International Research Journal of Multidisciplinary Scope (IRJMS), 2024; 5(1):36-41

Original Article | ISSN (O): 2582-631X DOI: 10.47857/irjms.2024.v05i01.0130

Abnormal and Maltreatment Intrusion Detection in Big and Small Data Storage Blue Brain Network

Rajesh D[1*], Giji Kiruba D[2], Ramesh D[3]

[1]Department of CSE, Vel Tech Rangarajan Dr.Sagunthala R&D Institute of Science and Technology, Chennai, India. [2]Department of EEE, Satyam College of Engineering and Technology, Nagercoil, India. [3]Anna University, Chennai, India. *Corresponding Author's Email: rajeshd936@gmail.com

Abstract

In modern network environment users facing several network attacks that creates harm to entire network environment. An efficient intrusion recognition approaches is obligatory to diminish such harm and to defend the reliability and accessibility of network environment. In this research work a novel approach for intrusion recognition in network environment depends on awareness method that discover by propagating Intrusion Detection System information to several layers. To enhance accurateness of intrusion recognition high dimensional data characteristic depiction is applied in IoT network. For illustration public data set KDD-Cup 99 is utilized. The outcomes demonstrate that the Maltreatment Intrusion Detection in Big and Small Data Storage (M-BSDS) can efficiently identify irregular malicious activities in IoT network environment, enhanced recognition accurateness and diminish fake optimistic rate evaluated with established intrusion detection approaches.

Keywords: Abnormal detection, deep learning, maltreatment detection, Blue Brain, Intrusion Detection.

Introduction

Rapid improvement on cloud computing cyber attacks is challenging issues that intimidate IoT security environment (1). Interruption recognition is a positive security solution that offers real-time safety against inside and outer threats, as well as misbehaviour. It can protect before misbehaviour arises, successfully defensive without any failure (2). Real time recognition of any attacks in IoT environment is complex (3). In the past several approaches about conventional machine learning (ML) have been established for intrusion recognition. In (4, 5) already some achieved outcomes, but still it is not acceptable. Established approaches cannot successfully solve huge intrusion problem in the real environment (6) In (7) Deep Neural Network (DNN) precedent regular encoder framework it accomplishes better outcome than existing but Long short-term memory (LSTM) exposed outstanding results. In (8) applies LSTM to accomplish better outcomes not successfully identify malicious activity. In this research work identify attacks by utilizing M-BSDS method of Multi-directional precedent large storage and watching method to record malicious activities and behavior calculation. Although the data contained in this document is not regarded for future applications, it may be utilized to detect assaults periodically. Prior network activity status information can be utilized to comprehend the present condition of the network as well. To capture attribute traits that significantly influence predicting of malevolent behavior, we thus include attention processes and use Maltreatment Intrusion Detection in Big and Small Data Storage using Blue brain Network. Blue brain that stores the previous complete details about the storage and network activities. Here M-BSDS model and basic techniques to gather attribute information that significantly affects the prediction of malicious behavior in order to enhance the aforementioned issues. The primary contributions to this research are as follows:

(Received 14th October 2023; Accepted 01st January 2024; Published 30th January 2024)

(i) Examine the existing machine learning-based network intrusion prevention technique.

(ii) A novel attention-based detection of network breaches approach that outperforms the LSTM method in speeding up the categorization process while capturing significant data that is helpful for classifying. Additionally, the model increases the accuracy of malicious activity identification.

Here dataset KDDCup99 classification is utilized and evaluated with proposed approach.

KDDCup 99

Public information (KDDCup 99, NSL-KDD, etc.) are extensively used in malware detection to test the efficacy of well-known neural network models genetic algorithms (9). The KDDCup 99 dataset is a 5 million sample points simulation software platform with a 10% simulation and experimental subset (10). Table 1 shows a model of an allocation table.

There are 41 characteristic tags and one grouping tag in each field of the data set. Tags for grouping can be classified as regular or irregular. DoS (denial-of-service attack), MiM (man-in-the-middle), R2L (illegal entry from remote hosts), U2R (illegal local super user confidential entry), and PROBING are the five types of attacks (port scanning). The abnormality was divided into 39 various threats, 22 of which have been identified in the training sample and seventeen of which were unidentified in the validation set.

Data Preprocessing

In this replica input will be based on digital vector so convert the original information into numeric data. In every information packet change the protocol, service, connection condition, and category of attack to digitalized IDs by encoding. Here protocol category is a discrete as TCP, UDP, and ICMP it contains three bits as 1 0 0, 0 1 0 and 0 0 1. Normalization technique to eradicate the dimensional manipulation among characteristic data desires to be stabilized to determine the comparability among characteristic pointers. When the original information is stabilized, the pointers are in the identical category level, so optimization procedure is best solution. In this approach a min-max normalization technique is utilized to modify the original data to characteristic data as 0 and 1. The exchange procedure as,

$$n' = \frac{(o-min)}{(max-min)} \quad [1]$$

where n' symbolize the normalized cost, o symbolize the cost of original characteristic, and min and max symbolize the characteristic of original data set with minimum and maximum costs.

Maltreatment Intrusion Detection in Big and Small Data Storage (M-BSDS)

In M-BSDS contains five layer parts input, output, embedded, M-BSDS, watching represented in Figure 1.

Embedded Layer

Every cycle in the dataset has a collection of characteristic series, each of which is represented by a vector v_i. For input series **S =** { v_1, v_2, v_3, …, v_n }, Thus obtains an entrenched matrix M = {m_1, m_2, …, m_n}. Every characteristic entry in record follows an eigenvector as,

$$m_i = ReLu(W_e v_i + be) \quad [2]$$

where, weight of matrix is $W_e \in R^{d\times 1}$, matrix offset is $b_e \in R^d$, and d is measurements of embedded matrix. The produced characteristic vector M is subsequently approved on to the subsequently level as a parameter.

Though Recurrent Neural Network (RNN) may theoretically resolve training data, it suffers from the same gradient vanishing problem as Deep Neural Network (DNN). This drawback is very risky while sequence of information is huge. Consequently the exceeding RNN representation is normally not straightforwardly appropriate to the application area. To overcome the gradient vanishing problem in recurrent neural networks, LSTM uses a gateway technique to manage the number of prior recordings kept by every LSTM component and to remember the current input, preserve significant characteristics, and reject insignificant ones. Figure 2 depicts the LSTM component model.

Table 1: KDDCup 99 Data Set Sample Categories

	Totality	Regular	PROB	DOS	U2R	R2L	MiTM
Train Set	594321	99278	5107	491658	72	1426	1567
Test Set	411329	62593	5166	330053	428	19189	5781

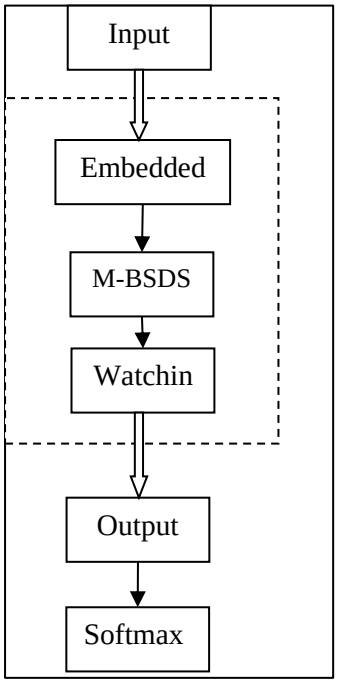

Figure 1: M-BSDS with watching model

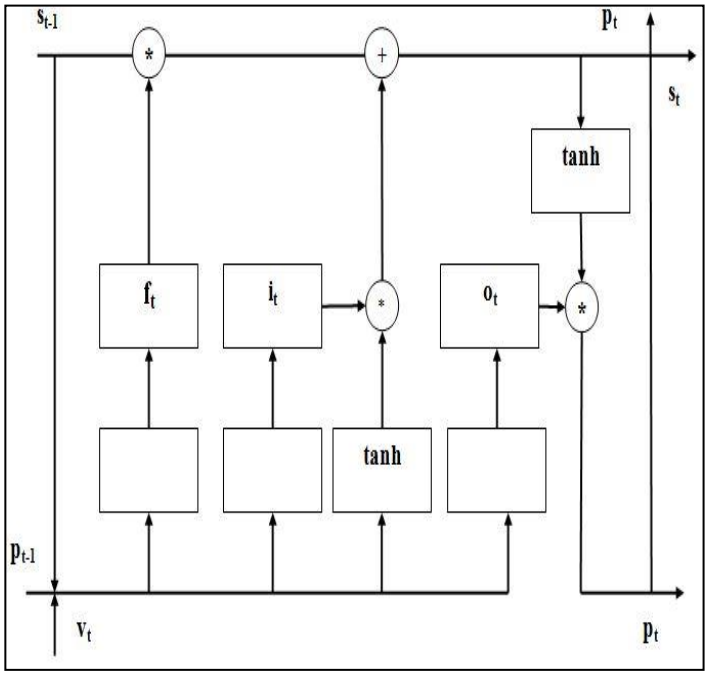

Figure 2: Model of LSTM component

Table 2: Uncertainty matrix

Real Guessing	Regular	Irregular
Regular	NP	AP
Irregular	AN	NN

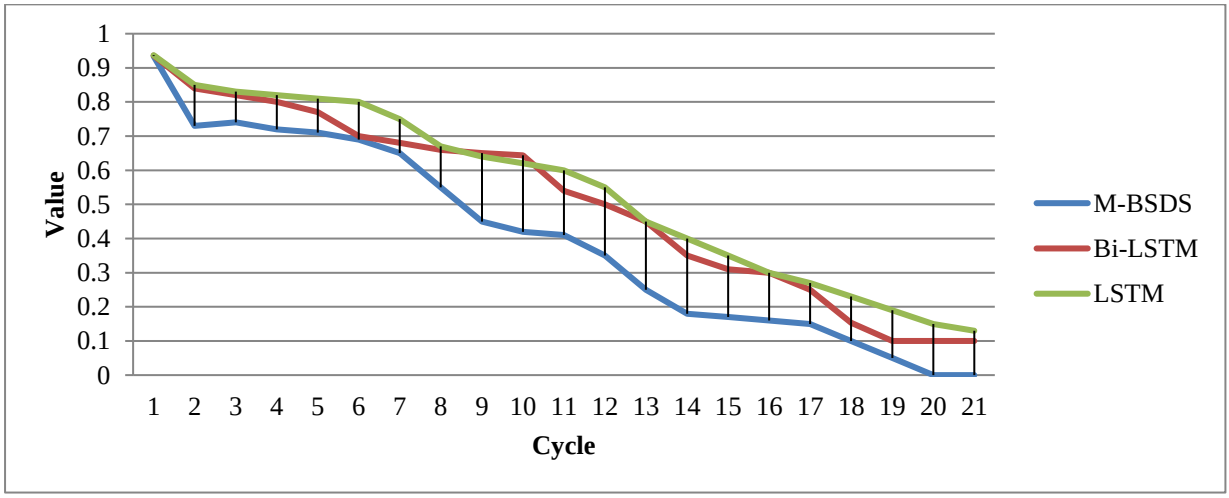

Figure 3: Loss Graph of M-BSDS using watching Approach

LSTM component contains three gates which manages recent network congested information and status in storage component. The execution of entire gates by present input v_t and output cost p_{t-1} of LSTM component at the preceding instant, it is executed by cost of storage component s_{t-1}.

The result of input gate is calculated as,

$$i_i = \sigma(W_{vi}v_t + W_{pi}p_{t-1} + W_{si}ps_{t-1} + b_i \quad [3]$$

Elapsed gate estimated as,

$$f_t = \sigma(W_{vf}v_t + W_{pf}p_{t-1} + W_{sf}s_{t-1} + b_f) \quad [4]$$

Component state information updating is calculated as,

$$s_t = f_t\, s_{t-1} + i_t \tanh(W_{vc}v_t + W_{pc}p_{t-1} + W_{sc}s_{t-1} + b_c) \quad [5]$$

Output gate estimated as,

$$o_t = \sigma(W_{vo}v_t + W_{po}p_{t-1} + W_{so}s_{t-1} + b_o) \quad [6]$$

$$p_t = o_t \tanh(s_t) \quad [7]$$

where, W signifies the weight matrix and t signifies time of input, Elapsed, Component state and Output gate as W_{pi}, W_{pf}, W_{pc} and W_{po}, i_t, f_t, s_t and o_t, finally σ is sigmoid factor.

For series representation, upcoming and precedent information at every instant are significant. The regular LSTM method does not obtain upcoming information. So utilize a multi way LSTM which combines multi LSTMs and distributes the similar layers in input and output. Consequently trained information can be associated with precedent and upcoming information. Then apply output vector of final series as characteristic vector, and at last execute Softmax categorization. The cost of every time sequence is analysed, afterward the complete weight is added as a characteristic vector, and finally Softmax categorization is performed.

In network intrusion recognition watching method is most significant feature. The goal of the observing approach is to determine the involvement of their hidden terminal in categorising the outcome by comparing hidden terminal weights from different time periods. To obtain entire reports from earlier hidden terminals watching method to obtain the association among $ht_1, ht_2, ..., ht_n$ and at last achieves the end vector pair demonstration for categorization as,

$$\alpha = \text{softmax}(V^T[ht_1, ht_2, ..., ht_n]) \quad [8]$$

$$ht^* = \tanh(H\alpha^T) \quad [9]$$

where, V^T is a factor inversion of a vector achieved by training and learning.

intrusion recognition, particularly in authoritarian environments, the acceptance of

In M-BSDS model Softmax classifier is to foresee the categorization symbol as s^, ht* input from hidden terminal as,

$$P = \text{softmax}(V_s ht^* + b_s) \quad [10]$$

$$s^\wedge = \text{argmax}(l) \quad [11]$$

where, V_s and b_s are constraint that require to learned.

In M-BSDS loss function can be calculated from cross entropy as,

$$L_f = -1/N_s(\Sigma^N{}_{i=1} s_i \log(l_i) + (1-s_i)\log(1-l_i)) \quad [12]$$

Where, N_s symbolize the amount of samples and l_i indicates possibility of i^{th} sample is foresee to be malevolent.

Performance Measure

Performance Measure of M-BSDS is evaluated by accuracy rate (AR) of intrusion recognition. Along with AR evaluating recall rate(RR) and false indicator rate(FIR). Normal Positive (NP) condition specifies the amount of samples guessed as regular by methodology in regular flow. Abnormal Positive (AP) condition specifies the amount of samples guessed as regular by methodology in irregular flow. Abnormal Negative (AN) condition specifies the amount of samples guessed as irregular by methodology in regular flow. Normal Negative (NN) condition specifies the amount of samples guessed as irregular by methodology in irregular flow. Table 2 shows uncertainty matrix of M-BSDS.

AR foretells the accurate amount of samples as a proportion of the entire samples as,

$$AR = (NP+AN)/(NP+AP+AN+NN) \quad [13]$$

The quantity of right trial in regular stream as a proportion of all trial in regular stream is predicted by RR,

$$RR = NP/(NP+AN) \quad [14]$$

The quantity of fault trial in irregular stream as a proportion of totality trial in irregular stream is predicted by FIR,

$$FIR = AP/(AP+NN) \quad [15]$$

From the perception of the classification accurateness and recognition rate is conflicting pointer. Huge accurateness contains less abnormal positive but high recognition rates contains less abnormal positive. For illustration, if extra distrustful attacks are categorized as attacks the recognition rate enhances, but accurateness will diminish. As a result, a single high detection rate or precision is worthless. From outlook of intrusion is extremely small, so RR is also a significant pointer to consider.

Results and Discussions

To improve training outcomes of neural network representation M-BSDS approach applies factors to achieve. Factors cost and concern them to M-BSDS with watching approach. The factors are learning cost as 0.001, 15 hidden terminals, duration 200s, and environmental nodes as 600. In M-BSDS KDD-Cup99 data is utilized that is most accepted standard data group for cyber attack recognition. LSTM and M-BSDS approaches executed in Tensorfolw 1.4.0 utilizing Python 3.5. In comparison to many traditional machine learning classifiers as Logistic Regression (LR), Naïve Bayes (NB), K-Nearest Neighbors (KNN), and Support Vector Machines (SVM) for research outcomes. Table 3 shows the results, which show that the representation was well-trained and achieved increased accuracy. Accurateness and Finite impulse response, LSTM is enhanced than conventional machine learning classifier, and M-BSDS with watching approach is enhanced than LSTM method. M-BSDS with watching approach focused on significant characteristics and diminish the feeble characteristics that affect recognition rate.

Table3: Comparison of existing experimentation outcomes

Classifier	Accuracy Rate (AR)	Recall Rate(RR)	False Indicator Rate(FIR)
M-BSDS	0.9901	0.9491	0.0329
Bi-LSTM + Attention	0.9836	0.9379	0.0352
LSTM	0.9672	0.9239	0.0627
KNN	0.9274	0.9049	0.0821
SVM	0.9012	0.8618	0.0772
NB	0.8727	0.8471	0.0986
LR	0.8306	0.8332	0.1315

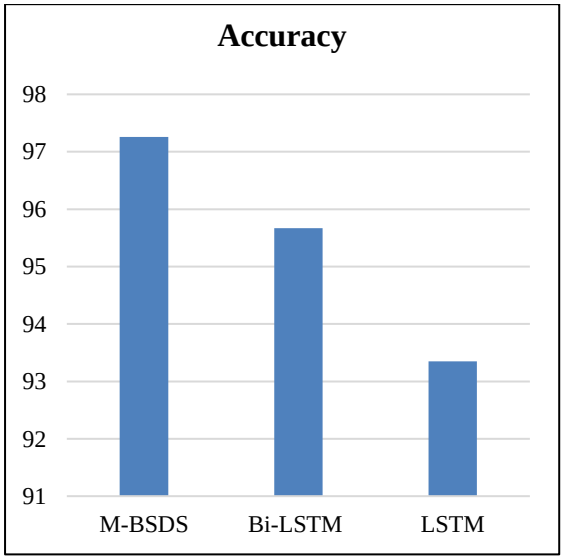

Figure 4: Accuracy comparison

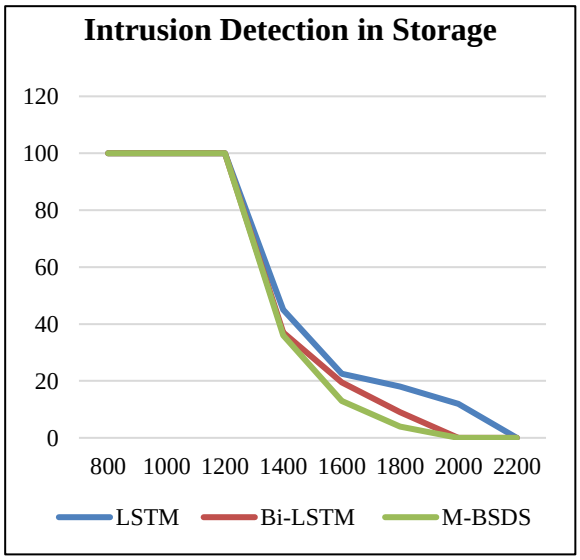

Figure 5: Intrusion Detection in Storage using Blue brain Network

Figure 3 evaluates LSTM with M-BSDS based watching approach in that experimentation process 22 cycles, representing that the approach can terminate training at a prior phases and training process is rapid. From outcome M-BSDS with watching approach contains higher accurateness and rapid processing so it archives enhanced intrusion recognition.

The accuracy level of M-BSDS is enhanced when compared with the existing methodologies. The accuracy level is high it can able to detect the intrusion in storage. In figure 4 shows the accuracy level proposed and existing methodologies.

The intrusion detection in storage in blue brain technology is enhanced when compared with the existing methodologies. The figure 5 shows that Intrusion reorganization in Storage by applying Blue brain Network. The Blue brain technology is more efficient in detection of malicious in storage.

Conclusion

A novel M-BSDS approach for intrusion recognition in network environment depends on awareness method that discover by propagating Intrusion Detection System information to several layers. To enhance accurateness of intrusion recognition high dimensional data characteristic depiction is applied in IoT network. M-BSDS with watching based on Neural Network intrusion recognition approach contains an instance distinctive that can broadly examine the investigation of network congestion. The proposed methodology is to create a precise and adaptable identification system that raises the intrusion detection probability while reducing the amount of false detection applying blue brain technology. The experimentation outcome demonstrates that proposed methodology has enhanced outcomes than LSTM. In future the Maltreatment Intrusion Detection in Big and Small Data Storage can be implemented in retacton networks.

Abbreviations

Nil

Acknowledgement

Nil

Author contribution

All Authors contributed entire manuscript in writing, reviewing, implementing, Conceptual-ization and Analysis.

Conflict of interest

The authors declare no conflict of interest.

Ethics approval

The research does not involve human participants.

Funding

No

References

1. Rajesh D, Giji Kiruba D, Ramesh D. Energy Proficient Secure Clustered Protocol in Mobile Wireless Sensor Network Utilizing Blue Brain Technology. Indian Journal of Information Sources and Services. 2023; 13(2): 30–38.
2. Rajesh D, Rajanna GS. CSCRT protocol with energy efficient secured CH clustering for smart dust network using quantum key distribution. International Journal of Safety and Security Engineering. 2022; 12(4): 441-448.
3. Sultana N, Chilamkurti N, Peng W, Alhadad R. Survey on SDN based network intrusion detection system using machine learning approaches. Peer-to-Peer Networking and Applications, 2018; 1(2): 1–9.
4. Rajesh D. Energy-Resourceful Routing by Fuzzy Based Secured CH Clustering for Smart Dust. International Journal of Electrical and Electronics Research (IJEER). 2022; 10(3): 659-663.
5. Devan, P, Khare N. An efficient XGBoost–DNN-based classification model for network intrusion detection system. Neural Comput. & Applic. 2020; 32(16): 12499–12514.
6. Singh CE, S. M. Vigila SMC. Woa-dnn for intelligent intrusion detection and classification in manet services. Intelligent Automation & Soft Computing. 2023; 35(2): 1737–1751.
7. Vinayakumar R, Alazab M, Soman K. P, Poornachandran P. A. Al-Nemrat and S. Venkatraman. Deep Learning Approach for Intelligent Intrusion Detection System, in *IEEE Access*. 2019; 7(1): 41525-41550.
8. Preethi D, Khare N. EFS-LSTM (Ensemble-Based Feature Selection with LSTM) Classifier for Intrusion Detection System. International Journal of e-Collaboration (IJeC). 2020; 16(4): 72-86.
9. Edwin Singh C, Maria Celestin Vigila S. Fuzzy based intrusion detection system in MANET. Measurement: Sensors, 2023; 26(1): 100578.
10. Staudemeyer RC. KDD Cup 1999 Data, 2018. [Online]. Available: https://kdd.ics.uci.edu/databases/kddcup99/kddcup99.html.