JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

INTELLIGENT MULTI-CHANNEL THREAT DETECTION FOR ENHANCED DATA SECURITY USING DEEP LEARNING

HRUTHKARSHA D S[1], DIVYA B S[2], CHAITRA D[3], ARPITHA R[4], Dr. PRAVEEN KUMAR K V[5]

Department of Computer Science and Engineering, Sapthagiri college of Engineering

#14/5, Chikkasandra, Hessarghatta main road, Bangalore-57, Karnataka, India

Abstract **-- The arrival of deep literacy ways, similar to Convolutional Neural Networks(CNNs) and intermittent Neural Networks(RNNs), has revolutionized colorful disciplines, including image processing and natural language understanding. Despite their remarkable success in these fields, their operation to information security, specifically attack discovery, remains limited. In this design we propose an innovative approach to enhance information security through intelligent attack discovery. We work Long Short-Term Memory- Transformer(LSTM-Transformer) and introduce a comprehensive frame that seamlessly integrates data preprocessing, feature abstraction, and multi-channel training. Our system initiates with rigorous data preprocessing to ensure the quality of input data. latterly, different features are strictly uprooted from the reused data, landing both subtle and overt patterns associated with attacks. A core element of our approach is multi-channel training, wherein neural networks are trained with distinct point sets. This holistic approach effectively retains the nuances of attack characteristics within input vectors, easing precise isolation between normal and vicious conditioning. To make robust opinions regarding the attack events, we employ a decision emulsion medium that summates the labors of multiple classifiers and also introduce a voting algorithm to decide whether the input data is attacked or not. This agreement-grounded approach significantly enhances the delicacy and trustability of attack discovery. Experimental evaluations demonstrate the superiority of our approach over conventional styles employing point discovery and traditional classifiers, similar as Bayesian or Support Vector Machines(SVMs).**

Keywords**—Attack detection, LSTM-Transformer, multi-channel training, robust decisions, voting algorithm, Support Vector Machine(SVM), Convolutional Neural Networks(CNNs), Deep Learning.**

I INTRODUCTION

The discovery of network attacks has sparked increased interest in social networking information security recently due to the addition of security risks like clickjacking, DDOS, identity theft, cross-site scripting, and inquiry. Distinguishing hostile conditioning from network business is the final step in the discovery of a network attack. In order to respond to novel or modified attacks, the discovery needs to be handled cleverly and successfully. Conventional attack discovery essay models all types of attacks or anomalies and describes them based on the available information. However, in the past, new attack types have caused significant harm before being discovered. It is difficult to model every type of attack and identify attacks before they cause significant harm, especially when new attacks emerge over time. To triumph over hours have been spent modeling the attack or anomaly using machine literacy techniques to solve this issue.

The following embodies the benefits of this work:

1. Based on deep literacy, we suggest a multi-channel attack detection system for social network information security. To the best of our knowledge, this is the first attempt to solve the attack discovery problem in social networks using a multi-channel detection system based on deep literacy.

2. In addition, we suggest a voting algorithm that advances to obtain the majority result of the multi-channel classifiers to assess if a business is under attack or not. This algorithm achieves high accuracy.
3. Our system can be applied to other tasks because it is scalable and allows for customization of the neural network selection based on the unique features of the data.

II. OBJECTIVES

- To implement an efficient attack detection system.
- To implement a multi-class classification to identify different types of attacks.
- To design an intelligent attack detection and prevention system.
- To compare various Deep Learning algorithms to detect different types of attacks.
- To monitor the traffic flow for any malicious activities of a network in real-time.
- Detecting potential security threats in real-time across multiple channels to identify and mitigate risks before they escalate.
- Utilizing deep learning algorithms to enhance the accuracy of threat detection by analyzing complex patterns and anomalies in data.
- Minimizing false positive alerts by employing sophisticated deep learning models that can

distinguish between normal variations and actual security threats.

- Incorporating deep learning models to analyze and understand typical user behavior, enabling the identification of unusual activities that may indicate a security threat.
- Incorporating threat intelligence feeds to enhance the system's ability to recognize and respond to emerging threats based on the latest information available.

III LITERATURE SURVEY

In the work done by Cheng Feng, Tingting Li and Deeph Chana[1]. They developed a multi-level anaomaly detection frame grounded on network package signatures and machine learning ways for the construction of an ICS-specific IDS which takes less human input and gives better accuracy. Their frame combines both package position content position and time- series position anomaly discovery and the database is also incorporated into a Bloom filter to find anomalous network Packages.

So to address the temporal dependences between the successive packages, they developed an further time- series anomaly sensor which consists of LSTM(Long Short Term Memory Networks) to substantially get knowledge on utmost likely package signatures past network packages. They had applies this frame to a public ICS dataset created from SCADA system for a gas channel for confirmation. nevertheless the debit in their frame is that more training data and to increase the degree of discretization of nonstop features so as to ameliorate the detection to perceptivity over physical process related variable changes. And this requires fresh design mechanisms for learning effective and optimized former k predictions so that they can get to descry over various attack types.

In the research conducted by Xueqin Zhang, Jiahao Chen, Yue Zhou, Liangxiu Han, and (Member, Ieee)[2]. By fusing gcForest with deep convolutional neural networks (CNN), they presented a multi-layer representation learning model for precise end-to-end network intrusion detection. Benefits of this work include:
1) a new P-Zigzag-based data ciphering scheme that converts network business data into two-dimensional grayscale images for representation learning without sacrificing original information; and 2) accurate discovery on imbalanced and small-scale data with smaller hyperparameters than deep literacy models thanks to the combination of gcForest and CNN, which increases computational effectiveness.NBC, a new dataset, and CICIDS2017, which conforms to 101 classes, are three real datasets that have been used to compare the proposed frame with existing deep literacy models. According to the experimental results, our suggested system performs better in terms of accuracy, discovery rate, and FAR than other single deep learning styles (such as AlexNet, VGG19, GoogleNet, InceptionV3, and ResNet 18). Nevertheless, the debit is Due to its armature or algorithmic selection, the multiple-layer representation model is limited in its ability to learn comprehensive features, which may limit its capacity to detect complex attack features. It is also limited in its scalability and adaptability to various datasets and network configurations, which may limit its use in dynamic or complex network environments.

In the paper by Enamul Kabir, Jiankun Hu, And Hua Wang, And Guangping Zhuo[3] a new statistical fashion for intrusion discovery could involve the operation of advanced statistical methods within machine literacy models to identify patterns or anomalies in network business or system geste . Provides an in-depth analysis of being intrusion discovery styles, Including rule- grounded systems, anomaly discovery, and machine literacy approaches. Creation of statistical models similar as anomaly algorithms which can identify diversions from normal geste grounded on uprooted features.However the debit is Ethical and sequestration enterprises in the Intrusion discovery systems, especially when employing sophisticated ways, may inadvertently intrude on stoner's sequestration or raise ethical enterprises regarding data collection and analysis and Cost and conservation enforcing and maintaining a sophisticated intrusion discovery systems grounded on new statistical ways might dodge advanced costs for associations, including original setup, training and ongoing conservation.

In the paper by Giuseppina Andresini, Annalisa Appice, Nicola Di Mauro, Corrado Loglisci, And Donato Malerba[4] a new deep neural network armature is defined, in order to learn flexible and effective intrusion discovery models, by combining an unsupervised stage for multi-channel feature learning with a supervised one exploiting point dependences on cross channels. An expansive discussion of the state- of- the-art workshop in deep literacy for intrusion detection. The description of a new deep literacy intrusion detection approach, named MINDFUL(MultI-chanNel Deep FeatUre Learning for intrusion detection), that uses auto encoders to decide a multi-channel representation of overflows, and resorts to a deep literacy armature with complications, in order to expose possible patterns hidden in the adopted multi-channel representation. Limitation of the proposed methodology is that it does not give detailed information on the structure and characteristics of the attacks.Efficient knowledge is needed for processing in health sectors. Problems in reducing the gaps between the maturity and nonage classes in dataset, i.e., dataset might be imbalanced.

In the paper by Shahzeb Haider, Adnan Akhunzada, Iqra Mustafa, Tanil Bharat Patel, Amanda Fernandez, Kim- Kwang Raymond Choo,(elderly Member, Ieee), And Javed Iqbal[5] necessitates the design of an effective and early discovery of large- scale sophisticated DDoS attacks. Software defined networks(SDN) point to a promising result, as a network paradigm which decouples the centralized control intelligence from the forwarding sense. In this work, a deep convolutional neural network(CNN) ensemble frame for effective DDoS attack discovery in SDNs is proposed. The proposed frame is estimated on a current state- of- the art Flow- grounded dataset under established marks. The deep CNN ensemble will not give as deep insight into temporal patterns as LSTM- RNN, potentially limiting its capacity to discern intricate time-grounded attack behaviours.

In the paper by Hao Zhang, Member, IEEE, Yongdan Li, Zhihan Lv, Senior Member, IEEE, Arun Kumar Sangaiah, Member, IEEE, and Tao Huang [6] proposes a network attack discovery system combining a inflow computation and deep learning. The system consists of two corridor a real- time discovery algorithm grounded on inflow computations and frequent patterns and a bracket algorithm grounded on the deep belief network and support vector machine(DBN- SVM). Sliding window(SW) stream data processing enables real- time discovery, and the DBN- SVM algorithm can improve classification accuracy. Eventually, to corroborate the proposed system, a system is enforced. Grounded on the CICIDS2017 open source data set, a series of relative trials are conducted. The system's real- time discovery effectiveness is advanced than that of traditional machine learning algorithms. The attack

classification accuracy is 0.7 percentage chance points advanced than that of a DBN, which is 2 percentage points advanced than that of the integrated algorithm boosting and bagging styles, Complexity in Handling High- Speed Data Traditional intrusion discovery styles face challenges in recycling high- speed network data. • In dynamic network surroundings where new attack patterns crop , the incapability to incrementally expand the model might limit its rigidity and responsiveness to new attack types or variations.

In the paper by AshwiniB. Abhale andS.S Manivannan,[7] They developed a generalized Wireless Sensor Networks(WSNs) are vulnerable to various security pitfalls, challenging robust intrusion discovery systems. This design aims to develop and apply a supervised machine learning-based approach for detecting and grading anomalies within WSNs. apply an effective discovery system using supervised learning ways and Improves security and trustability of WSNs against vicious conditioning. Gather data with detector nodes landing normal and anomalous network actions. In real- world scenarios, the circumstance of anomalies might be significantly lower compared to normal cases. The process of labeling anomalies in WSN datasets can be subjective and time consuming. Annotating anomalies directly might be challenging due to diversity and evolving nature of intrusion patterns.

The goal of the paper by Dinesh Vishwakarma, Akash Maan, Daksh Chaudhary, and Abhinav Singhal [8] is to provide the most effective machine learning technique among the many that have been employed. The NSL-KDD dataset is used for testing and training our Network Intrusion Detection Model, and machine learning techniques such as Decision Tree, Naïve Bayes, K-Nearest Neighbors (KNN), and Support Vector Machines (SVM) are employed in the relative analysis. When tested separately, the accuracy results for Decision Tree, Naïve Bayes, K-Nearest Neighbors (KNN), and Support Vector Machines (SVM) are 98.088%, 82.971%, 95.75%, and 81.971%; when tested in conjunction with the conclusion discovery model, the results are 98.554%, 66.687%, 97.605%, and 93.914%. dependence on predetermined dataset parameters and a lack of adaptability to novel outcomes. Insufficient comparative analysis may limit our comprehension of the optimal technique for varying attack scripts or data kinds. decreased Naïve Bayes technique accuracy when combined with the conclusion model.

In the paper by Wooseok Seo And Wooguil Pak[9] proposes a two- position classifier that can contemporaneously achieve high performance and real- time classification. It employs position 1 and 2 classifiers internally. The position 1 classifier originally performs realtime discovery with moderate accuracy for incoming datatraffic.However, the bracket is delayed until the traffic inflow terminates, If the data can not be classified with high probability by the classifier. The position 2 classifier also collects the statistical features of the traffic inflow for performing precise bracket. The design focusing on real- time network intrusion prevention using a two- position bracket system is that the packet- based classifier at the first position might not achieve the same accuracy as the inflow- grounded classifier. This distinction in accuracy between the two situations might affect in misclassifications during real- time processing.

An IoTID20 dataset attack was used in the paper by Hasan Alkahtani and TheyaznH.H. Aldhyani[10] to develop the suggested system; it is a recently generated dataset from the IoT structure. Three sophisticated deep learning algorithms—a CNN complication neural network, an LSTM long short-term memory, and a hybrid CNN-LSTM complication neural network—were used in this frame to categorize the intrusion. The flyspeck mass optimization system (PSO) was used to select relevant features from the network dataset in order to enhance the suggested system and reduce the dimensionality of the dataset. Deep learning algorithms were used to reuse the acquired features. According to the experimental findings, the accuracy attained by the suggested systems was CNN96.60%, LSTM99.82%, and CNN-LSTM, 98.80%. The suggested framework achieved the desired results on a newly variable dataset, and our university's IoT terrain will enforce the system. The original dataset has 80 features, which could lead to dimensionality problems and computational outflow, particularly when processing data in real-time in an Internet of Things environment.

In the paper by Chang Liu, Member, IEEE, Ruslan Antypenko, Iryna Sushko, and Oksana Zakharchenko[11] three data- grounded exploration schemes are constructed step by step in this composition, which are a data addition scheme grounded on the variational autoencoder(VAE), a data-balancing scheme grounded on the conditional VAE, and a data- balancing scheme grounded on arbitrary under slice and conditional VAE. The three data- position- grounded schemes are combined with the deep- learning- grounded IDS. In this composition, and make trials based on the CSE- CIC- IDS2018 dataset to verify the effectiveness of three data processing schemes. After data improvement through the third scheme, theMacro-F1-score of the convolutional- neural- network-grounded IDS model bettered by3.75% and theMacro-F1-score of the reopened- intermittent- unit- grounded IDS model bettered by5.32%. The drawback is the incremental advancements inMacro-F1 scores(3.75% and5.32%) might not adequately address fleetly evolving or sophisticated attack patterns.

In the paper by Asmaa Halbouni,(Member, Ieee), Teddy Surya Gunawan,(Senior Member, Ieee), Mohamed Hadi Habaebi,(Senior Member, Ieee), Murad Halbouni, Mira Kartiwi,(Member, Ieee), And Robiah Ahmad,(Senior Member, Ieee)[12] they took advantage of the Convolutional Neural Network's capability to prize spatial features and the Long Short- Term Memory Network's capability to prize temporal features to produce a mongrel intrusion discovery system model and added batch normalization and powerhouse layers to the model to increase its performance. Based on the binary and multiclass bracket, the model was trained using three datasets CIC- IDS 2017, UNSW- NB15, and WSN- DS. The confusion matrix determines the system's effectiveness, which includes evaluation criteria similar as accuracy, perfection, discovery rate, F1- score, and false alarm rate(FAR). The effectiveness of the proposed model was demonstrated by experimental results showing a high discovery rate, high delicacy, and a fairly low FAR. still, the drawback is the CNN-LSTM model struggles with specific attacks like web attacks in CIC- IDS2017 and certain pitfalls like worms or backdoors in UNSW- NB15, performing in fairly lower discovery rates for these types of intrusions.

In the paper by P.L.S. Jayalaxmi, Rahul Saha, Gulshan Kumar, Mauro Conti, Tai- Hoon Kim[13]. The survey was conducted in which the ML and DL models were distributed and induce new confines of security frame. It is the first to offer a mapping technique study of risk factor analysis and a hybrid framework proposal for an effective security model for intrusion detection and/or prevention. We examine the significance of different AI-based methods, instruments, and techniques applied to IoT detection and/or prevention systems. More precisely, we present a comparative analysis centered on

the viability, compatibility, difficulties, and real-time issues of Machine Learning (ML) and Deep Learning (DL) approaches for intrusion detection-prevention systems. Good accuracy is achieved but only in discovery of anomaly or not, which is not suitable to descry types of attack.This survey focuses on different research works depending on IDS and IPS. This elaborates different intruision detection and prevention based on various methodologies, techniques and provide a detailed analysis of all models. It talk about an IDS base that falls into different categories based on functions, positions, and architecture. The different IDS solutions are also categorized according to the most recent research findings. We have put forth a risk factor analysis that combines mitigation strategies with mapping techniques. Since there isn't currently a survey with a framework and prevention model, our survey helps IDS and IPS designers envision how their technologies and methods will advance. The paper also provides a state-of-the-art comparison of IDS models.

In the paper by Sydney Mambwe Kasongo[14] proposed a frame which uses different types of Recurrent Neural Networks(RNNs), namely, Long-Short Term Memory(LSTM), Gated Recurrent Unit(GRU) and Simple RNN. To assess the performance of the proposed IDS frame, the NSL- KDD and the UNSW- NB15 standard datasets are considered. also, being IDSs suffer from low test accuracy scores in detecting new attacks as the point dimension grows. In this study, an XGBoost- based feature selection algorithm was enforced to reduce the feature space of each dataset. Following that process, 17 and 22 applicable attributes were picked from the UNSW- NB15 and NSL- KDD, respectively.The accuracy attained through the test subsets was used as the main performance metric in confluence with the F1-Score, the confirmation accuracy, and the training time(in seconds). The results showed that for the double bracket tasks using the NSL- KDD, the XGBoost- LSTM achieved the stylish performance with a test delicacy(TAC) of88.13%, a validation accuracy(VAC) of99.49 and a training time of225.46 s. For the UNSW- NB15, the XGBoost-Simple- RNN was the most effective model with a TAC of87.07%. For the multiclass bracket scheme, the XGBoost- LSTM achieved a TAC of86.93% over the NSL- KDD and the XGBoost- GRU attained a TAC of78.40% over the UNSW- NB15 dataset. The debit is the RNN- grounded IDS, especially for complex datasets like NSL-KDD, showed longer training times(e.g., 5516s to 11444s). This might hamper scalability in real- time operations or resource- constrained surroundings.

In the paper by Thanh Thi Nguyen and Vijay Janapa Reddi[15] presents a survey of Deep Reinforcement Learnings(DRL) approaches developed for cyber security. We touch on different vital aspects, including DRL- based security methods for cyber – physical systems, independent intrusion discovery ways, and multiagent DRL- grounded game proposition simulations for defense strategies against cyberattacks. expansive conversations and future exploration directions on DRL- grounded cyber security are also given. This review provides the foundations for and facilitates future studies on exploring the eventuality of arising DRL to manage with decreasingly complex cyber security problems. This composition focuses on the ultimate where DRL styles are used to break cyber security problems with the presence of cyberattacks or pitfalls. An arising area is the use of DRL for security results for CPSs. The large- scale and complex nature of CPSs,e.g., in environmental monitoring networks, electrical smart grid systems, transportation operation networks, and cyber manufacturing operation systems, require security results to be responsive and accurate. This has been addressed by various DRL approaches,e.g., TRPO algorithm, LSTM- Q-literacy, DDQN, and A3C. One of the great challenges in enforcing DRL algorithms for CPS security results is the lack of realistic CPS simulations.

TITLE	ALGORITHM	DATASET	RESULT (ACCURACY)	DESCRIPTION	DRAWBACKS
Supervised Machine Learning Classification Algorithmic Approach for Finding Anomaly Type of Intrusion Detection in Wireless Sensor Network.	Machine Learning Algorithms	NSLKDD	1)Random-Forest classifier-0.83 2)Support Vector-Machine-0.84 3)Decision Tree Classifier-0.81 LGBM Classifier-0.78 4)Extra Tree_Classifier-0.80 5)Gradient Boosting Classifier-0.77 6)Ada Boost Classifier-0.78 7)K-Nearest NeighbourClassifier-0.82 8)MLP-Classifier-0.83 9)Gaussian Naive Bayes Classifie-0.81 0)Logistic Regression Classifier-0.80	In this work, supervised classification models for intrusion detection are built using such as Random-Forest classifier,Support Vector-Machine, Decision Tree Classifier,LGBM Classifier,Extra Tree_Classifier, Gradient Boosting Classifier, Ada Boost Classifier, K Nearest Neighbour Classifier, MLP-Classifier, Gaussian Naive Bayes Classifier and Logistic Regression Classifier.	1)In real-world scenarios, the occurrence of anomalies might be significantly lower compared to normal instances. 2)The process of labeling anomalies in WSN datasets can be subjective and time consuming. Annotating anomalies accurately might be challenging due to diversity and evolving nature of intrusion patterns.
A Hybrid Machine Learning and Data Mining Based Approach to Network Intrusion Detection	LSTM-CNN	CICIDS2017	98.60%	Propose a control plane-based orchestration for varied sophisticated threats and attacks. The proposed mechanism comprises of a hybrid Cuda-enabled DL-driven architecture that utilizes the predictive power of Long short-term memory (LSTM) and Convolutional Neural Network (CNN) for an efficient and timely detection of multi-vector threats and attacks.	1)Reliance on predefined dataset conditions and lack of adaptability to new inferences. 2) Lack of comprehensive comparison might restrict the understanding of which technique performs best across diverse attack scenarios or data types. 3)Decreased accuracy of the Naïve Bayes technique when integrated with the inference model
Real-Time Network Intrusion Prevention System Based on Hybrid Machine	Two level Classifiers: Packet Based, Session Based, Algorithms: DT, RF	1)UNSW-NB15 2)CICIDS2017	1) COMPARISON OF THE PERFORMANCE FOR MULTI-CLASS CLASSIFICATION: For UNSW-NB15 dataset: i)DT-95.8% ii)RF-96.2% For CICIDS2017 dataset: i)DT=99.98% ii)RF-99.89% 2) COMPARISON OF THE PERFORMANCE FOR BINARY-CLASS CLASSIFICATION: For UNSW-NB15 dataset: 1)DT-97.9% 2)RF-98.1% For CICIDS2017 dataset: 1)DT-99.98% 2)RF99.98%	Proposed two-level classification method can achieve superior performance in terms of accuracy and detection time.	The project focusing on real-time network intrusion prevention using a two-level classification system is that the packet-based classifier at the first level might not achieve the same accuracy as the flow-based classifier. This discrepancy in accuracy between the two levels might result in misclassifications during real-time processing

TITLE	ALGORITHM	DATASET	RESULT (ACCURACY)	DESCRIPTION	DRAWBACKS
Multi-Level Anomaly Detection in Industrial control Systems via package Signatures and LSTM Networks	1)Stacked Long Short Term Memory (LSTM) network based soft-max classifier 2)A Bloom filter is used to store the signature database	Real dataset created from a gas pipeline SCADA system	Precision-0.94 Recall -0.78 Accuracy-0.92 F1-score-0.85	1)It is able to learn normal behaviour solely from normal data, and thus can detect unseen attacks, 2) It is able to deal with complicated data samples with hybrid features,	1)The value of k for time-series level anomaly detection is fixed. 2)The detection rates of our framework for CMRI, MSCI, MPCI attack types are lower than other attack types.
A Multiple-Layer Representation Learning Model for Network-Based Attack Detection.	(CNN) with gcForest	NBC, a combination of UNSW-NB15 and CICIDS2017 consisting of 101 classes	Accuracy- caXGBoost9 :95.79% gcForest:95.79% GoogleLeNetNP-43.4%	Proposed method outperforms other single deep learning methods (i.e., AlexNet, VGG19, GoogleNet, InceptionV3, ResNet18) in terms of accuracy, detection rate, and FAR, which demonstrates its effectiveness in detecting fine-grained attacks and handling imbalanced datasets with high-precision and low FAR	1)The multiple-layer representation model have limitations in achieving comprehensive feature learning due to its architecture or choice of algorithms, potentially restricting its ability to capture intricate attack features. 2) Have limitations in scalability or adaptation to diverse datasets and network structures, potentially restricting its application in evolving or complex network environments.
A Novel Statistical Technique for Intrusion Detection	Optimum allocation-based least square support vector machine (OA-LS-SVM)	KDD 99 dataset	99.84%	Proposes a novel approach for intrusion discovery systems based on sampling with Least Square Support Vector Machine (LS-SVM).	Privacy and Ethics Issues with intrusion detection systems can unintentionally violate user privacy or give rise to moral questions about data collection and analysis, particularly when advanced techniques are used.
Multi-Channel Deep Feature Learning forIntrusion Detection.	Two autoencoders are separately learned on normal and attack flows, respectively. Algorithms:MINDFUL	KDDCUP99 dataset, UNSW-NB15 dataset, CICIDS2017 dataset.	Accuracy and F-score for 1)KDDCUP99 dataset-92.49% -95.13% 2)UNSW-NB15 dataset-93.40% -95.29% 3)CICIDS2017 dataset-97.90% -94.93%	The proposed neural network architecture leads to better predictive accuracy when compared to competitive intrusion detection architectures on three benchmark datasets.	1)Limitation of the proposed methodology is that it does not give detailed information on the structure and characteristics of the attacks. Efficient knowledge is required for processing in health sectors. 2)Problems in reducing the gaps between the majority and minority classes in dataset, i.e., dataset might be imbalanced.
A Deep CNN Ensemble Framework for Efficient DDoS Attack Detection in Software Defined Networks.	Ensemble CNN	Flow-based dataset CICIDS2017	Accuracy-99.45% F1 score-99.61%	A deep convolutional neural network (CNN) ensemble framework for efficient DDoS attack detection in SDNs is proposed. . Improved accuracy is demonstrated against existing related detection approaches.	The deep CNN ensemble will not provide as deep insight into temporal patterns as LSTM-RNN, potentially limiting its capacity to discern intricate time-bas
A Real-Time and Ubiquitous Network Attack Detection Based on Deep Belief Network and Support Vector Machine.	DBN-SVM, Sliding window (SW) stream data processing enables real-time detection, and the DBN-SVM algorithm can improve classification accuracy.	CICIDS2017,	The attack classification accuracy is 0.7 percentage points higher than that of a DBN, which is 2 percentage points higher than that of the integrated algorithm boosting and bagging methods.	The method's real-time detection efficiency is higher than that of traditional machine learning algorithms. It is suitable for the real-time detection of high-speed network intrusions.	Complexity in Handling High-Speed Data: Traditional intrusion detection methods face challenges in processing high-speed network data. • In dynamic network environments where new attack patterns emerge, the inability to incrementally expand the model might limit its adaptability and responsiveness to new attack types or variations.

V. WHY IS THE PARTICULAR TOPIC CHOSEN?

Attacks in wireless detector networks(WSNs) aim to help or annihilate the network's capability to perform its anticipated functions. Intrusion discovery is a defense used in wireless detector networks that can descry unknown attacks. Due to the inconceivable development in computer- related operations and massive Internet operation, it is necessary to give host and network security. The development of playing technology tries to compromise computer security through intrusion. To avoid the security breaches we have motivated to choose this content.

VI. METHODOLOGY

There are two phases to the suggested intelligent attack detection system: training and testing. In the training phase, there are three methods: data preprocessing, multi-feature creation, and multi-channel training. In the testing phase, there are three methods: data preprocessing, multi-feature extraction, and attack detection. In both phases, the first two methods are the same. Data preprocessing, which includes data sampling, data cleansing, and data dimensionality, is a collection of processing methods used to provide high-quality data during the training phase. Different kinds of data features can be extracted as vectors using multi-feature extraction. In order to create classifiers based on neural networks that distinguish attacks from normal data while preserving the attack features of input vectors, multi-channel training is utilized.
In the testing phase, input vectors will be placed into multi-channel processing for classifier discovery following preprocessing and multi-feature extraction.
We implement a voting algorithm based on the classifier discovery result to determine whether or not the input test data is an attack. To increase the accuracy of the attack detection, these variables combine and are simultaneously optimized.

Preparing Data Converting the input data into a vectorizable matrix format is one of the preprocessing steps. Data dimensionality reduction, data sanctification, and data slice are examples of common operations. Both the training and testing phases use the same processing step. Multiple-Feature Extraction Due to their diverse origins, the business data within the network typically possesses a variety of features. The features that have been uprooted as vectors are combined into multiple features, which are then allocated to various training channels. The traffic data of the KDD dataset, for example, can be divided into three categories of features: traffic-based features, content-based features, and introductory features. Introductory features, traffic-based features, and content-based features make up the multifeature set known as
"ALL-TYPE"

Multi-Channel Instruction Based on Neural Nets In addition to producing classifiers to detect network attacks, each training channel is analogous to a neural network. The input for the neural network training is the features that were removed in the previous step.. Scalability of the number of channels is based on the factual operation. The choice of neural

network should take into account the unique features. Given that the traffic data is organized in a sequence, this paper names the Long Short Term Memory Transformer (LSTM-Transformer) because of its benefits for sequence modeling. Attack Identification Every classifier associated with a discovery channel determines whether or not the traffic is an attack. Additionally, the outcome is sent to Vote and Decision, which determines whether or not the initial traffic is an attack using a voting algorithm. Prior to the attack detection stage, feature extraction and data preprocessing are required.

VII. CONCLUSION

The perpetration of intelligentmulti-channel trouble discovery using deep literacy technologies is vital for fortifying data security. By early identification of implicit pitfalls, adding delicacy, and integrating different data sources, this approach provides a comprehensive and adaptive defense medium. The reduction of false cons, robotization of responses, and scalability contribute to a robust security posture. Incorporating user behavior analysis, nonstop monitoring, and compliance adherence ensures a holistic approach

.

Likewise, the integration of trouble intelligence feeds enhances the system's responsiveness to arising pitfalls. Eventually, by addressing these objects, associations can establish a visionary and sophisticated defense against evolving cyber pitfalls, securing sensitive information in an decreasingly complex digital geography.

REFERENCES:

[1] C. Feng, T. Li and D. Chana, "Multi-level Anomaly Detection in Industrial Control Systems via Package Signatures and LSTM Networks," *2017 47th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN)*, Denver, CO, USA, 2017, pp. 261-272, doi: 10.1109/DSN.2017.34.

[2] X. Zhang, J. Chen, Y. Zhou, L. Han and J. Lin, "A Multiple-Layer Representation Learning Model for Network-Based Attack Detection," in *IEEE Access*, vol. 7, pp. 91992-92008, 2019, doi: 10.1109/ACCESS.2019.2927465.

[3] Enamul Kabir, Jiankun Hu, Hua Wang, Guangping Zhuo, A novel statistical technique for intrusion detection systems,Future Generation Computer Systems,Volume 79, Part 1,2018,ISSN 0167-739X.

[4] G. Andresini, A. Appice, N. D. Mauro, C. Loglisci and D. Malerba, "Multi-Channel Deep Feature Learning for Intrusion Detection," in *IEEE Access*, vol. 8, pp. 53346-53359, 2020, doi: 10.1109/ACCESS.2020.2980937.

[5] S. Haider *et al.*, "A Deep CNN Ensemble Framework for Efficient DDoS Attack Detection in Software Defined Networks," in *IEEE Access*, vol. 8, pp. 53972-53983, 2020, doi: 10.1109/ACCESS.2020.2976908.

[6] H. Zhang, Y. Li, Z. Lv, A. K. Sangaiah and T. Huang, "A real-time and ubiquitous network attack detection based on deep belief network and support vector machine," in *IEEE/CAA Journal of Automatica Sinica*, vol. 7, no. 3, pp. 790-799, May 2020, doi: 10.1109/JAS.2020.1003099.

[7] Ashwini B. Abhale, Manivannan, S.S. Supervised Machine Learning Classification Algorithmic Approach for Finding Anomaly Type of Intrusion Detection in Wireless Sensor Network. *Opt. Mem. Neural Networks* **29**, 244–256 (2020). https://doi.org/10.3103/S1060992X20030029.

[8] Singhal, A. Maan, D. Chaudhary and D. Vishwakarma, "A Hybrid Machine Learning and Data Mining Based Approach to

Network Intrusion Detection," *2021 International Conference on Artificial Intelligence and Smart Systems (ICAIS)*, Coimbatore, India, 2021, pp. 312-318, doi: 10.1109/ICAIS50930.2021.9395918.

[9] W. Seo and W. Pak, "Real-Time Network Intrusion Prevention System Based on Hybrid Machine Learning," in *IEEE Access*, vol. 9, pp. 46386-46397, 2021, doi: 10.1109/ACCESS.2021.3066620.

[10] Hasan Alkahtani, Theyazn H. H. Aldhyani, "Intrusion Detection System to Advance Internet of Things Infrastructure-Based Deep Learning Algorithms", *Complexity*, vol. 2021, Article ID 5579851, 18 pages, 2021. https://doi.org/10.1155/2021/5579851.

[11] Liu, R. Antypenko, I. Sushko and O. Zakharchenko, "Intrusion Detection System After Data Augmentation Schemes Based on the VAE and CVAE," in *IEEE Transactions on Reliability*, vol. 71, no. 2, pp. 1000-1010, June 2022, doi: 10.1109/TR.2022.3164877.

[12] Halbouni, T. S. Gunawan, M. H. Habaebi, M. Halbouni, M. Kartiwi and R. Ahmad, "CNN-LSTM: Hybrid Deep Neural Network for Network Intrusion Detection System," in *IEEE Access*, vol. 10, pp. 99837-99849, 2022, doi: 10.1109/ACCESS.2022.3206425.

[13] P. L. S. Jayalaxmi, R. Saha, G. Kumar, M. Conti and T. -H. Kim, "Machine and Deep Learning Solutions for Intrusion Detection and Prevention in IoTs: A Survey," in *IEEE Access*, vol. 10, pp. 121173-121192, 2022, doi: 10.1109/ACCESS.2022.3220622

[14] Sydney Mambwe Kasongo, A deep learning technique for intrusion detection system using a Recurrent Neural Networks based framework, Computer Communications, Volume 199, 2023, ISSN 0140-3664.

[15] Thanh Thi Nguyen, Vijay Janapa Reddi, Deep Reinforcement Learning for Cyber Security, IEEE Transactions on Neural Networks and Learning Systems, 2021 (Early Access), arXiv:1906.05799, https://doi.org/10.1109/TNNLS.2021.3121870