion detection system could be used which monitors the network and remote nodes and identifies the intrusions. So, an alert is triggered to the network administrator to respond for the security issues. Figure 1 depicts an illustration of intrusion detection system.

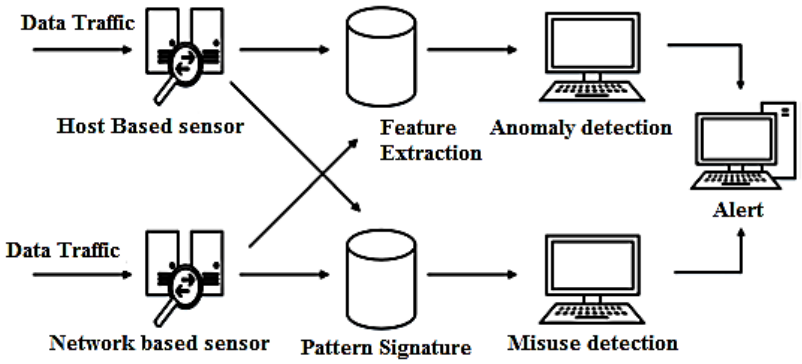

Fig. 1 Intrusion detection system

ISSN: 2582-1369 (online)
Submitted: 29.08.2020
Accepted: 23.09.2020
Published: 30.09.2020

Journal of ISMAC (2020)
Vol.02/ No.04
Pages: 190-199
http://irojournals.com/iroismac/
DOI: https://doi.org/10.36548/jismac.2020.4.002

The operation of intrusion detection system is divided into three phases. Monitoring is the initial phase in IDS which is based on network or host sensors. Analysis is the second phase of IDSs which performs feature extraction and pattern identification based process. Detection is the last phase of IDSs which detects the anomaly or intrusion in a network. IDS helps to monitor and analyze the information, services and networks, traffic analysis through its effective network management and identification of vulnerabilities in a minimum span of time. It protects the network against attacks and improves the data, network confidentiality and integrity. IDS summarize the data traffic of system, and analyze it to detect harmful or malicious activities.

Conventional intrusion detection system architecture is mainly focused to provide security to internet management characteristics and it lags in real time large volume data streams security. Basically conventional IDS are categorized into three types such as placement strategy, detection strategy and validation strategy. Figure 2 depicts the different types of intrusion detection systems in IoT environment. Among these three categories, detection strategy gains more attention and most of the systems are developed based on detection strategies only. Signature based IDS, Anomaly based IDS, specification based IDS and Hybrid IDS are the sub categories in detection strategies.

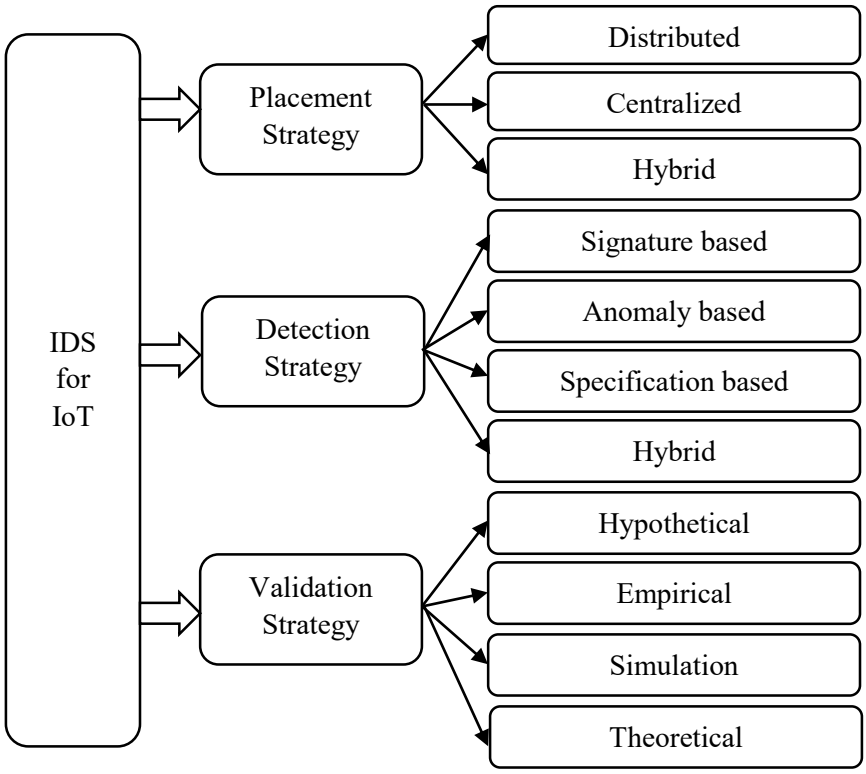

Fig. 2 Intrusion Detection Systems in IoT environment

- Signature based IDS – It describes the attacks and its patterns and identifies the attacks. On detecting an attacks in a network, signature based detection system raises an alert about the suspicious activities and perform pattern matching. Based on the similarity and difference the access or alert provided to the user and detect the attacks effectively.
- Anomaly based IDS – It is an initial stage intrusion detection system which collects the data and identifies the abnormalities in the system. Based on a threshold value, the normal and abnormal behaviors are identified and an alert is raised to network administrator about the abnormalities. It detects the unknown attacks efficiently, but it requires large memory to process and computation cost are the limitations of anomaly based intrusion detection system.

ISSN: 2582-1369 (online)
Submitted: 29.08.2020
Accepted: 23.09.2020
Published: 30.09.2020

Journal of ISMAC (2020)
Vol.02/ No.04
Pages: 190-199
http://irojournals.com/iroismac/
DOI: https://doi.org/10.36548/jismac.2020.4.002

- Specification based IDS – Based on the specific operation, these systems continuously evaluated the system operations. The specific operation is defined by the network administrator and it is monitor the process continuously to validate the operation. If abnormalities detected as per the operation, an alert is forwarded to the network administrator.
- Hybris IDS – Combination of anomaly and signature based IDSs are considered as hybrid models which provides better tradeoff between the storage and computing cost with less false positive alarms. Recently most of the systems are based on Hybrid IDS due to its effective detection and simplified operation.

2. Related Works

Intrusion detection system mainly focuses on detecting attacks and it is essential to define the different of types of attacks encounters in an IoT environment. Various research works are evolved to define an advanced intrusion detection system and still the process is going on to obtain an efficient system to identify different kinds of attacks. Some of the major attacks are categorized in IoT are Sybil attack, selective forwarding attack, service attack, wormhole attack, replay attack, sinkhole attack, false data attack, black hole attack, jamming attack etc., figure 4 provides a detailed view of different types of attack in IoT environment.

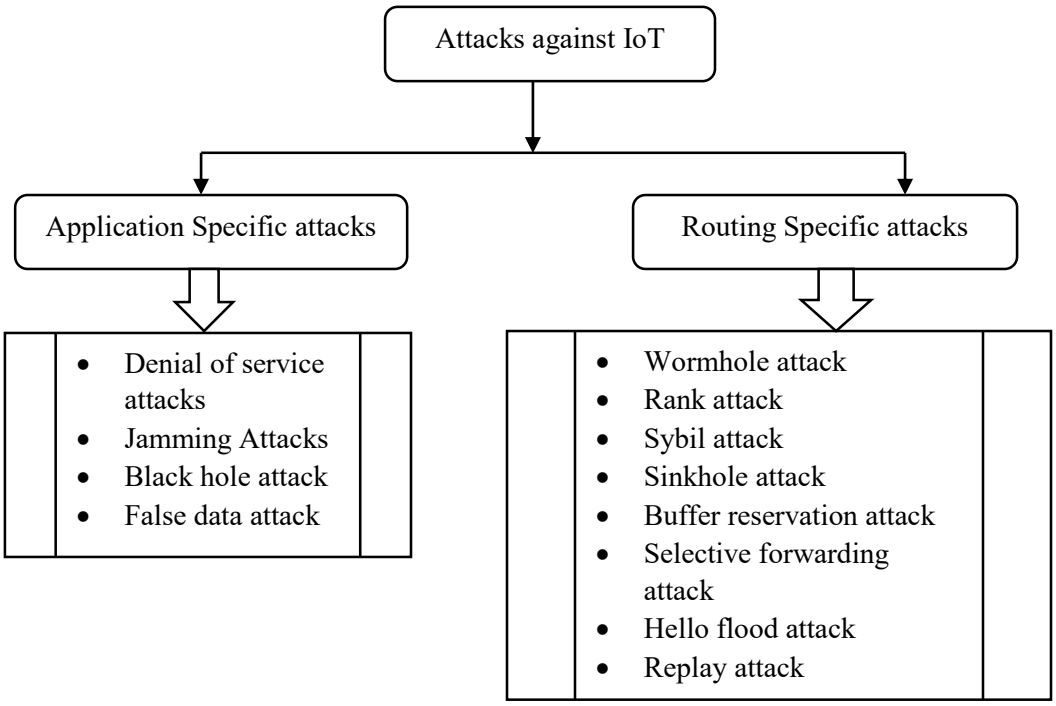

Fig. 3 Classification of attacks in IoT Systems

Snehal *et.al.* [1] reported routing specific attack in an IoT environment. Research work focused wormhole attack in which the target node is attacked or breached from two different directions. Identifying the position of intruder in a network is difficult and research focused to identify the intruder position and alerts the network administrator. Identifying the neighborhood nodes and extracting the impact of threat is considered as a merit of this research work. Rup Kumar *et.al.* [2] discussed about rank attacks in an IoT environment. It is basically a routing based intrusion which occurs in a low power networks. The nodes are specified by certain ranks and its values are updated at regular time intervals. On certain conditions, intruder modifies the ranking process so that a worst node is selected by the routing process which reduces the system performance. Based on the rank rule an efficient topology is framed in the research work by avoiding conventional loop formulation process which provides better overhead.

ISSN: 2582-1369 (online)
Submitted: 29.08.2020
Accepted: 23.09.2020
Published: 30.09.2020

Journal of ISMAC (2020)
Vol.02/ No.04
Pages: 190-199
http://irojournals.com/iroismac/
DOI: https://doi.org/10.36548/jismac.2020.4.002

The impact of Sybil attack over IoT network is focused in Shailendra *et.al.* [3] research model. In Sybil attack the node has produce multiple identities so, it would produce various routing protocols. Detection algorithms and spoofing methods are required to identify such attacks. Depends upon the intruder efficiency and impact of attack Sybil attacks are classified. Alekha *et.al.* [4] discussed about social graph based Sybil attack which identifies the intruder in a network through its graph process. Classification based detection are considered as the important domain in IoT security. If a specific node is comprised to extract all the data from its neighbor nodes, then it is technically termed as sinkhole attack. Guangjie *et.al.* [5] reported sink hole attack and its impact over the network in his research work which identifies the malicious nodes and its routing process in the network. Based on the routing cost these types of attacks are identified in the network. Yuxin Liu *et.al.* [6] Proposed work introduces an intrusion detection system to identify the sinkhole attack using RPL routing protocol which evaluates the received packets and transmitted packets ratio to obtain the intrusion ratio. On identifying the malicious nodes, system generates an alert to network administrator to minimize the intrusion impacts.

Bin Xu *et.al.* [7] reported about buffer reservation attack which caused due to duplication of nodes in the network. Intruder fragments the nodes and created duplicate nodes for attack and performs malicious operations in the network. The user is unaware of such network change and the fragmented information. So the intruder user the buffer space and captures the other nodes in the network. Chen Lyu *et.al.* [8] reported one of the important issues in IoT security such as denial of service (DoS) attack. In this process, intruder attacks over the node and denies other nodes request for data service. These inability of node condition is referred as denial of service. While Distributed Denial of Service (DDoS) used multiple nodes for the same process to make the network unusable for the user. Proposed intrusion detection model identifies the malicious user in the network. Mahmudul Hasan *et.al.* [9] reported various strategies of denial of service attacks as a survey. Research summary provides an overview of different prevention mechanism and detection techniques against DoS and DDoS attacks.

Ju Ren *et.al.* [10] reported the issues in IoT network due to selective forwarding attack. In this, a malicious node presents itself as a primary node for transmission and affects the network routing and transmission performance. In this process, selective messages are considered for transmission and other messages are slinked in the node itself and blocks the data transmission which affects the routing operation. Noshina Tariq *et.al.* [11] Intrusion detection model using this research work utilizes artificial neural network to identify such attacks in an IoT network. Research work is validated with a real time data transmission system which forwards the control messages and blocks other messages. With high detection ratio and less computation cost the proposed model identifies the intruder in the network.

Pham *et.al.* [12] proposed an intrusion detection system to identify the hello flood attack in a network. This type of routing protocol continuously transmits hello messages in the network and creates disturbance in network transmission. Identifying such attacks in difficult as the intruder changes the node positon upon every transmission. Proposed detection model identifies attacks in an IoT network through back propagation neural network model. The learning algorithm selects the malicious features and identifies the intruder in an effective manner. Along with flooding attack, denial of service attack and wormhole attack are also identified and analyzed in the experimental model. Bo Chen *et.al.* [13] discussed about intrusions in IoT environment and focused the research work to identify the sinkhole, replay attack and Sybil attacks. In this replay attack is intrusion is performed on different timings to collect the necessary data and then replayed by the intruder in the network. This leads into unwanted issues to the user community which faces serious issues on important transmissions. Proposed model effectively identifies such attacks through fuzzy based intrusion detection system which perform detection process through set of rules.

Olivier Brun *et.al.* [14] discussed about jamming attack in an IoT environment in which the transmission medium is monitored by the intruder. In this type of attacks, intruder gains attention over the network by tracking the control frequency and interrupts the communication between source node and destination node. Research work proposed an intrusion detection system using adaptive fuzzy neuro inference system to identify jamming, Sybil and denial of service attacks. The computation cost of these system is high which is the major limitation. Haythem *et.al.* [15] proposed an intrusion detection system using deep neural network which effectively identifies the black hole attack and false data attack. In the black hole attack, an intruder observes the user requested data packets to obtain confidential information. Observing the properties of routing module intruder performs such attacks and gains essential user information which affects the trustworthiness of the network. In case of false data attack, intruder observes the network organization and structure and tampers the network by inserting fake reply packets. Proposed

ISSN: 2582-1369 (online)
Submitted: 29.08.2020
Accepted: 23.09.2020
Published: 30.09.2020

Journal of ISMAC (2020)
Vol.02/ No.04
Pages: 190-199
http://irojournals.com/iroismac/
DOI: https://doi.org/10.36548/jismac.2020.4.002

model used hybrid machine learning approach to detect such attacks in the network. Table 1 provides a summary of attacks and its nature in detail.

Table 1 Summary of IDSs in IoT

Reference	Detection Category	Strategy	Attack Type
Snehal *et.al.* [1]	Anomaly based IDS	Hybrid	Wormhole attack
Rup Kumar *et.al.* [2]	Specification based IDS	Hybrid	Rank attack
Shailendra *et.al.* [3], Alekha *et.al.* [4]	Routing based IDS	Distributed	Sybil attack
Guangjie *et.al.* [5] Yuxin Liu *et.al.* [6]	Anomaly based IDS	Hybrid	Sink hole attack
Bin Xu *et.al.* [7]	Specification based IDS	Hybrid	Buffer reservation attack
Chen Lyu *et.al.* [8] Mahmudul Hasan *et.al.* [9]	Anomaly based IDS	Distributed	Denial of Service
Ju Ren *et.al.* [10] Noshina Tariq *et.al.* [11]	Anomaly based IDS	Distributed	Selective forwarding attack
Pham *et.al.* [12]	Specification based IDS	Hybrid	Flooding attack, denial of service attack and wormhole attack
Bo Chen *et.al.* [13]	Anomaly based IDS	Hybrid	Sinkhole, replay attack and Sybil attacks
Olivier Brun *et.al.* [14] Haythem *et.al.* [15]	Specification based IDS	Centralized	jamming attack, black hole attack and false data attack

3. Proposed Work

The proposed intrusion detection system is developed on analyzing the issues in existing IDSs. From the survey it is clear that research works are lags in intrusion detection since the research models are focused towards detection of single attacks. Few research models are focused towards multiple attack detection and its computation cost is quite high which makes the system is not suitable for wide range of applications. In order to obtain an efficient detection system this proposed research work focused towards convolutional neural network which is familiar in recent times. It is a well-known deep learning model for data classification and provides better performance for diverse database collections. Recently convolutional neural network based intrusion detection systems are evolved and its performance is better than existing detection systems. Though the performance is better, to detection wide range of anomaly and malicious attacks in the network proposed research model combines long short term memory (LSTM) which is basically a recurrent neural network (RNN) model to achieve improved performance.

Proposed model is divided into four stages such as collection of data, pre-processing of data, training the network and identifying the attack. In this collection of essential data from the network is an essential process. System log and its features are selected as data and it is pre-processed to remove unwanted noises. These fine-tuned data is provided as input to training model by defining the convolutional layer, size of sliding window, neuron link weights and outputs. Finally in the detection stage, the trained data and actual collected information are processed together to obtain the weights and the training period is used to detect the attacks. The network structure consists of an input layer which has a set of matrices $m_0 \times n_0$ and the output layer has set of neurons for each labels. Hidden layers are used to generalize the features which includes more than one convolutional matrixes and its filter matrices. A set of parameters is used to calculate the product of convolution and filter features such as $(s, w_n * h_n, st_1)$ and $(s, w_m * h_m, st_2)$. Where s is the shared matrices weight depth and sliding steps are represented as st_1, st_2. The sliding window size is given as $w_n * h_n$ and the filter window size is defined as $w_m * h_m$. Hidden layer is the last layer which is used to connect the output layer and obtains the classification results. Based on the sliding window size and convolution the resulting matrix size is obtained. Similarly to resulting matrix, the filter window size is also defined and it is given as

ISSN: 2582-1369 (online)
Submitted: 29.08.2020
Accepted: 23.09.2020
Published: 30.09.2020

Journal of ISMAC (2020)
Vol.02/ No.04
Pages: 190-199
http://irojournals.com/iroismac/
DOI: https://doi.org/10.36548/jismac.2020.4.002

$$w_n * h_n = \left(\frac{w_{n-1}-w_m}{st1_n} + 1\right) \times \left(\frac{h_{n-1}-h_m}{st1_n} + 1\right) \quad (1)$$

where $w_n * h_n$ and $w_{n-1} * h_{n-1}$ represents the resulting matrix size, sliding step size is given as $st1_n$, the size of sliding window is given as $w_m * h_m$. Long short term memory (LSTM) is used in this stage to learn the content across the network. This process is introduced to obtain essential features from the nodes and it helps to identify the malicious nodes and its attacks. LSTM is basically an RNN based network model which used time stamps to obtain the output for an input function. But using LSTM alone could not efficiently detect the intrusion in the network since LSTM has gradient vanishing issue which unable to learn the information for long duration. But for short time duration the performance of LSTM is much better and it greatly reduces the system complexity. Due to this LSTM is used along with convolutional neural network in the proposed intrusion detection system. Figure 4 depicts the general architecture of Bidirectional LSTM. In the Conventional LSTM, a sequence of inputs are forwarded to the network hidden layers and produces outputs in the respective output layer. Later bidirectional LSTM models are evolved which process the input sequence in forward and backward direction using two hidden layers. These properties are related to the data transmission in the network and obtained the necessary data.

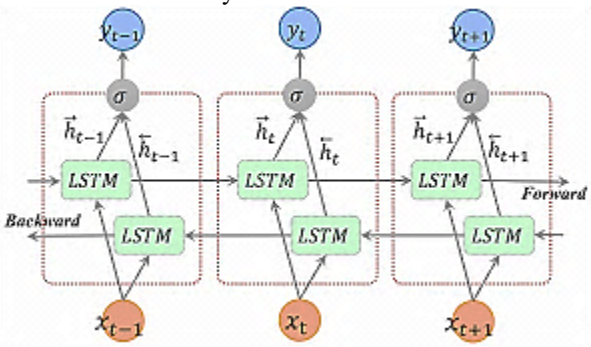

Fig. 4 Bidirectional LSTM architecture

In the training phase, the input features are labelled and each element is assigned in feature matrix based on the input neurons. On processing the inputs, it obtains the neural link weights and weight matrix for the convolutional layer. The setup has x number of convolutional layers and vector layers are represented as f, output neurons are represented as y and the weight function is obtained as

$$W_y = \sum_{n=1}^{N} \sum_{m=1}^{M_n} (x_n * f_n + 1) + x * f \quad (2)$$

where W_y is the network total weight, $x_n * f_n$ is the window filter size, M_n is the number of filters in the convolutional layer. In the training process, each input and its corresponding weights creates a label based on the loss function. The loss function is obtained based on compactness and descriptiveness of the model training and validation data and it is given as

$$L_f = L_c + \varphi * L_d \quad (3)$$

where φ is the scaling factor which is used to evaluate the node priority and L_c, L_d represents the compact loss and descriptive loss respectively. In the detection phase, the features are extracted from the dataset and then converted into feature matrix. Matrix function helps to obtain the weight set from the training process and the output layer defines the neuron label. Using activation function the outputs are observed and it is given as

$$f_m(y) = \frac{e^{om}}{\sum_{m-1}^{n} e^{on}} \quad (4)$$

The activation function obtains the output probability of each neuron and its fully connected layer weight. Generally, the value of activation function lies between 0 to 1 and a maximum value represents the output label. Figure 5 depicts the overall process flow of proposed intrusion detection system for an IoT environment.

ISSN: 2582-1369 (online)
Submitted: 29.08.2020
Accepted: 23.09.2020
Published: 30.09.2020

Journal of ISMAC (2020)
Vol.02/ No.04
Pages: 190-199
http://irojournals.com/iroismac/
DOI: https://doi.org/10.36548/jismac.2020.4.002

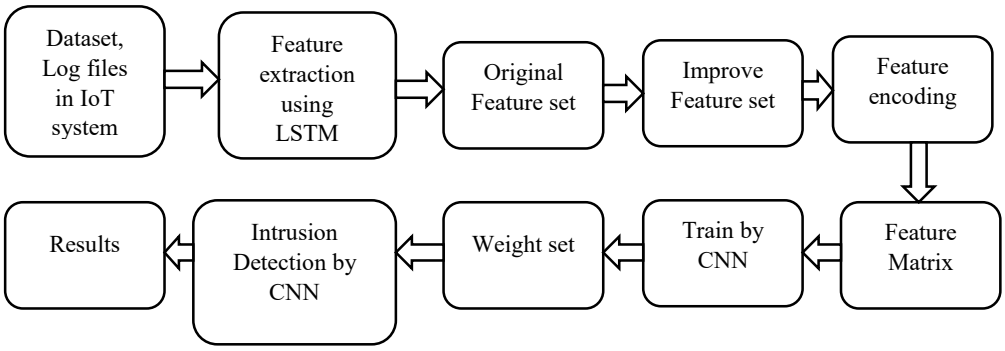

Fig. 5 Proposed Intrusion Detection System

In the training phase the data set and its log files are collected to extract the necessary features, and its compared with original feature set to improve the features of existing data using LSTM. Upon defining the label function, the selected data in trained using CNN. Based on the weight function obtained after CNN training process the intrusion is categorized as results.

4. Result and discussion

The proposed intrusion detection system is experimentally verified and compared with RNN based intrusion detection system. UNSW NB15 data set is used with validation ratio of 70% for training and 30% of test validation. Proposed system extracts the features from the dataset and identifies the attack and normal conditions. Proposed model is experimented using tensor flow installed on an Intel i5 processor 2.4GHz with 8GB of RAM. Table 2 depicts the details of samples used for experimentation.

Table 2. Samples used from the dataset

S.No	Class	Sample Size
1	Normal	240
2	Attack	3890

Evaluation metrics used to validate the proposed system are true positive, false positive, accuracy, precision, recall, f-score and error function. Table 2 depicts the average values of proposed model and RNN model based intrusion detection systems. It is observed from the values, proposed model attains better detection performance over RNN model. Few parameters such as recall and precision are similar to RNN however the ration of true positive and false positive is much better than RNN mode1.

Table 2. Performance metrics comparison

S.No	Parameter	RNN	Proposed HCNN
1	Precision	1	1
2	Recall	0.99	1
3	f-score	0.98	0.99
4	Miscalculation rate	0.041	0.032
5	Detection time (sec)	2.19	1.88
6	Accuracy (%)	95.7	98.6

ISSN: 2582-1369 (online)
Submitted: 29.08.2020
Accepted: 23.09.2020
Published: 30.09.2020

Journal of ISMAC (2020)
Vol.02/ No.04
Pages: 190-199
http://irojournals.com/iroismac/
DOI: https://doi.org/10.36548/jismac.2020.4.002

Detection accuracy of the proposed model is compared with RNN model and it is depicted in figure 6. It is observed from the figure, proposed Hybrid convolutional neural network model attains better efficiency of 98% which is 3% greater than conventional recurrent neural network model.

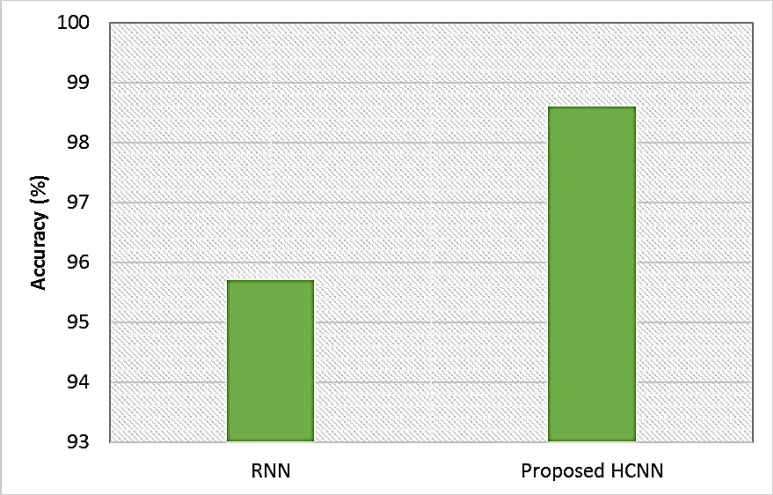

Fig. 6 Accuracy Comparison

5. Conclusion

Intrusion detection systems is an inevitable processing unit in recent wireless networks due to lack of security and increased number of intruders. IoT is a heterogeneous network which severely faces security threats similar to wireless networks and it is essential to develop an intrusion detection system to avoid performance degradation in IoT networks. Proposed research work analysis the different types of attacks in IoT and proposed a hybrid convolutional neural network module by incorporating long short term memory process. Proposed model is experimentally verified and compared with conventional recurrent neural network and attains better detection accuracy of 98% which makes the application suitable for different IoT environments.

References

1. Snehal Deshmukh-Bhosale, Santosh S. Sonavane (2019). A Real-Time Intrusion Detection System for Wormhole Attack in the RPL based Internet of Things. *Procedia Manufacturing*. 32:840-847.
2. Rup Kumar Deka, Dhruba Kumar Bhattacharyya, Jugal Kumar Kalita (2019). Active learning to detect DDoS attack using ranked features. *Computer Communications*. 145:209-222
3. Shailendra Rathore, Jong Hyuk Park (2018). Semi-supervised learning based distributed attack detection framework for IoT. *Applied Soft Computing*. 72:79-89.
4. Alekha Kumar Mishra, Asis Kumar Tripathy, Deepak Puthal, Laurence T. Yang (2019). Analytical Model for Sybil Attack Phases in Internet of Things. *IEEE Internet of Things Journal*. 6(1): 379-387.
5. Guangjie Han, Xun Li, Jinfang Jiang, Lei Shu, Jaime Lloret (2015). Intrusion Detection Algorithm Based on Neighbor Information Against Sinkhole Attack in Wireless Sensor Networks. *The Computer Journal*, 58(6): 1280-1292,
6. Yuxin Liu, Ming Ma, Xiao Liu, Neal N. Xiong, Anfeng Liu, Ying Zhu (2020). Design and Analysis of Probing Route to Defense Sink-Hole Attacks for Internet of Things Security. *IEEE Transactions on Network Science and Engineering.* 7(1): 356-372.
7. Bin Xu, Weike Wang, Qiang Hao,Zhun Zhang, Pei Du, Tongsheng Xia,Hongge Li, Xiang Wang (2018). A Security Design for the Detecting of Buffer Overflow Attacks in IoT Device. *IEEE Access*. 6: 72862-72869.
8. Chen Lyu, Xiaomei Zhang, Zhiqiang Liu, Chi-Hung Chi (2019). Selective Authentication Based Geographic Opportunistic Routing in Wireless Sensor Networks for Internet of Things Against DoS Attacks. *IEEE Access*. 7: 31068-31082.

ISSN: 2582-1369 (online)
Submitted: 29.08.2020
Accepted: 23.09.2020
Published: 30.09.2020

Journal of ISMAC (2020)
Vol.02/ No.04
Pages: 190-199
http://irojournals.com/iroismac/
DOI: https://doi.org/10.36548/jismac.2020.4.002

9. Mahmudul Hasan, Md. Milon Islam, Md Ishrak Islam Zarif, M. M. A. Hashem (2019). Attack and anomaly detection in IoT sensors in IoT sites using machine learning approaches. *Internet of Things*. 7: 1-16.
10. Ju Ren, Yaoxue Zhang, Kuan Zhang, Xuemin Shen (2016). Adaptive and Channel-Aware Detection of Selective Forwarding Attacks in Wireless Sensor Networks. *IEEE Transactions on Wireless Communications.* 15(5): 3718-3731.
11. Noshina Tariq, Muhammad Asim, Zakaria Maamar, M. Zubair Farooqi, Thar Baker (2019). A Mobile Code-driven Trust Mechanism for detecting internal attacks in sensor node-powered IoT. *Journal of Parallel and Distributed Computing.*134:198-206.
12. Thi Ngoc Diep Pham, Chai Kiat Yeo, Naoto Yanai, Toru Fujiwara (2018). Detecting Flooding Attack and Accommodating Burst Traffic in Delay-Tolerant Networks. *IEEE Transactions on Vehicular Technology.* 67 (1): 795-808.
13. Bo Chen, Daniel W. C. Ho, Guoqiang Hu, Li Yu(2018). Secure Fusion Estimation for Bandwidth Constrained Cyber-Physical Systems Under Replay Attacks. IEEE Transactions on Cybernetics. 48(6): 1862-1876
14. Olivier Brun, Yonghua Yin, Erol Gelenbe (2018). Deep Learning with Dense Random Neural Network for Detecting Attacks against IoT-connected Home Environments. *Procedia Computer Science*. 134:458-463.
15. Haythem A. Bany Salameh, Sufyan Almajali, Moussa Ayyash, Hany Elgala (2018). Spectrum Assignment in Cognitive Radio Networks for Internet-of-Things Delay-Sensitive Applications Under Jamming Attacks. IEEE Internet of Things Journal. 5(3): 1904-1913

ISSN: 2582-1369 (online)
Submitted: 29.08.2020
Accepted: 23.09.2020
Published: 30.09.2020