Journal of Harbin Engineering University
ISSN: 1006-7043

Vol 45 No. 7
July 2024

Threat Modelling Based on NIDS Attack Emulation with Deep Learning & Optimization Techniques

[1]Mukul Gaharana Kulshrestha, [2]Dr Satish Salunkhe, [3]Dr Vaishali Khairnar,
[1]Terna Engineering College
Department of Information Technology
Navi Mumbai
[2]Terna Engineering College
Department of Information Technology
Navi Mumbai
[3]Terna Engineering College
Department of Information Technology
Navi Mumbai

Abstract
The prevalence of cyber-attacks has become a part of every software organization today which necessitates the need of protection so that user data, policies and procedures remain intact. Attacks and threats tend to create an imbalance in the confidentiality and integrity of the system. The infrastructure of the software is thus at risk and can be exposed to various malicious attacks. In such a scenario, a threat modelling procedure is needed so that user data remains secured. A service model that caters to the discerning issues of cyber-attacks is an intrusion detection technique that provides a coherent view and makes the detection system more robust in nature. The associated security concerns are therefore identified using the IDS technique and respective configurations are thus made. Therefore, the study thus proposed focuses to implement a network based intrusion detection system that inclines to identify cyber-attacks in conjunction with deep learning based strategies. Additionally the study makes use of Long Short-Term Memory (LSTM), Bi-directional Long Short-Term Memory (Bi-LSTM), and Bi-directional Long Short-Term Memory with Particle Swarm Optimization (BILSTM with PSO) in order to determine the excruciating patterns within a networking traffic. The entire process of implementation is done using the three algorithms based on DL. For this purpose a dataset consisting of various threat and attack scenarios is used. UNSW-NB15 is acquired from the Kaggle repository and further trained and tested on. However, evaluation is done on the basis of accuracy and precision factors and the model is rigorously run to generate improved results. The study on evaluation highlights that the Bi-LSTM model along with PSO generates highest optimization accuracy of 99percent and is therefore considered to inhibit tremendously potential in terms of generating insights to detect cyber threats and attacks.
Keywords: *cyber threat, cyber-attacks, threat modelling, NIDS, HIDS*

Introduction
As technology continues to inhibit every part of our daily lives, cyber threats and attacks have become an indispensable space for everybody who uses it. The growing threat posed by cybercriminals to an organization's digital security is driving it to look for more intelligent ways to protect the system. Detection measures are thus becoming more and more necessary to guard against growing cyber threats as digital platforms and solutions are adopted more widely. The goal of such detection systems is to prevent unauthorized access, harm from cyber-attacks and threats, and safeguard devices, networks, and data. This domain is constantly evolving, and organizations and individuals need to remain vigilant in order to stay away from breaches who aim to compromise their safety. Deep Learning is therefore becoming a more sophisticated weapon against these new cybercrimes, and many companies and governments have their sights set on it. Deep Learning (DL) is a technology that has become more and more common in many industries in recent years. Data indicates that over the past few years, the use of DL in cyber security has increased rapidly across the globe, indicating that an increasing number of businesses are looking for more efficient solutions than the

conventional ones. However, some people are hesitant to put it into practice. Previous studies indicate that the cyber security branch discusses this issue. It can automate complicated processes and make forecasts that are complacent on large amounts of data it has been trained on. Numerous developments in DL have the potential to increase its usefulness and power for companies and organizations [1]. With each new set of data it encounters, these techniques are utilized to evaluate, interpret, and make predictions and conclusions, allowing the system to learn even more. As more and more data becomes available, deep learning (DL) systems can be trained to remember from vast and diverse data sets. In the domain of modeling threats, specifically, DL has the potential to leverage historical data to anticipate, identify, and avert potential attacks before they do harm to an organization. By continuously scanning the system for anomalies or weaknesses, a DL may lessen the openings that hostile systems could take advantage of. DL is now widely accepted by organizations as a vital component of both their business and security, serving as a weapon against cybercriminals who would compromise their security.

The 21st century's technological revolution is mostly being driven by DL and ML, which are drastically changing a variety of technological fields. Among its most notable applications is threat modeling. The most sensible way to address the issue of cyber threats and attacks is to deploy a distributed intrusion detection system (IDS) on virtual networks from possible threats. An intrusion detection system is a piece of software that is frequently used to monitor how well a system is operating. This is carried out with the goal of reporting to the system and stopping unexpected behaviors as and when detected. The mechanism works by identifying a suspicious activity and further taking an initiative to protect the network against the attack. This is carried out to guard against network breaches. The intrusion detection system offers a more efficient way to guarantee the security of the network as a whole when compared to other types of security systems. Furthermore, one of two main methodologies can be used to develop IDS in many cases. The first method is intended to detect anomalous events. Finding unusual behaviors or data that deviates from a pre-existing model is one of the applications of "anomaly detection." Conversely, it could result in a sizable number of false conclusions. Signature-based detection, which relies on a knowledge base, is the second method for building an intrusion detection system, or IDS [2]. Because it is so good at identifying known threats by using the signatures of recorded events to infer likely attackers, the signature-based detection method is tremendously helpful. Because of this, the signature-based detection method is a very significant strategy. A collection of data instances often referred to as objects, records, points, vectors, patterns, cases, samples, and observations, always makes up the general input data.

Hence, the aim of the research study is to increase the overall threat precision factor through the usage of NIDS and implement the same using deep learning based strategical algorithms. For this purpose; three techniques are used and the fundamental security of the system is enhanced. The author also aims to develop a hybrid based PSO algorithm within the normal functioning of the Bi-LSTM technique. The entire issue of securing the system model from cyber threats and attacks is therefore proposed to be deployed.

Following are the primary objectives of the research study:

- To automate the process of threat attacks using NIDS
- To deploy the same using a hybrid model by integrating the concepts of Bi-LSTM along with PSO
- To enhance the overall accuracy of the system and achieve an inclined position of optimization
- To conduct an overall comparative analysis of the algorithms thus conducted

An in-depth examination of the crucial cyber threat and development of the modelling system with DL is provided in the following sections. This investigation starts by looking at a network intrusion detection system (NIDS) uses DL to anticipate and stop cyber-attacks. It does this by efficiently coordinating a variety of security tools and connecting information from various sources, including security information and event

management, intrusion detection systems, endpoint detection and response, and others. The discussion then turns to the relative works being done by the respective authors. Furthermore, the used methodology and implemented techniques are also mentioned. On the other hand, the results section highlights the observations thus generated followed by the conclusions. The research finally comes to an end with the key mention of references used.

A. Taxonomy of NIDS

The working principle of an Intrusion Detection System (IDS) is based on securing the network from malicious activities so that its application software's remain intact. Such malicious activities when identified are expected to be alarmed to the information system. Any form of violation or breach of firewalls is included in this identification process. For instance; any activity that slows down or abrupt the process of authenticating a legit user is considered to be a form of intrusion. In some scenarios; the deployed firewalls are unable to identify and report the occurrence of such malicious activities. Hence, its detection must be prevailed through the usage of intrusion detection system's (IDS). The implementation of IDS can be categorized to be as host based or network based. On the other hand; the conceptual usage of hybrid based detection system is a combination of host based and network based IDS.

A *host based IDS* are responsible to detect cyber threats that tend to occur only on a specific machine and hence are capable to monitor the attack in minute details. This eventually indicates that the HIDS can monitor the attack taking place to the machine it is assigned to. A major difference between NIDS and HIDS is that; the HIDS is fully aware so as to what disruption might be caused in the system due to the attack which took place. This makes the HIDS fully aware of the outcomes which are expected to be generated in case of a cyber-threat.

On the other hand, a *network based IDS* are considered to be those devices which are placed within the network and can therefore access and comprehend the attacks that might takes place within that network. An NIDS can either be detected in software's or hardware's. Hardware mediums of an NIDS include Ethernet and FDDI. The implementation of an NIDS takes place on two networking interfaces; the first interface is primarily used to monitor the occurrence of an attack and report it respectively; whereas the second interface is used to listen to the networking conversations that occur in a promiscuous mode [3]. Further, the working implementation of an NIDS can either be signature based or anomaly based. However, NIDS does depict certain drawbacks such as overloading and tuning difficulty. Figure 1 illustrates an example of a conventional NIDS system.

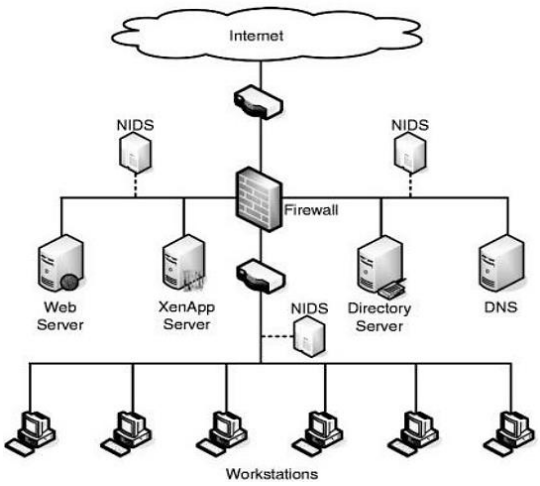

Figure1: A conventional NIDS System

A *hybrid based IDS* is expected to be a combination of HIDS and NIDS wherein it integrates the strengths of both the systems and generates a comparatively efficient system which is responsible to detect malicious data coming through HIDS and NIDS. However; there are many

advantages and disadvantages associated with the working implementation of HIDS and NIDS and hence the usage of both the IDS is heavily dependent on the purpose it tends to serve. A commonality factor between the two is the acceptance of both the operations i.e. to use signature based and anomaly based IDS.

In such a scenario, choosing the right IDS becomes a crucial task. Therefore an IDS which is capable to cater the objective of a software system must be used by understanding its respective protocols. A systematic channel of protocol analysis must be followed so that the overall accuracy of the software is enhanced and a decrease in the rate of false positives must be observed.

B. Deep Learning based IDS

The concepts of deep learning are derived through a sub-category of machine learning wherein multiple layers of neurons are used in order to model the software system and further establish intricate relationships amongst each other. Outputs are generated at the lower levels wherein supervised and unsupervised algorithms are used to identify threat attacks. Such algorithms help to generate optimized levels of accuracy in conjunction to the level of layered abstraction they provide. In such a scenario, IDS plays a vital role wherein its fundamental responsibility is to monitor the network and trigger alarms on detection of malicious activities. In this way; a networking system is defended from vulnerable threats. With wide adoption of IDS in cyber security; the conceptual implementation of deep learning (DL) has also evolved tremendously [4]. Various findings are initiated and used through multiple stages of image processing, computer vision and NLP. The usage of DL is also inclined due to its feature representations which are being made in a hierarchical format and its acquisition involves long term temporal patterning. Due to its heuristic and hierarchical approach; the implementation of DL has become exceedingly effective amongst various research scholars and software developers. Hence, an amalgamation of DL with IDS has been meticulously highlighted so that the overall perspective towards threat modelling and detection can be done in an enhanced manner. However, despite of the disadvantages an ML would go through; due to lack of research, unavailability of datasets; the inclination of DL overshadows its usage and tends to facilitate high-quality learning for complex data processing. This has led to the evolution of a parallel processing system wherein a robust mechanism is developed. On the other hand; there are certain drawbacks that assist with the implementation of DL in an information system. It majorly includes: generation of false positive rates due to inefficiency in the dataset and detection of various malicious activities due to absence of a firewall. In such a scenario; DL based models are unable to neutralize the detection process and therefore tend to skip various attack vectors which are already present in the dataset. Hence, the integration of DL with IDS appears to be sustainable solution wherein the expanding dataset could be heterogeneously monitored in real time over a designed network.

A two-stage architecture adaptive network intrusion detection system is defined to be as the taxonomy of IDS. By using the evolution theory to explain how data and connections evolve inside a network, the author of the proposed research study tends to lower the overall complexity of the threat detection system model. As an attack occurs on one node, it propagates over the network to notify other nodes that are cooperating about new attack patterns. This will result in early assault identification and prevention of further attacks.

An intrusion detection system (IDS) with high throughput is used as the base of NIDS. It makes use of the Bi-LSTM algorithms along with the Particle Swarm Optimization (PSO) technique. This would improve the accuracy of the result and fasten the detecting process. Because of its attributes, including dimensionality, highly correlated features, and large stream volumes, it may be able to assist in solving intrusion detection problems in a lesser time frame.

Related Works

One of the most important developments in this field is the implementation of NIDS, which represents a move away from discrete security measures and towards a more intelligent and integrated approach to securing the cyber system from security threats. With a comprehensive

approach to threat modelling, NIDS is an integrated set of security tools that offers centralized threat detection, investigation, and response capabilities across many security tiers [5]. The goal of NIDS is to combine several security products into a unified system that can process and correlate data from servers, networks, endpoints, and system workloads. By fusing data from several sources into a unified, efficient analytical framework, NIDS aims to overcome these obstacles in contrast to traditional security solutions. The main benefit of NIDS is that it can be used to uncover subtle and sophisticated threats that could otherwise go undetected by using advanced analytics, ML, and DL to the aggregated security data. Through the use of these technologies, NIDS platforms are able to identify patterns and abnormalities that point to malicious behaviour, providing a level of detection that is both more thorough and comprehensive than that of conventional techniques. Because of its integrated response feature, mitigation and remediation steps can be completed more quickly, minimizing potential damage and the amount of time attackers spend in the system (known as dwell time). With its broad reach and thoughtful, automated answers, the usage of NIDS is an evolutionary step forward in threat detection and response, with the potential to improve and streamline cyber security operations.

When Deep Learning and Machine Learning are used in conjunction with NIDS's immense potential, an unmatched combination for digital space security is created. NIDS allows for a more complete, in-depth and exhaustive examination of cyber threats by taking into account both supervised and unsupervised learning techniques. Furthermore, the system can create and execute prompt, efficient, and customized responses to different types of attacks, guaranteeing a thorough security plan that is reactive, adaptable, and proactive all at once. This implies that enterprises are ready for potential future attacks in addition to being shielded from present dangers [5].

This quick reaction lowers the possibility of a materially harmful outcome by identifying the margin of risk exposure. In the present era of cyber security, where threats are incredibly dynamic and continually developing in both complexity and time consuming intent, it is imperative to be able to respond swiftly and effectively. This improves DL/ML systems' capacity to provide more thorough and precise analysis, possibly recognizing risks that are more intricate and distinct. By expanding the breadth and depth of threat identification and enhancing the efficacy of attack response, the integration of NIDS thereby underscores the significance of cooperative interaction across various forms of security data. Because of this, a threat modelling system that combines the strength of NIDS and DL/ML technologies can more effectively tackle the difficulties posed by contemporary cyber security. In order to provide proactive and effective defence against ever-changing and more diverse cyber threats, a multifaceted and all-encompassing strategy is therefore needed.

Authors in [6] presented their work on an intrusion detection model using machine algorithms in a big data setting. This study indicates that the growing volume of big data has changed the importance of analytic and data security technologies. An intrusion detection system (IDS) keeps a check on and evaluates data to find any potential breaches into the system or network. Because of the amount, variety, and speed at which data is generated within networks, traditional methods for identifying network attacks have grown more intricate. IDS analyses big data accurately and efficiently by utilizing big data methodologies. They were able to build an intrusion detection model that can handle massive volumes of data by utilizing the Spark-Chi-SVM architecture. For the purpose of expediting the handling and analysis of data, the Spark Big Data platform was employed in the suggested manner.

The categorization process is made more complicated and time-consuming by the enormous dimensionality of big data. Kumar, Saravanan and Vijayakumar presented a survey of intrusion detection systems that used machine learning techniques in [7]. The authors claimed that in today's world, computers and network-based technologies are becoming more and more typical. In the era of computers, network security is extremely important. An Intrusion Detection System (IDS) is designed to identify system attacks and therefore categorize the system activity into

normal and abnormal forms. Machine learning-based intrusion detection systems (IDS) are becoming more and more popular. The suggested system on the cloud will be accompanied by edge network components from cloud providers. As a result, the edge network routers on the physical layer may intercept incoming network traffic. Each Cloud router gathers network data, which is pre-processed using a time-based sliding window technique before being sent to a module that uses the Fuzzy Classifier to find anomalies. Each anomaly detection module has access to server nodes powered by Map Reduce and Hadoop when there is an accumulation of network congestion. Each time frame is assigned to a server for synchronizing aberrant network traffic data. Every router in the system provides data about aberrant network traffic to this server. Therefore it is in this process that various attacks are thus being identified.

In another research as observed in [8], the authors assert the concerns regarding the security of computer networks are shared by all stakeholders, including corporations, governments, and customers. The tactics that attackers employ to carry out such attacks also change as it gets harder to defend networked systems against attacks. Because deep learning is so effective at creating intrusion detection systems, this method is gaining popularity (IDS). The system's overall performance increases significantly as IDS attributes like representation and discrimination are improved. Using Principal Component and Deep Learning Auto-Encoder (AE). For the purposes of this investigation, the dimensionality of the characteristics was decreased using Principal Components Analysis (PCA) (PCA). Combining these two methods produced low-dimensional features that were used to create classifiers like Bayesian networks, Random Forests.

Methodologies Used

It is crucial to explain the rationale behind selecting a methodology over other viable ones in order to demonstrate why such approaches are the most evident method of gathering data on this subject. To find the information that would be most useful for our research study, there may be a number of ways to look into this area. A literature review is one type of research methodology that focuses on analysing the body of knowledge on the study thus presented. A literature review is crucial for any research project, but in the case of this paper, it would not be sufficient to address the research work done by previous authors; rather tend to use methodologies that might pertain to detection of threats and attacks at the right time.

Regarding similar works, literature reviews used in [8], [9] and [10] present their views on threats and breaches and tend to go through assessments being made from the available data, but they do not produce any new empirical evidence. Instead, when faced with a problem in the field, they depend on the body of existing knowledge and resources. On the other hand, the proposed study aims to focus on the fundamental issue of detecting cyber threats through the usage of NIDS and further prevent its occurrence in real time. For this purpose, it makes use of a set of methodologies and implements the same through a set of algorithms based on deep learning concepts.

A. Neural Networks

Deep learning is the process through which a computer learns from its own experiences. This type of instruction combines learning through analogies with learning from prior experiences. Deep learning research is often carried out apart from its real-world applications. In order to assess the utility of a newly created classification method, a researcher could create a brand-new approach and then compare its performance (such as accuracy or AUC) with the performance of an already-existing data set of publically available classification models. A computer that is capable of deep learning may automatically adapt to the intricacies of its environment; this ability can be further enhanced by experience and exposure to a greater number of examples. Currently, the most popular example of deep learning software are the neural networks. The aim of artificial neural network development is to emulate the capabilities of biological neural networks. In order to address artificial intelligence difficulties, each neuron in the network has been meticulously trained to collaborate without the need to first construct a model of an actual system. The network as a whole is able to resolve these issues.

One way to characterize a neural network is as a system built on a model of the human brain's architecture. Numerous nerve cells those are able to communicate with one another make up the human brain. These nerve cells are the basic building blocks of the brain's information processing machinery, which is powered by neurons.

B. Algorithms Used

- LSTM: The acronym for LSTM stands for Long Short Term Memory and is considered to be as the special case of RNN execution. An LSTM is generally capable of learning dependencies which are considered to be long term and hence are capable to process larger datasets. Since it's a special case of RNN; LSTM's is explicitly a variant designed to solve complex issues which involves longer period of run time. They tend to connect various bits of information and hence portray an illustration of a chain like structure. This structure is expected to have a repeating module which interacts with each other and thereby forms a single neural network. One of the most important key components through which the information flows is termed as the cell state. A cell state is capable to add or remove any transfer of information which is regulated within the LSTM module.

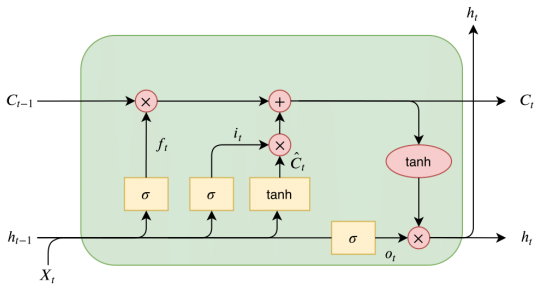

Figure 2: Visual Representation of LSTM

- Bi-LSTM: The acronym for Bi-LSTM stands for Bidirectional LSTM and is considered to be as the subtle example of an RNN network. It is primarily used on NLP and is capable to transfer information in both the directions; unlike a conventional LSTM. It tends to consume the information, directs the input flow and models the sequence in which the final transfer of information must take place. This sequential flow can take place in both the directions with the additional layer of LSTM therefore capable to reverse the direction of information flow whenever required. In such a scenario, when the input sequence flows in a backward direction; the final output is assumed to be as the aggregation from both the LSTM layers.

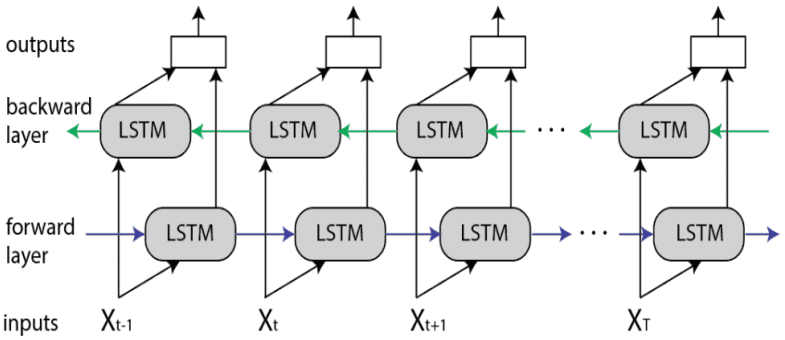

Figure 3: Visual Representation of Bi-LSTM

- Bi-LSTM with PSO: Particle Swarm Optimization is a stochastic based optimization algorithm which tends to make use of specific parameters in order to optimize complex problems surrounding it. Each particle in the PSO is observed to have its own velocity and fitness value with

which it is expected to be present. It is important to keep a track of all these particles so that the point wherein the particles might come together as a swarm can be determined. The author of the proposed study tends to deploy a hybrid model that consists of PSO along with a Bi-LSTM model. The deployment of the same aims to enhance the overall accuracy of the system and improves the final prediction of the mode thus built. The PSO-Bi-LSTM is therefore capable to capture transfer of information that takes place in both the directions and further models them in a complex temporal sequence so that the overall traffic flow of the data is also maintained. Due to the presence of Bi-LSTM in the model; the system becomes less prone to the vanishing gradient issue. In this way the network never stops learning and hence the convergence rate of the basic PSO tends to become non-linear. The model is therefore observed to capture the best temporal dependency by balancing all the associated hyper-parameters.

System Design

A. Dataset Description

A networking traffic data is present in the dataset thus acquired from the Kaggle repository. The data is labelled as UNS-NB15 and is created by an Australian Centre in order to serve the purpose for cyber security [11]. The centre majorly studies the attack behaviours that take place in real time. The attacks are further detected through the usage of hybrid models created by IXA PerfectStorm. A Tcpdump tool is also opted which is used to capture 100GB of raw incoming data attacks. A total of 9 attack types are present in the dataset, namely; Fuzzers, Analysis, Backdoors, DoS, Exploits, Generic, Reconnaissance, Shellcode and Worms. Apart from this, the dataset also comprises of a train and test file which is present in the csv format. 49 features are labelled in the train class and are further described UNSW-NB15_features.csv file.

B. Workflow of the Proposed Model

The primary aim of the author in the proposed research study is to detect cyber threats and attacks using the technique of NIDS. In addition to this, the author also proposes to implement deep learning based three algorithms namely; LSTM, Bi-LSTM and a hybrid approach of combining Bi-LSTM along with PSO. For this reason; the author has gathered the dataset from Kaggle repository which contains the UNS-NB15 dataset pertaining to train and test csv files for the respective attack. Once the dataset is acquired, this data is loaded into the system model with specific libraries which are required to run it.

An approach of CRISP-DM methodology is used so that the issues of NIDS can be targeted and an effective mechanism can be built so as to achieve higher precision rates for threat modelling. The next stage of the study majorly involves exploration of the data traffic on the network so that the features of NIDS can be cleaned and pre-processed. The stage of data cleaning is primarily done so as to eradicate any null values from the dataset to avoid further hindrance during the training stage. On the other hand; data pre-processing ensures that the raw data from the dataset is efficiently transformed into a suitable format which can be fed to the DL based models. Data pre-processing is one of the most crucial steps that must be carried out so that missing values and outliers can be removed and normalization can be performed.

The next stage of the workflow involves the process of data visualization. This process is done so as to understand the bifurcation of balanced and imbalanced data. An imbalance in the dataset at the initial stages might result into decreased accuracy and increased run time. Hence this step is mandatory to comprehend the distribution of data. This process is done by plotting graphs and analysing the distribution of the same. Figure 4 below illustrates an imbalance in the dataset thus caused.

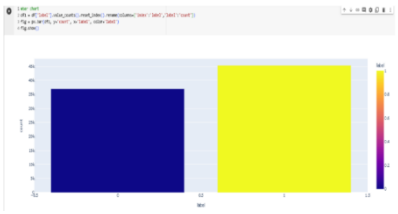

Figure 4: An imbalance of attack features in the UNS-NB15 dataset

On the other hand, figure 5 below depicts the distribution of attack data in the form of a pie chart.

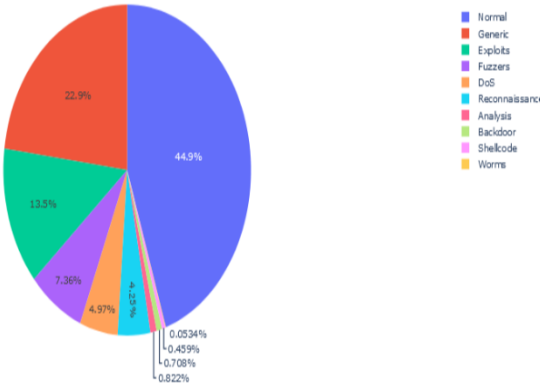

Figure 5: Data distribution of attack categories

A pie chart showing the distribution of data across different categories is shown in Figure 5. There are various segments in the chart, and each is represented by a different colour. The biggest portion, indicated in blue, makes up 44.9% of the entire set of data. After then, the green segment makes up 13.5% of the data, while the red segment accounts for 22.9%. In addition, a violet section accounts for 7.36% of the total data, an orange segment for 4.97%, and a third blue segment for 4.25%. The other segments in the chart illustrate the composition of the dataset throughout the different categories, with each segment contributing a specified percentage to the overall distribution.

Once the process of visualizing the data is executed; the next step of data train and test is done. For this purpose; the author has performed a data split of 80percent to train the data and 20percent to test the data. In the next stage; three DL based algorithms are used for the testing purpose and the algorithm with highest generating accuracy and precision factors is declared to be as the optimized model.

Figure 6 below portrays the architectural diagram of the same.

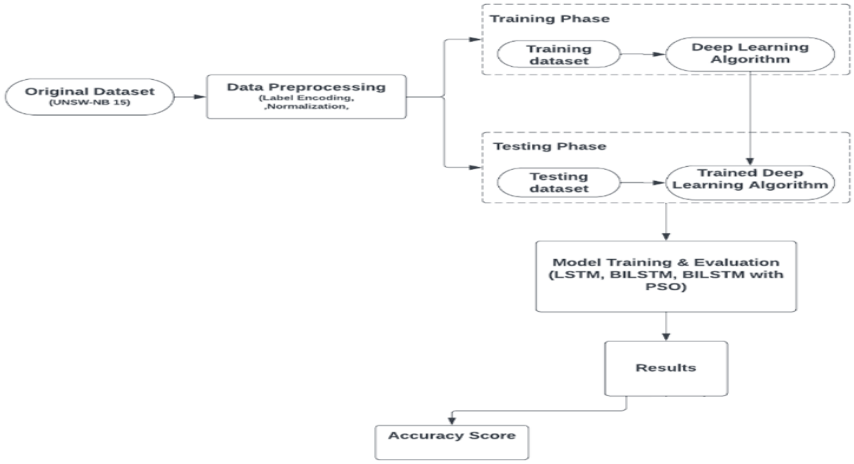

Figure 6: Architectural Flow of the Study

Results

This section of the study depicts the results thus generated using LSTM, Bi-LSTM and Bi-LSTM with PSO.

During evaluation, the LSTM model accurately predicted the intended output for almost 91% of the dataset, with an accuracy of about 90.75%.

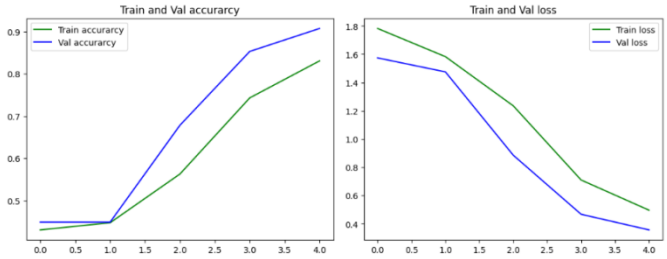

Figure 7: Accuracy Loss Graph of LSTM

With an astounding accuracy of about 95.11%, the BiLSTM model demonstrated its capacity to correctly predict outcomes for the great majority of the dataset .

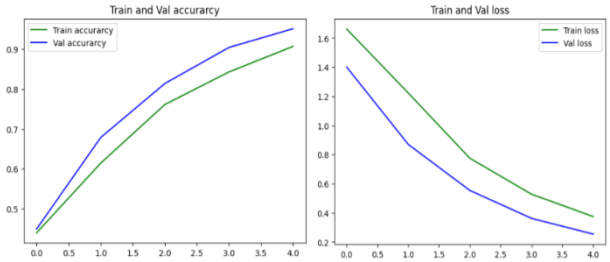

Figure 8: Accuracy Loss Graph of Bi-LSTM

The remarkable accuracy of the BILSTM PSO model was about 98.90%. Among other models, it performs better at predicting outcomes than any other model, as evidenced by its remarkable accuracy of 99%, which makes it the top model .

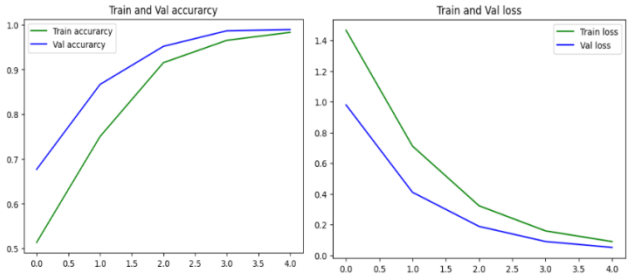

Figure 9: Accuracy Loss Graph of Bi-LSTM + PSO

The implementation process is made simpler by this model. It is still rather easy to integrate BILSTM with PSO using standard deep learning frameworks. Because it is so simple to use, a wider range of network security settings can be deployed more quickly by lowering acceptance barriers. The method shows potential in terms of scalability and adaptability to various network conditions. Variable sizes of attacks taking place on network traffic data are supported by its flexible architecture and dynamic PSO optimisation, which ensure constant performance as datasets grow. Our approach is positioned as a workable long-term solution that can handle increasing network complexities due to this scalability characteristic. Sustaining this model is compliant with industry norms. The architecture's modular design makes it possible to easily modify or improve it in response

to new threats or modifications to cloud network patterns.

Conclusions

The primary aim of this research is to identify the attacks that takes place and built a threat modelling system around it. For this purpose, the author has primarily focused on deploying a threat model based on NIDS that could detect the occurrence of threat and attacks by using the conceptual working of deep learning algorithms. LSTM, Bi-LSTM and Bi-LSTM along with PSO have been proposed and further implemented. The outcomes showed that BILSTM with PSO had the maximum accuracy of 99%, indicating that it might improve network intrusion detection. To examine the models' interpretability and pinpoint areas in need of improvement and optimisation, more research is needed.

References

[1] Sudqi Khater, B., Abdul Wahab, A.W.B., Idris, M.Y.I.B., Abdulla Hussain, M. and Ahmed Ibrahim, A., 2019. A lightweight perceptron-based intrusion detection system for fog computing. applied sciences, 9(1), p.178

[2] Pooja, T.S. and Shrinivasacharya, P., 2021. Evaluating neural networks using Bi-Directional LSTM for network IDS (intrusion detection systems) in cyber security. Global Transitions Proceedings, 2(2), pp.448-454

[3] Azeez et al., 2020 N.A. Azeez, T.M. Bada, S. Misra, A. Adewumi, C. Van der Vyver, R. Ahuja Intrusion detection and prevention systems: An updated review Advances in Intelligent Systems and Computing, 1042 (2020), pp. 685-696

[4] Latha KM. Learn about intrusion detection and prevention. USA: Juniper Networks; 2016

[5] Moustafa N, Slay J. Unsw-NB15: a comprehensive data set for network intrusion detection systems (UNSW-NB15 network data set). In: Military communications and information systems (MilCIS). Canberra: IEEE; 2015. p. 6

[6] Thaseen, I.S.; Poorva, B.; Ushasree, P.S. Network Intrusion Detection using Machine Learning Techniques. In Proceedings of the 2020 International Conference on Emerging Trends in Information Technology and Engineering (ic-ETITE), Tamil Nadu, India, 24–25 February 2020; pp. 1–7

[7] Kumar, K.P.M.; Saravanan, M.; Thenmozhi, M.; Vijayakumar, K. Intrusion detection system based on GA-fuzzy classifier for detecting malicious attacks. Concurr. Comput. Pr. Exp. 2021, 33, 5242

[8] Karatas, G.; Demir, O.; Sahingoz, O.K. Increasing the Performance of Machine Learning-Based IDSs on an Imbalanced and Up-to-Date Dataset. IEEE Access 2020, 8, 32150–32162

[9] Sarker IH, Kayes A, Badsha S, Alqahtani H, Watters P, Ng A. Cybersecurity data science: an overview from machine learning perspective. J Big Data. 2020;7(1):1–29

[10] Shaukat K, Luo S, Chen S, Liu D. Cyber threat detection using machine learning techniques: A performance evaluation perspective. In: 2020 International conference on cyber warfare and security (ICCWS). Islamabad: IEEE; 2020. p. 6

[11] https://www.kaggle.com/datasets/mrwellsdavid/unsw-nb15