IOT INTRUSION DETECTION USING BI-DIRECTIONAL LSTM RNNs: A DEEP LEARNING APPROACH

K Pavani[1], Keerthi Mani Purna Chandrika[2], Kamatham Kusuma[3], Nivani Chandini[4], Matcha Sai Sowmya Sree[5]
[1,2,3,4,5]Department of Computer Science and Engineering, Vignan's Institute of Engineering for Women, Visakhapatnam, Andhra Pradesh, India

ABSTRACT
The Internet of Things facilitates the connection between various objects and the Internet, there by enabling communication between these objects. The IoT is composed of interconnected devices with varying complexity and trends. This inherent nature of the IoT structure increases the number of potential targets for attacks, which may have a negative impact on the sustainable growth of the IoT. Consequently, addressing security concerns becomes a matter of great importance. In this study, a novel deep learning approach is proposed for the real-time detection of security threats in IoT systems. This approach utilizes the Bi-directional Long Short-Term Memory Recurrent Neural Network (BLSTM RNN). The UNSW-NB15 dataset, which contains sequential samples and contemporary attack patterns, is utilized for training and testing the proposed approach. This work employs a binary classification technique to differentiate between attack and normal patterns. The experimental results demonstrate the effectiveness of the introduced model in terms of recall, precision, FAR, and f-1 score. The model achieves a detection accuracy ofover93%.Thetest results indicate that BLSTM RNN is highly efficient in constructing a highly effective model for intrusion detection and presents a unique research methodology.
Keywords: Bi-directional Recurrent Neural Network, Deep Learning, Intrusion Detection, IoT.

INTRODUCTION
Since the 1960s, the Internet has revolutionized communication, breaking down geographical barriers andfacilitatingcollaboration.TheemergenceoftheInternetofThings(IoT)signifies aneweraofconnectivity,whereintelligentobjectsgatherandexchangedata.CoinedbyKevin Ashton in 1999, IoT comprises globally identifiable devices equipped with sensors and intelligent capabilities. It represents a convergence of the Internet and physical objects, enabling remote health monitoring, improved government services, enhanced enterprise operations, and streamlined daily life. For instance, IoT enables remote health monitoring, exemplifiedbyminiaturecomputingdevicesdevelopedbytheUniversityofEdinburgh,which attachtothehumanchesttomonitorrespiratoryinformation.Governmentsworldwideleverage IoTto gather data and provide improved facilities in areas like security, health, development, and transportation. Enterprises utilize IoT to enhance customer service, employee safety, and security. The expansion of IoT is rapid, with projections indicating approximately 75 billion connected devices by 2025, according to Gartner. These interconnected devices enhance everyday activities and foster the development of smart solutions. However, the significant potential and conveniences offered by IoT also raise security concerns. As IoT networks expand, so do the vulnerabilities, necessitating robust security measures to safeguard against potential threats. In summary, IoT represents a transformative force in modern society, revolutionizingcommunication,connectivity,andeverydaylife.Whileofferingunprecedented benefits, it also demands vigilant attention to security to mitigate potential risks in our increasingly interconnected world.

LITERATURESURVEY

"Cloud Base Intrusion Detection System using Convolutional and Supervised Machine Learning" (2023) by Aditya Kumar Shukla, Ashish Sharma [1]: The study examines convolutionaldeeplearning,supervisedmethods,andahybridapproachforintrusiondetection using CNN, SVM, and KNN models. The rise in popularity of cloud computing is driven by its pay-per-use services. However, cloud computing faces security challenges. Security solutions are essential for enhancing cloud security for both providers and users. Network security is crucial in the rapidly advancing technology landscape. Intrusion detection systems playakeyroleinpreventingunauthorizednetworkresourceuse.Theresearchdelvesintodeep learning and supervised methods for intrusion detection.

"Intrusion Detection System using Long Short-Term Memory and Fully Connected Neural Network on Kddcup99 and NSL-KDD Dataset" (2023) by Shiv Shakti Shrivastava andAnkit Chakrawarti [2]: This paper examines intrusion detection using LSTM and FCNN on the KDDCup99 and NSL-KDD datasets for cyber threat analysis. A deep learning approach is developed for the correct categorization of network connections. Traditional approaches strugglewithhugedatasets.DeeplearningmethodssuchasLSTMandFCNNtrytocategorise connections in incursion datasets. The suggested model performs well on both datasets. The proposed deep learning model shows high accuracy on KDDCup99 (99.99%) and NSL-KDD (99.95%) datasets, providing maximum output.

"DesignandDevelopmentofRNN-basedAnomalyDetectionModelforIoTNetworks"(2022) by Imtiaz Ullah and Qusay H. Mahmoud [3]: The research examines deep learning-based anomaly detection for IoT network cybersecurity using CNNs and RNNs. Various IoT cybersecurity datasets are used to test these models for binary and multiclass classification. With the growth of IoT, cybersecurity gains significance, especially in IDS where deep learning,includingRNNsandCNNs,aidsindetectingmalicioustraffic.Theproposedmodels outperformcurrentimplementationsinaccuracy,precision,recall,andF1scoreacrossdatasets. "An Enhanced Intrusion Detection System for IoT Networks Based on Deep Learning and Knowledge Graph" (2022) by Xiuzhang Yang and Guojun Peng [4]: The author offers an enhanced IDS for IoT networks based on deep learning and knowledge graphs. The system improvesaccuracyandrobustnessbycombiningseveralviewsoffeatures,extractingsemantic relationships, and detecting attacks in real time. The attention-based CNN-BiLSTM model outperforms prior systems, with a detection accuracy of 90.01%. The model detects several sorts of stealthy attacks by adding semantic connections and essential characteristics from knowledge graphs, as well as multiview feature fusion. Experimental findings show that resilience, feature selection, and accuracy outperform state-of-the-art systems.

"Using Deep Learning Technique to Protect Internet Network from Intrusion in IoT Environment" (2022) by Ashwaq Fahhad Almutairi, Asma Abdulghani Alshargabi[5]: The article presents an RNN-based intrusion detection model for IoT that achieves 87% accuracy on the NSL-KDD dataset. Securing IoT settings is critical given the fast expansion of IoT, whichisexpectedtolinkover20billiondevicesby2024.Whilenumerousintrusiondetection systems exist, their accuracy and effectiveness differ. The suggested RNN model shows potential, and future work will include additional optimisation with methods to improve detection accuracy.

EXISTINGSYSTEM

ExistingIoTIntrusionDetectionSystemsUsingBi-DirectionalLSTMRNNstakeavarietyof techniques. Anomaly Detection from Sensor Data uses sensor data to establish regular behaviour patterns and identify deviations as probable intrusions, necessitating powerful featureextractionalgorithms.LSTM-basedIntrusionDetectionusesLSTMnetworkstorecord temporalrelationshipsinnetworkdata,allowingforreal-timedetectionofcomplexattack patterns and improved cybersecurity. Three-Layer RNN architecture, with three recurrent layers, analyses sequential data such as time series or text while retaining recollection of previousinformation,potentiallyboostingintrusiondetection.RNN-basedintrusiondetection, whichusesRNNssuchasLSTM,showspotentialincapturingtemporaldependenciesbutmay struggle with high-dimensional characteristics, necessitating more refining for successful detection in IoT contexts.

PROPOSEDSCHEME

Our proposed system uses Bi-LSTM RNNs to detect intrusions by capturing temporal dependencies. Network data is preprocessed to extract features for Bi-LSTM input. The bidirectionalBi-LSTMlearnsfrompastandfuturedatatoidentifyintrusionpatterns.Training involves distinguishing normal behavior from anomalies using backpropagation. Validation and testing ensure model robustness. Deployed model monitors traffic for intrusions in real-time. Proactive approach allows for timely response to security threats and adaptation to new attack methods. Periodic updates maintain system vigilance against emerging threats, enhancing network security.

Pre-processingdataforIntrusionDetectionusingBLSTMwithUNSW-NB15datasetinvolves TensorFlow tools for data preprocessing. Python libraries like panda and NumPy are used for data manipulation and numerical computing. These tools help in preparing data for analysis andmachinelearning.Thetrainingsetincludes9typesofattacks,butonly5typesrelevantto IoT attacks are extracted. The training set has a total of 45 features, but only 5 features are consideredforreducingoverfittingandimprovingaccuracy.Theresultingtraining-setconsists of 5 attack types, 5 features, and two class labels. Table below show the structure and format of the resulting dataset, with specific values indicating normal and attack samples.

service	sbytes	sttl	smean	ct_dst_ sport_ ltm	attack_cat	label
dns	264	60	132	3	Normal	0
Smtp	3563	62	162	1	Dos	1
-	156	254	78	1	Backdoor	1
http	1246	254	89	1	Reconnaissance	1
-	200	254	100	6	Analysis	1
http	1988	254	52	1	worms	1

Table1:Data-setstructureafterextractingthefeatures

In the training phase we used the reduced training dataset. However, before training we split the dataset into two subsets: training dataset and validation dataset. The split ratio is 67% for training & 33% for validation. The training dataset is used to update the model’s parameters duringtraining,whilethevalidationdatasetisusedtoupdatethemodel’sparametersaftereach epoch. This evaluation helps us monitor how well the model generalizes to unseen data and detect any overfitting or underfitting issues. Then we analyze the model’s performance and iterativelytuneitsparameterstoimproveitsperformanceuntilsatisfactoryresultsareobtained. In the testing phase we load the reduced testing dataset and feed it to our trained model. This meansweletthemodelanalyzeeach exampleofnetworkactivityinthetestdatasetandmake predictions about whether each activity is normal or suspicious.

DESIGNSTRUCTURE

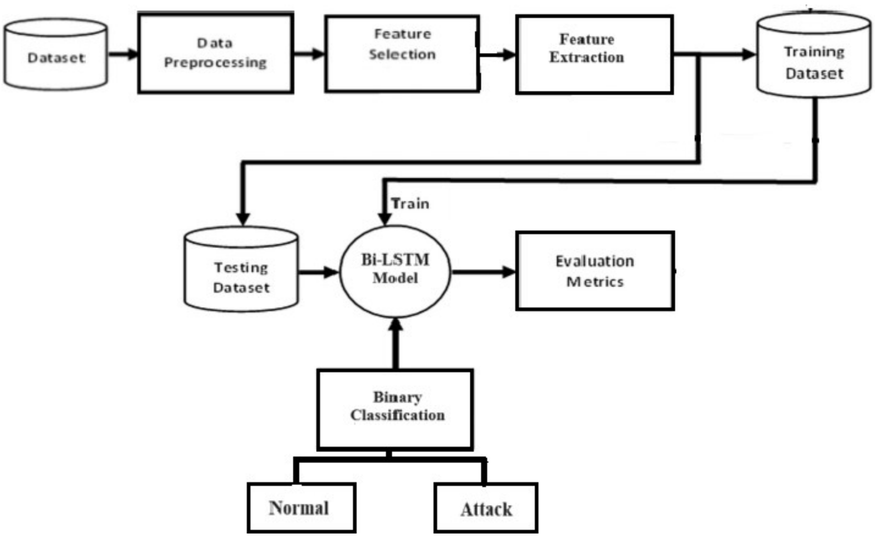

Fig1: SystemArchitecture

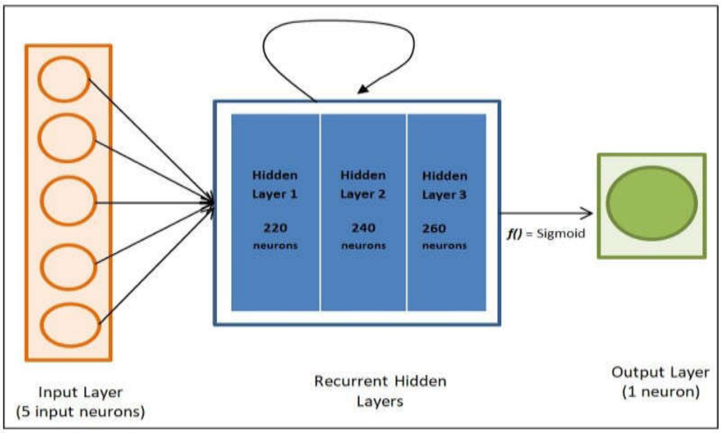

Fig2:Bi-LSTMmodel

RESULTANALYSIS

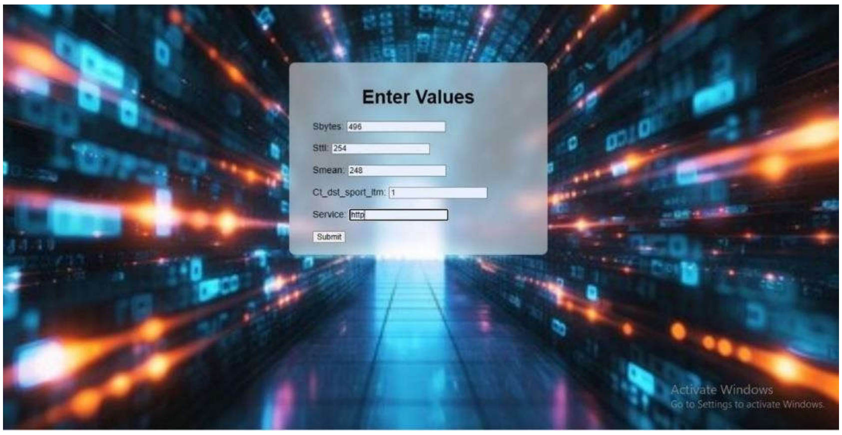

Fig3:TestcasevaluesforNormal

Fig4:TestcaseResultforNormal

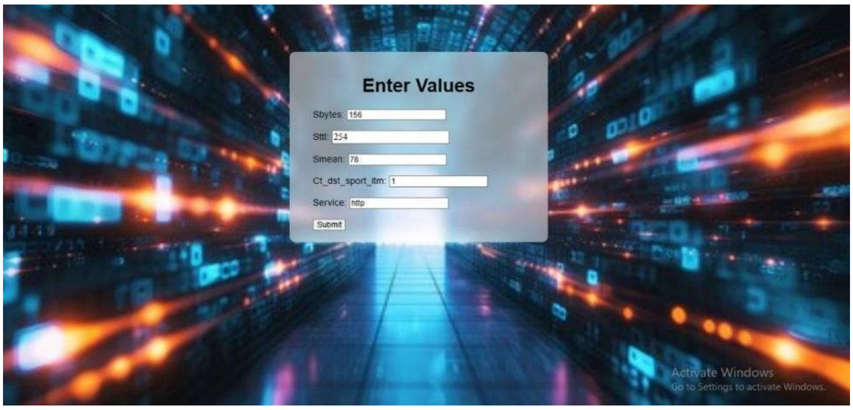

Fig5:TestcasevaluesforAttack

Fig6:TestcaseResultforAttack

EVALUATION

PerformanceMeasure	Percentage
Accuracy	0.93
Precision	0.98
Recall	0.93
f1-score	0.95
Miscalculationrate	0.06
FAR	0.0

Table2:ReportedAccuracy,Precision,Recallandf1-scoreoftheproposedclassifier including FAR

CONCLUSION

The project aimed to identify intrusions in IoT networks using Deep Learning with BLSTM RNNandTensorFlow.DeepLearningeffectivelyaddressedsecurityissuesinIoTnetworksby detecting various types of attacks. The model showed high accuracy in intrusion detection, including FAR evaluation. Future work involves using larger datasets to improve model generalizationanddeployingitforreal-timethreatdetection.Integratingthreatintelligencecan enhance the model's ability to detect emerging threats. Continuous model updating is crucial against evolving cyber threats, and promising advancements in network security. The project also suggests future research directions in network security, emphasizing the importance of threat intelligence integration and IDS deployment on edge devices. Overall, the project contributes to the field of network security and intrusion detection.

REFERENCES

[1] "Cloud Base Intrusion Detection System using Convolutional and Supervised Machine Learning"(2023) by Aditya Kumar Shukla, Ashish Sharma

[2] "IntrusionDetectionSystemusingLongShort-TermMemoryandFullyConnectedNeural Network on Kddcup99 and NSL-KDD Dataset"(2023) by Shiv Shakti Shrivastava andAnkit Chakrawarti

[3] "Design and Development of RNN-basedAnomaly Detection Model for IoT Networks" (2022) by Imtiaz Ullah and Qusay H. Mahmoud

[4] "AnEnhancedIntrusionDetectionSystemfor IoTNetworksBasedon DeepLearningand Knowledge Graph"(2022) by Xiuzhang Yang and Guojun Peng

[5] "Using Deep Learning Technique to Protect Internet Network from Intrusion in IoT Environment"(2022) by Ashwaq Fahhad Almutairi, Asma Abdulghani Alshargabi

[6] "IntrusionDetectionin IoTUsing DeepLearning"(2022) byAlaaMohammed Banaamah

[7] "Deep Learning-BasedIntrusionDetectionSystems:ASystematicReview" (2021)by Jan Lansky and Saqib Ali

[8] "IntrusiondetectionsystemsforIoT-basedsmartenvironments:asurvey"(2018)by Mohamed Faisal Elrawy and Ali Ismail Awad

[9] "Attack ClassificationAnalysis of IoT Network via Deep Learning Approach"(2017) by Bayu Adhi Tama and Kyung Hyune Rhee

[10] "DataMiningand IntrusionDetection Systems"(2016)byZibusiso Dewaand Leandros