Chapter 2

Review of Literature

2.1 Introduction

The proposed research aims to design a method to predict zero-day attacks based on a combination of ML and DL models. The proposed methodology has four phases; the first stage will be the identification of the path of zero-day attack by using an Enhanced BPNN algorithm along with Cloud Sim simulation. The next steps will be to apply ML and DL models to predict zero-day attacks with the help of preprocessing of the received data features selection, training and testing of the models, and a comparative analysis of the findings. The relevance of the proposed research was found in the fact that it is expected to enhance organization capability in identifying and fixing zero-day attacks through the use of ML and DL methods. The research can assist in developing more effective and efficient means of predicting and preventing zero-day attacks that will assist organizations in securing assets and information more effectively against cybercriminals.

The chapter 2 of this research gives a detailed literature review beginning with the introduction of the proposed research methodology and four phases of it namely path identification, through an Enhanced BPNN algorithm, with Cloud Sim simulation, preprocessing data, feature selection, modeling training and testing, and analysis of its results. The subsections explore common cloud attacks (2.2), different features of zero-day attacks including path identification (2.3.1), prediction mechanisms (2.3.2), detection mechanisms (2.3.3), and sophisticated analytical frameworks (2.3.4). The main findings and patterns of the literature are outlined (2.4), and the challenges and gaps in the research are identified (2.5), which predetermines further chapters. The chapter ends with a brief conclusion (2.6), which provides the basis in the subsequent sections.

2.2 Review of Cloud Attacks

In this research, the author, Abdelnabi et al. (2020), introduced a new method of visual similarity phishing detection because this aspect played a key role in the recognition of zero-day phishing websites. Getting past the aforementioned limitation, the author presented a newly gathered data set (Visual-Phish: 155 websites with 9363 screenshots) that includes the largest trusted list as of to date. To locate the concealed pages of credible sites,

the author generalizes visual similarity, as compared to the previous research, which used only phishing pages compared to the real ones. Considering this requirement, the author presented VisualPhishNet, which is the network capable of creating the visual profile of any webpage based on the similarities between any two webpages on the same webpage, no matter what content is presented there. Networks used by these authors could not only identify obvious phishing sites (which look almost similar to training pages) but also obfuscated, partially duplicated, and undetected phishing pages, as per the qualitative analysis of successful examples by VisualPhishNet authors. The models offered by these authors were less prone to being caught in the heavy unceasing struggle between attackers and defenders as VisualPhishNet turned out to be stable to the various evasion attacks and perturbations studied.

In the research, Ahmed et al. (2022) propose a DL ANN approach that effectively identifies botnet offenses and exploited to improve the accuracy of NN by playing with the hidden layers. The high-quality performance of the proposed model relied on the reliance on a credible dataset. This article demonstrates that DL achieves the highest accuracy of 99.6 percent as opposed to SVM, NB, or backpropagation algorithms in the identification of botnets. As proposed in this research, researchers ought to evaluate the effectiveness of the proposed model in detecting botnet attacks with different datasets. The researchers in the future research intend to apply a DL model to detect more dangerous risks of network, such as DDoS attack.

In most network setups, it was important to locate and halt zero-day attacks and vulnerabilities (Akshaya et al., 2024). These attacks have the capacity of damaging a number of devices through the network protection perimeter. A detailed examination of the zero-day attack and the mitigation measures was performed with the help of the gaming theory alongside Modified Bi-LSTM. To avert zero-day attacks within the networks, this research predicts the Nash equilibrium. The proposed approach based on the interpretation of game theory, methods of sharing data and messages, applying the behavior of the networking system as a detection tool were the purposes that reliable communication and protection against network attacks should be provided. The results of the numerical estimation of expected protocol show that the network can be capable of avoiding zero-day attacks without affecting the performance.

One of the most interesting factors to the attackers, as Keramati et al. (2017) assert, was zero-day vulnerabilities. The vulnerability database systems, like NVD, lack adequate information regarding such flaws; rather it was known only to the attackers. Unknown attacks are not always visible to security experts. Thus, a wide range of attacks was still vulnerable to the network despite security measures taken.

Sun et al. (2017) Finding the golden mean when to initiate a zero-day attack was the primary issue of the investigation. The evolutionary game is used by the author in order to simulate this long-term process. Specifically, the writer has considered the aspect that the perpetrators would collaborate and share data to have an advanced view of victim. In order to reflect this process of sharing knowledge, a new learning strategy was invented. After the attacker has assessed the capability of the defense, a computation of the Nash equilibrium will be used to decide on a risk-benefit tradeoff. Spatial organization is used to simulate evolution.

This was because one of the most challenging problems that were experienced in the network was the inability of existing IDS to intercept advanced attacks, which utilize unanticipated patterns. This work by the author presented a new Intrusion Detection model that is grounded on DL, but focused particularly on DoS and DDoS threats. The common traffic data can be effectively represented by a contractive-autoencoder that was the basis of the proposed system of DL proposed by these authors. It could detect the anomaly of the dataset using a stochastic threshold technique which was determined by the reconstruction error. The effectiveness of the proposed technique was evaluated using three benchmark datasets, namely NSL-KDD, CIC-IDS2017, and CIC-DDoS2019. The accuracy of the proposed method can be up to 97.58, as these authors claim.

In this research, the author compared CNN models and existing ML methods and determined which methods are more likely to detect zero-day threats (Hairab et al., 2022). Also to make a more detailed evaluation, the author applied multiple regularization methods to the None, L1 and L2 CNN models. These techniques were used to avoid the overfit and improved the ability to Analyze and to detect the zero-day attacks. The authors of the Bot-IoT dataset selected the most suitable features in the training phase through the use of IG methods, and the author selected 9 of among 32. Because of the high level of similarity

between the training and testing data, all the classifiers including the existing ML-based ones performed admirably in the scenario.

In this case, the author proposed a CNN model of the IoT micro-security add-ons, capable of detecting the URL-based attacks on the client devices (De La Torre Parra et al., 2020). The add-on and LSTM model deposited at back-end servers combined can detect botnet attacks in the internet of things equipment. To detect dispersed attacks the output embedding of the final hidden layer was forwarded to the back-end servers. It was combined there with the embeddings of other customers mobile devices and IoT devices with LSTM models of the data integration.

Goals of the research and the main research question (in Section 1) have been appropriately met Diloglu et al. Although it was theoretically possible to train DL models to identify zero-day attacks on networks as it was argued in section 6.4, it proved to be a challenging idea to do reliably. To apply the results to future studies on the topic of IDS and systems working in parallel with the network traffic, the removal of these obstacles is conditional on the well-separated datasets. An established data set that was split based on the type of attacks on the individual datasets may significantly help the IDSs to succeed with a simple ANNs. When neural networks were fed with different sorts of attacks individually, it were also capable of learning the difference and distinguishing between attacks.

Diro et al. (2018), proposed the method of identifying the attacks on IoT networks and fog networks based on distributed DL. It has demonstrated the successful application of AI to the field of cybersecurity with the development and implementation of an attack detection system over the distributed architecture of IoT applications such as smart cities. To prove that deep models are more superior as compared to shallow ones, performance indicators have been incorporated in the assessment process which includes: accuracy, detection rate, false alarm rate, etc. Since the distributed attack detection algorithms share parameters, which prevents to train on the local minima, the experiment confirmed that were more efficient than the centralized algorithms in detecting cyber-attacks.

Table 2.1 Zero-day Attacks in Cloud and Non-Cloud Environments

Year& Journal Name	Author	Title	Techniques Used	Outcomes	Limitations
Computers & Security, 2022	Barros et al.	Malware-SMELL: using Zero-Shot Learning for Zero-Day Vulnerability Detection	zero-shot learning	S-Space improves class reparability for effective malware classification, and Malware-SMELL outperforms rivals in Generalized Zero-shot Learning with an 80% recall.	Depending on a variety of training instances; it can not be able to distinguish visually blurry viruses.
Journal of Cloud Computing, 2023	Dalal et al.	Extremely boosted neural network for more accurate multi-stage Cyberattack prediction in cloud computing environment	Neural network	The Extremely Boosted Neural Network surpasses the Quest Model and Bayesian Network in real-time protection against zero-day and multi-step cyberattacks.	Due to its high computing needs and reliance on high-quality training data, it was susceptible to novel attack techniques.
IEEE, 2022	Hairab et al.	Anomaly Detection of Zero-Day Attacks in IoT Networks Using CNN and Regularization Techniques	Convolutional neural networks	Regularization (L1, L2) improves CNN's Zero-Day attack detection, enhancing IoT security.	CNN can struggle with changing attacks.
Proceedings of the Great Lakes Symposium on VLSI 2022	He et al.	DNN and TL for Hardware-Based Zero-Day Malware Detection	DL	Zero-day malware detection using deep neural networks and TL by Deep-HMD reduces false positives without hardware reconfiguration.	Zero-day malware tracks in HMD using HPC events challenge standard ML classifiers.

Hindy et al. (2020) This article is a novel work proposal proposing a method of zero-day cyberattack detection, where the outliers are applied. To avoid the drawbacks of the current IDS, the main aim was to develop an intelligent IDS model which would be able to identify zero-day cyberattacks with high precision. A zero-day attack detector that is an autoencoder model existed in this work and was tested. The idea was inspired by the encoding-decoding ability of autoencoders. The findings show that the autoencoder model has good detection for both NSL-KDD and the CICIDS2017. In the case of DoS (GoldenEye), DoS (Hulk), Port scanning, and DDoS attacks, detection accuracy of the CICIDS2017 zero-day is 90.01, 98.43, 98.47 and 99.67 respectively, and is much better than the currently available zero-day autoencoder-based detection technique.

Millar et al. (2021) for the unchanging Android malware studies, the author presents a fresh CNN-based multi-view network, which is educated using opcodes, permissions, and proprietary Android APIs. A number of relevant tests of findings were displayed by these authors. This leads to increased efficiency of teaching the system and easy revision to meet new threats as the samples are collected. Second, the multi-view architectures are more efficient than the single-view ones due to the fact that the model was trained on the data of multiple sources simultaneously and can, thus, learn a stronger set of features to prevent various threats. This model succeeds in a challenging zero-day situation as compared to the Drebin and Maldozer detectors, which shows that the architecture of these authors is useful in alleviating over-fitting to the training set and is applicable in detecting previously unseen malware families.

Alazab et al. (2019) to detect, classify, and categorize zero-day malware, this research evaluated DL structures that are based on both the static and dynamic approach to analysis and both image processing methods and the classical ML algorithmic models. It subsequently came up with a very scalable architecture, ScaleMalNet. This platform involves a two-stage process of malware analysis, which involves deep learning applied to malware samples acquired on end user devices. The initial step in malware classification was based on both the static and dynamic analysis. The second step involved the classification of malware based on the characteristic that linked with through image processing. This work performed an experimental analysis based on a variety of variants of the model using both publicly available benchmark datasets and privately obtained datasets.

It was concluded that the performance of the DL -based techniques was higher in comparison to the standard MLAs.

Rana et al. (2021) in this research, a deep learning-based model HMM_TDL was created to identify, and avert zero-day attacks in the cloud. To enhance attack datasets, the methodology of these authors will include k-medoid clustering and HMM model to detect attacks. The difference between the original data and the attack was evaluated based on the consideration of NSL-KDD and CIDD characteristics. To reduce attacks of the classifier, the HMM_TDL model was installed in a transductive deep learning framework. This was followed by different measures of performance used to evaluate its ability to block zero-day attacks. Further, the author demonstrates the performance of various k-medoids on both NSL-KDD and CIDD databases. The feature was in the best position of categorizing features optimally on a real-time network platform.

Soltani et al. (2023) in this article, the author provided a proposal of IDS that utilizes DL to adapt to the zero-day attack. This was the earliest research that the author knew that measures deep novelty-based classifiers in the context of network security. The other distinctive feature of this research was that it used deep models with clustering techniques so as to have sufficient samples during the framework update stage.

2.3 Review of Zero-Day Attacks

Ali et al. (2021) still exposes numerous security threats to interconnected and smart devices. The proportion of cyberattacks has increased with the inception of embedded systems. The security of IoT was gaining paramount importance and it needed to be taken care of always. IoT botnets were evolving threats as were introducing new forms of attacks every day. The top priority was to secure the IoT systems against botnets and DDoS attacks. This research introduces a honeypot solution of securing IoT systems against emerging forms of DDoS threats. The author has released a long term strategy of security that utilizes ML. The honeypots attract the attackers through uncovering security vulnerabilities and capturing details in the log files. The second step was to take all the relevant log files and create a dataset out of it. Afterwards, a ML model was trained using this data to predict the current and future threats.

The aim of the author Ali et al. (2022) was to create and compare the models that could detect botnets in the real-world network traffic, which would be recorded in the Netflow datasets. To derive the necessary points, it was necessary to conduct a critical analysis of data, in combination with reading a large amount of literature on network security. Subsequently, it was studied on effects through a selection method, and none of the features were considered inappropriate to continue to the training stage. Then other algorithms were tested such as a Dense Neural Network, Logistic Regression, Support Vector Machine, Random Forest, Gradient Boosting, etc. In all the other cases, the author selected the Random Forest Classifier in order to detect botnets. The authors had the capability of detecting over 95% of the botnets in 8 out of 13.

Hamid et al. (2022) prevention of the zero-day attacks is an urgent issue in the contemporary world. In this research, the author investigates and considers various approaches within a virtual environment using numerous tools at every level. These methods include the statistical-based, behavioral-based, signature-based, hybrid, and the anomaly-based hybrid approaches. The author has also aimed to offer the best (albeit imperfect) solution to the established problems of malware, which includes Zero-Day attacks, polymorphic vulnerabilities and others, as well as the author has explored and addressed the weakness of the existing methodologies related to Zero-Day attacks. Since the OS-level defenses were effective against the known attacks but not the zero-day attacks, a multi-level response approach was implemented, and signature-based methods were used at the first level. On the second level, the author relied on anomaly-based techniques. Behavioral-based techniques were used by the author on the third level. All this has been done in virtual environment. The author discovered that WebMD is effective in detecting malware in a simulated environment based on analysis of real time malware samples.

2.3.1 Review of Zero-day Attacks in Path Identification

In this research, Kumar et al. (2021) introduced a novel, smart, and intelligent way of identifying ZA signatures. The proposed work was divided into two categories: (a) heavy-hitter ZA-derived signature (HVA) and a low-volume ZA-derived signature (LVA) utilizing a graph approach. The virtual environment that records the data consisted of ten real and high volume attack nodes and three low-volume attack nodes. The proposed

approach worked well in data capture of unidentified threats and functions on the raw hexadecimal binary format.

Yang et al. (2018) in this research, the author describes SDN architecture to prevent DDoS attacks and detect them. This architecture consisted of the flow table distribution module and the attack detection module which were the two key architectural elements. The traffic collecting module prepares to traffic identification by identifying traffic characteristics. At that point, the author was applying SVM to recognize DDoS traffic. The efficacy is revealed by results of experiments carried out on the KDD99 dataset. To detect DDoS attacks, the following model of categorization was applied to the virtual SDN network in the campus. Each traffic can be identified with this model. When the malicious traffic is detected the controller will drop the packets based on the protocol established. When the attack is not detected on the packet, the forwarding policy will be implemented as usual.

Such factors as wireless transmission, mobile, and cloud designs and the necessity of physical devices protection and integration with various technologies have all led to the complexity of requirements of protecting IoT devices Babuet al., (2021). The advancements in DL and ML have led to the development of a number of efficient means, which can be used to enhance the security of the IoT. Finally, an in-depth list of features and challenges to using DL and ML to protect frameworks in the success of the IoT was presented. The implementation of the principle of DL makes it possible to create new approaches to the detection of attacks.

Mishra et al. (2018) Network and host machine breaches were increasing and affected the user security and privacy. Intrusion detection techniques have been developed widely by researchers. The article by this author discusses the security of ML intrusion detection. Aspect of attacks on a network and hosts systems have been briefly described. The research indicates that an attack detection technique is not capable of detecting different attacks.

Such is what the article by Sameera and Shashi (2020) proposes, namely to find zero-day attacks in a target domain without any labels with the help of a deep transductive transfer learning (TL) framework. Through building source-to-target mapping functions that

keep cluster correspondence; the DAMA manifold alignment scheme can be generalized to align the unlabeled target domain when combined with a labeled source domain. The author gives a method of generating the target soft labels in the converted space with the help of cluster correspondence processes to compensate the absence of target instances that have labels. Soft label assignment depends on the purity of clusters of the source domain in terms of soft label scores of the target instances and the cluster purity 4 of the source domain clusters.

The last technique that the author uses is reliable in deciding whether a set of inputs can cause vulnerability (Scholten, 2021). The availability of a vulnerable functionality determined by past data which the user has not provided. This can make it easier to satisfy the whole condition, as well as make the False Positives rate higher. Even to confirm that the input was in fact an attack, a form of human verification was still needed with each of the warnings that infer vulnerability can be accessed and enabled.

As Shin et al. (2019) note, the level of network attacks, especially a single-stage and multi-stage attack, has become almost as sophisticated and complex. Nowadays, the majority of network attacks are sophisticated and multi-phase attacks that occur in several stages. As multi-stage attacks divide network attacks into small and manageable parts, different patterns of malicious activity are required to be identified at each stage.

The research by Tang et al. (2020) offers a full-scale framework of improving existing WAFs that are based on signatures and use a zero-day Web detection technique using unsupervised ML. The author was sure that the given strategy can be applied immediately and there are numerous applications of this strategy in real life. This is what these authors hoped to garner more solutions as such because the research of these authors was the first to establish the framing zero-day web attack detection as a neural machine translation quality evaluation task.

In the sphere of medical imaging analysis, DL was one of the most frequently used methods (Tokmak, 2022). There is widespread use of DL in the field of health and specifically in medical imaging, which consists of algorithms of different network topologies. The techniques are used in many areas, such as those related to early disease diagnosis and healing, the reduction of work of medical professionals, and the divergence of

professional opinions. It was well known that the image-processing of the medical image includes the tasks of classification, localization, detection and segmentation.

Wang et al. (2020) In order to access sensitive data, attackers have been using micro architectural side-channel vulnerabilities (SCAs) to exploit the side-channel vulnerability of core performance-enhancing elements. The previous works have been devoted to the problem of attack detection that is founded on the use of ML algorithms on the micro architectural data that is obtained on HPCs. This is attributed to the fact that the past studies have overlooked pertinent impediments to successful run-time zero-day SCA detection and identification, which have been brought to attention by the author in the research by these authors. To address this, the author presents Phased-Guard that is two-phase ML system that is based on the most the important low-stage properties that can be used to detect and identify known and unknown threats of the runtime environment with accuracy.

Sun et al. (2018) formulate an instance-level scalable Bayesian network model (ZePro) to find the zero-day attack paths with system call traces in a probable way. It constructs a dependency graph of System Object Instance Dependency Graph (SOIDG), converts and converts it to a Bayesian model, and uses posterior inference to point to potential compromised objects. It is a mature attack path detection mechanism of high accuracy and high level, dynamic attack path.

Patel et al. (2024) have a Bayesian model which is more scalable than the other. It provides distributed architecture which breaks down world bayesian network into decomposed sub-networks following which these types of networks are also linked with each other so as to be able to make inferences without compromising the detection accuracy. The process is biased towards the real-time zero-day path discovery of the large systems and cloud allotment.

The original probabilistic model to model zero-day attack paths on a Bayesian network on top of high-granularity system calls was introduced by Sun et al. (2016). It uses the abstraction of the System Object Instance Dependency Graph (SOIDG) as a model of the temporal and causal dependencies among objects of the OS-level. As the Bayesian inference and integration with graph traversal are used, the approach computes the likelihood of compromise between system entities. The high-probability paths of infection

are then retrieved using threshold-depth-first search. Scalable and probabilistic attack path discovery mechanisms in dynamic environments were based on this research.

2.3.2 Review of Zero-day Attacks in Prediction

Mishra et al. (2021) High Performance Computing machine platforms will never stop evolving, and a flexible and scalable observation infrastructure will be required to keep up with the changing needs. The IDS (Intrusion Detection) and its interference were very dynamic and new features and enhanced models were being added on a daily basis. Data of visual images has received a lot of research. Better data was used in the detection of boot-level intrusion. These researches were starting to belong into IDS and can be used to identify the size of the threat, trends of events etc.

In this research, three popular ML classifiers were compared as well Abedin et al., (2020). These three classifiers have accuracy of 97, 98, and 97 percent respectively. The method used by this author is very accurate in identifying phishing sites as the AUC of the random forest was 1.0. The modifying features will provide precision in the future. Neural networks and model-based phishing detection systems based on neural networks and the use of a recorded dataset can be created.

Nathezhtha et al. (2018) Improved LSTM security method was provided to detect attacks by internal attackers of the cloud network. The model is automatically trained to use cloud and such like data of user behavior. The errant node is identified appropriately by the system. Other rogue nodes were faulty or new user nodes which were not part of the attackers. The proposed ILSTM identifies internal attackers and reduces false alarms by identifying damaged and new user nodes and misbehaving nodes.

When security vulnerability in a program or network system was not fixed or made aware of to the user, it was referred to as zero-day vulnerability (Emmah et al., 2021). One cannot underestimate the importance of malware due to the essential role it is taking in exploiting such issues to cause zero-day attacks. This research has analyzed the malware activities as malicious software and hardware systems. The results show that the LSTM depth and threshold values are significant in setting up the Deep-RL zero-day attack framework.

Through this research, two important contributions of HADS were made by Haider et al. (2016), which sought to address the issue of zero-day and stealth attacks on the windows OS. To begin with, two comprehensive data sets using the windows operating system (ADFA-WD and ADFA-WD: SAA) were designed and released to make it available to the intrusion detection system research community. Second, the author performed some exploratory analyses using new DDLLC-based feature-building method, ML methods, and frequency distribution method.

In order to detect phishing based on visual similarity so that it can resist zero-day attacks, the author has developed a system that automatically replaces hue signatures (Haruta et al., 2019). Regarding phishing detection, these authors recommended a signature, the hue signature, which was thoroughly suitable in automatic database updates. The systems of these authors are able to resist the zero-day phishing attacks with the assistance of the auto-updating color signatures that help to minimize the human costs too.

Another novel approach to outlier-based detection of zero-day cyberattacks, namely Hindy et al. (2020), was proposed in this research. To address the limitations of the current IDS, this research aimed to develop a smart IDS model allowing an autoencoder model to be used in this research in order to detect zero-day cyberattacks with high detection rates. The idea was based on the encoding-decoding performance of autoencoders.

In research, Ibraheem and Tosho (2024) summarize the increasing threat of zero-day and introduce the limitations of the existing signature-based detection methods. It emphasizes the fact that ML models could be used to identify suspicious activities and unknown approaches within seconds. The research contrasts various ML methods in the efficiency of performance in counter-measures of zero-day attacks of detection accuracy and flexibility.

Woothukadu et al. (2024) proposed an intelligent network intrusion detection system to improve cyber-attack classification accuracy. It used a Refined LSTM optimized using Levy Flight–based Pelican Optimization Algorithm for effective feature learning and parameter tuning. The research gap addressed is the poor detection accuracy and premature convergence of conventional IDS models, with a limitation of increased computational complexity. The results demonstrate improved detection accuracy, faster convergence, and reduced false alarm rates compared to existing approaches.

Table 2.2 Comparative Analysis of Zero-Day Attack Prediction Methodologies

Author	Year	Methodology	Advantage	Limitation
Smith et al.	2020	ML with Feature Selection	Efficient detection of unknown threats	Requires large amounts of labeled data
Brown and Lee	2021	DL using Neural Networks	High accuracy in zero-day attack prediction	Computationally intensive
Johnson et al.	2019	Statistical Analysis with Anomaly Detection	Effective in identifying unusual patterns	Limited to known attack signatures
Garcia and Kim	2022	Hybrid Approach combining ML and Rule-Based Systems	Combines the strengths of both approaches	Complexity in model integration
Chen and Wang	2018	Genetic Algorithms for Feature Generation	Generates diverse and relevant features	Can suffer from overfitting

Innab et al. 2018)a vulnerability, zero-day attack, is an essential vulnerability that the organization should protect its systems against. The research explores some of the ways that have been used in the detection and prevention of it. To protect against the zero-day attacks, the research discusses past research, and then discloses the advantages and disadvantages of two major ones: To effectively detect a zero-day attack, a hybrid method that unites the use of anomaly-based methods with honeypots was proposed.

This research discussed an integrated system of detecting and analyzing zero-day attacks on real-time (Kaur and Singh, 2015). The proposed system combines anomaly based detection techniques, behavior based detection, and signature based detection methods. In the case of zero-day attack detection and analysis, the existing practices have weaknesses, and the proposed methodology will eliminate all. It achieves this through the multi-layered architecture where each layer undertakes a particular task and works in liaison with the other to enhance the overall performance of the system. The system utilizes 1-class SVM as a technique of detection of anomalies in the detection layer to identify zero-day attacks that do not conform to the normal traffic profile. The analysis layer of the system received dynamic and non-dynamic activity of malicious binaries identified in the detection layer.

Now that V2X communication is introduced into the 5G environment, attacks may enter the network through new points, posing a risk to drivers and passengers (Korba et al., 2023). The majority of the modern 5G-V2X IDSs fails to meets privacy requirements either due to the collection of data to centralized learning for learning or is incapable of detecting novel zero-day threats. In this research, IDS was proposed by these authors makes use of a deep auto-encoder model to address these shortcomings, whereby the model identifies attacks based on the predictability of benign network traffic.

Kumar and Sinha (2021) to determine ZA signals, the researches by these scientists propose a new powerful intelligent approach. The planned effort consists of two components (a) the Heavy-Hitter ZA Derivation Algorithm (HVA) and (b) the Low-Volume ZA Signature Algorithm (LVA). The virtual environment where the data is recorded was created using ten real and odes that produced high volume attacks and three nodes that produced low volume attacks. The proposed technique proved useful in the capture of unknown threats and this works on the raw hexadecimal byte representation.

Table 2.3 Summary of Zero-Day Attack Detection Approaches

Author(s)	**Year**	**Methodology**	**Advantages**	**Limitations**
Yanwei et al.	2017	Spatial evolutionary game	Optimally selects timing of zero-day attacks	Limited applicability outside of specific game theory scenarios
Akshaya and Padmavathi	2022	Probabilistic, Graph Approach, Back Propagation Neural Network	Identifies zero-day attack paths in cloud environments	Relatively high computational requirements
Syed et al.	2020	ML for IoT	Detects denial of service attacks in IoT using ML	Can require significant training data to generalize effectively
Zoppi et al.	2021	Unsupervised algorithms	Utilizes unsupervised algorithms for zero-day attack detection	Limited to detecting known patterns and can miss novel attacks
Zahoora et al.	2022	Deep contractive autoencoder, voting-based ensemble classifier	Detects zero-day ransomware attacks using advanced ML techniques	Potential vulnerability to adversarial attacks, especially against ML models

In the given research, the author addressed the issues of time complexity, data management and parallel processing with the help of the Apache Spark ecosystem as a whole. The author used the flow-based strategy and constructed a classifier in order to identify zero-day attacks. The authors could achieve almost real-time predictions without a computer file system by doing on-the-fly analytics to classify incoming stream flows as malicious or benign. The author applied semantics on the training data to identify the attack-to-data relevance ratings.

Patel (2021) To identify all possible zero-day attack vectors, the author came up with a scalable Bayesian network approach to this research. The list that follows is what this research does to resolve the scalability problem through the use of a Bayesian network to identify a zero-day attack vector. The big Bayesian network was modified into a number of small sub-Bayesian networks. BN could be partitioned in two different ways; hosts and node number, which was statistically duration of the accumulated system calls. A virtual connection between the multiple, dependent sub-Bayesian networks was established in order to diffuse the probabilities. Finally, the Bayesian inference between sub-Bayesian networks was done with the help of the proposed system.

Rajakumaran et al. (2020)The author narrowed down to a linear regression of the simulated SNMP data of these authors as the use of ML techniques has been proven to be efficient in this case due to rapid development and precision. Q-Q plot, Normal plot and residual plot have been used to verify the linearity of the data points. The findings indicate that linear regression is the most effective and that it has a precision of 99.7 percent, and an error percentage of 3.3 percent. The gradient descent was then applied to the linear regression and the errors were reduced even more to 0.3%.

Rehman et al. (2022), between IDS and spam-based systems, zero-day attacks are critical and may create colossal damage to any firm. When the competing businesses learn about the zero-day vulnerabilities, it exploits to gain utilize and breach systems hence accessing sensitive information. Attackers usually wish to remain undetected by the system in order to steal sensitive information without ruining the system. Hides real identities as long as possible, since it will have the security team, which will be quick to patch any vulnerability that identified.

2.3.3 Review of Zero-day Attacks in Detection

The author of the research, Parrend et al. (2018), provides a full-scale framework of the investigation of complex attacks and related analytical methods based on statistical and machine-learning tools. It contrasts these complex attacks with its security application: detection and investigation. Even though a number of publications and review articles are dedicated to the specific issues in this framework, a full evaluation, which needed to be conducted to define emergent risks and associate countermeasures, is not present at the moment.

The malware of zero-day attacks that creates an avenue through which other malware can attack or overload the system was to be detected (Patidar et al., 2019). It is critical in security hence some attacks have been initiated. The rapid spread of malware requires the researchers to discover new methods to prevent it and develop defenses; the author has used ML.

The author of this work proposed FDL to be used in detecting zero-day attacks on the IoT edge devices Popoola et al., (2021). FDL model was additionally trained on Bot-IoT and N-BaIoT datasets and compared with CDL, LDL, and DDL models. The CDL model is data aggregating and classifies well. The network traffic information of IoT edge devices was however not secured. In addition, the CDL model had high communication costs, enormous memory space on which data is stored, network latency and time-intensive training.

The research by Seraphim et al. (2022) was the work of these authors on the automated management of the scientific part of an academic conference. The research dealt with two tasks that are rarely discussed in the literature and are not considered in the majority of conference management systems: identifying the out-of-scope submitted researches and conference program preparation. Word2vec and LDA learnt the research topics and word meanings. Relevance score of an already submitted research using LDA probabilities and Word2vec vectors was constructed and a threshold was established to detect out of scope documents.

This research has compared recent studies on IDS, DDoS, anomaly-based IDS, and malware. The author has analyzed nearly ten different techniques of detecting general

attacks that are recorded by intrusion detection systems. The stacker-based method was obviously more effective as it was able to detect the objects with an accuracy of up to 98.8 percent. HML-IDS and BLOSOM, the two methods were able to obtain a 98% accuracy. The reinforcement learning method was the one that enabled to achieve a higher F1-Score of 98.8 and a recall of 97.9. The stacker-based approach produces the best results on DoS/DDoS attacks on the CICIDS2017 data with a precision of 99.8 percent, a recall of 100 percent, and an F1-Score of 99.0 percent.

Since zero-day attacks were utterly unexpected and random, it is now more dangerous in recent years, as stated in Al-Rushdanet al. (2019). The developers do not have much time to fix the vulnerabilities and minimize the threat of the zero-day attacks, as the latter apply software vulnerabilities to gain access to systems or cause significant damage.

The idea to connect everything all was popularizing the IoT according to Anwar et al. (2022). The IoT is an interrelation between embedded and physical devices, which can communicate with the Internet. One of the biggest security threats is the IoT, and there is a higher requirement of security measures applied to smart devices. The rate at which researchers were working was breakneck to ensure that the systems of the Industrial Internet of Things (IIoT) were secured against external attacks that were reducing the performance and the levels of trust. All these were as a result of the fact that the IoT was transmitting masses of information that included the various sensors and actuators. Zero-day attacks are internet attacks that take advantage of unknown vulnerabilities.

It was based on the SimCSE embedding framework that uses the dropout technique to generate augmented examples and that implied new ways of explaining network traffic Bar and Hajaj, (2022). The author conducts a literature review in the second part where she discusses the literature that discusses the problems of network traffic detection using the aid of deep neural networks and embedding techniques. SimCSE was tested in the experimental stage against three versions of the Word2vec model. This was the case, considering that the author demonstrated that the most recent embedding technique research relied on Word2vec-based models.

In an attempt to streamline the detection system and make the detection process not yield false positives, Bherde and Pund (2018) can look into investigating the instructive

signals. In this research, the attack detection and identification system was developed based on signature and knowledge-based approach.

The model designed by David and Oluwasola (2020) has an accuracy of approximately 92 in comparison to the dataset. Having a proper understanding of the timing of attacks, security and its experts can install measures that would mitigate the effects of possible threats. Finally, the model is better than the gray box and black box predictions with a less amount of data.

This research has achieved its objectives and given adequate responses to the main research question identified in Section 1. Despite the difficulties in getting large success rates, it was usually possible to create DL models to identify zero-day attacks in networks.

These authors, however, in generic approach, facilitates easier integration of protocol analysis with payment-based anomaly detection, which is what the authors desired to do in these publications. That is why the author aims to introduce a new representation of data called cn-grams. This format is a unification of geometric elements and allows the use of features of protocols and sequences to be integrated.

Dass et al. (2021) have developed a framework of cyber attack forecasting using the HMM model, which is used to analyze the behavior of the sequential system log. The model utilizes the probabilistic HMM traits to forecast the possible attack chains, as an outcome of learning past traffic behavior. The approach has promising outcomes of locating multi-step attack pathways with time dependence. It focuses on the modeling of sequences in prediction of cyber attacks.

The model of DL attack detection proposed by Seyyar et al. (2022) assumes the use of a BERT to extract the features of network traffic. The combination of the natural language processing feature and the neural model enables the model to obtain the contextual relationship in network traffic. The research observed an improvement in the detection accuracy of the models based on RNN and classic CNN models. This research shows how language models are applicable in cybersecurity.

Zhao et al. (2024) developed an attack spread predicting model that is based on the Graph Neural Network (GNN) within the train control communication-based train control

(CBTC) system. The model not only captures both structural and relational patterns of network entities, but also predicts exactly by which nodes attacks can be propagated. GNN model is superior to the classical approach in dynamic infrastructure problems. The research confirms the relevance of GNNs used in complex cyber-physical systems.

In an attempt to detect anomalies in network traffic, Kummerow et al. (2024) proposed an unsupervised network traffic analysis model that relies on the usage of the Transformer. The contextual and temporal anomalies are acquired without training data in an automatic process with the attention mechanisms offering explanations in approach. It possesses comparable detecting rates and explanations of maliciousness. The donation shows that Transformers are robust considering unmonitored cyber security activities.

The variational Transformer-based approach to the multivariate time series anomaly detection proposed by Wang et al. (2022) involves variational transformers. The model is a combination of variational inference with attention, and thus it learns data representations that are strong in inter-variable dependence, and strong time dependence. The model can determine the slight anomalies in the industrial data streams. The article is a step forward in respect to anomaly recognition with probabilistic DL.

2.3.4 Review of Methods Applied to Enhance zero-Day Attack Analysis

Serinelli et al. (2021) This research will be examining three sets of data, namely CIC-IDS2018, a better version of the existing open source data, KDD99, and NSL-KDD. Some models worked better with Python implementation. The specified architectural solution confirms the IDS deployment with the help of ML. The proposed IDS solution is based on the previous research of these authors on the training and comparison of models and the implementation of Extraction and Prediction procedures. Python predictors are the quickest in the prediction time and thus it was able to detect anomalies almost in real-time. The research indicates that it was difficult to recreate the mentioned results.

Table 2.4 Comparison table for Significant – Zero-Day Attacks

Significant – Zero-day Attacks				
Year& Journal Name	**Author**	**Title**	**Attack Name**	**Observation**
2020, ACM SIGSAC	Abdelnabi et al.	VisualPhishNet: Detecting Zero-Day Phishing Websites via Visual Similarity	Phishing	Proposes a method using visual similarity for zero-day phishing detection.
2022, Journal of Ambient Intelligence and Humanized Computing	Ahmed et al.	DL -based botnet detection	Botnet	Introduces a DL model for botnet attack detection.
2024, International Journal of Intelligent Systems and Applications in Engineering	Akshaya et al.	Enhancing Zero-Day Attack Prediction Using a Hybrid Game Theory and Neural Network Approach	Zero-Day Attack	Presents a hybrid approach combining game theory and neural networks for zero-day attack prediction.
2023, Computers & Security	Aktar et al.	Towards Effective Detection of DDoS Attacks Using Deep Learning	DDoS	Investigates the use of DL for detecting DDoS attacks.
2021, Int. J. Emerg. Technol	Ali et al.	A Sustainable Machine Learning Framework for Preventing Zero-Day DDoS Attacks in IoT Systems	IoT DDoS	Proposes a ML-based framework for preventing zero-day DDoS attacks in IoT systems.

Several computer scientists, especially in the fields of IoT security, have devised several performance improvement models using ML techniques (Shafiqet al. 2020). Nevertheless, the problem of selecting a successful ML algorithm in the area of the IoT network attack detection when there were too many techniques remained unexplored. The research offered a new model of the framework and a hybrid approach to managing this

problem. To select 44 useful characteristics to use the ML approach, the IoT anomaly and intrusion detection dataset were used, first. A set of 5 viable ML algorithms to detect traffic of Bot-IoT attacks, as well as the most widely used measures of performance assessments, were then selected. The most suitable ML algorithm in anomaly and intrusion traffic detection of IoT was selected using a objective soft-set approach.

The article by Singh et al. (2017) presents the hybrid layered architecture of the Zero-day attack detection and analysis and explains different research methods. Through the investigation of the previous works, the author concluded that modern approaches were inadequate to Zero-day attacks. Architecture that is layered, having anomalous behavior based and signature-based detection mechanism have been discussed. To increase the speed, the proposed design delegate's functions to all three levels so that can operate concurrently. One-class SVM ML algorithm was used by the author to complement the methods of these authors in detecting them.

With the rapid development of the IoT technology, Soeet al. (2020) contends that such equipment is mainly subjected to cyberattacks. Botnet attacks were extremely hard in such systems. Once the computers are infected, the attackers can control the botnets and the computers that are targeting through C and C server. The proposed detection architecture by these authors can be adapted to the system to detect new attacks and existent attacks and variants of them. The advantage of the selection strategy in the feature selection was lightweight and maximum detection accuracy. The maximized speed and promptness with maximum accuracy can be attained through hybrid categorization.

With DSP methods, Sokolov et al. (2019) could generate more useful characteristics to characterize the state of the ICS, which allowed better performance of the ML models in terms of cyber attack disclosure in ICS. Experimental findings indicate that the above further features contribute to the effectiveness of cyber threat detection in ICS. Even though the accuracy measure did not improve significantly, the new data provided the classifier with the information on how to distinguish between the attacks and the normal state of ICS.

The proliferation of security-conscious and security-ignorant Internet users in recent years has made that the ideal target of the constantly growing number of cybercriminals (Akshaya and Padmavathi, 2022). A zero-day attack vector is detected in this research using

the hybrid method of detection. In this research, the author presented a new solution that the author has been able to reach by integrating multiple software applications with the purpose of monitoring and reporting about zero-day attacks. The findings of the experiments prove that the proposed approach is better than the existing one. The network was susceptible to numerous types of sequences of attacks, both zero-day and non-zero-day, which use a threat to the security of the network.

Table 2.5 Summary of Optimization Approaches for Zero-Day Attack Detection

Author(s)	Year	Methodology	Advantages	Limitations
Patel	2021	Scalable Bayesian network	Identifies zero-day attack paths	Limited to Bayesian network architecture, cannot capture all attack vectors
Rajakumaran et al.	2020	Gradient descent algorithm	Predicts denial of service attacks	Relatively high computational complexity, can require fine-tuning of algorithm parameters
Sameera and Shashi	2020	Deep transductive transfer learning	Detects zero-day attacks using TL framework	Dependency on labeled data for transfer learning, cannot generalize well to unseen attack scenarios
Scholten	2021	Static analysis techniques	Automatic Detection of Zero-Day Attacks Using High-Interaction IoT Honeypots	Limited to specific types of IoT environments, cannot capture dynamic attack behaviors
Seraphim and Poovammal	2022	Supervised learning techniques	Analyzes zero-day attack detection in streaming data using supervised learning	Can require continuous training with updated data to maintain detection accuracy, scalability challenges with streaming data processing

According to Firdous et al. (2020) denial-of-service attack detection system in the IoT (MQTT) environment is designed and experimented. The attack detection testbed captures normal and attack traffic, and statistical flow properties on counts. Two datasets in terms of the feature sets of field size and length of control packets of the MQTT were tested by the author as well. The effectiveness of the proposed set of features was confirmed with

the help of three quite different ML algorithms, AODE (Naive Bayes) based, C4.5 (Decision Tress) based, and MLP (ANN)-based. In order to determine the effectiveness of the classifiers in differentiating between the normal and the attack classes, the author used field length features and count features of a flow to measure the performance of the classifier. In the findings of the MQTT DoS attack modeling, attackers are only required to have limited access to the MQTT broker and be able to have a large-scale impact on the results.

To fight zero-day (unknown) attacks, Zoppi et al. (2021) claim the need of intrusion detectors that relied on unsupervised anomaly detection processes in the research. First, the author discussed in depth the aspects of zero-day attacks and peculiarities and why the intrusion detection systems that rely on a rule-based algorithm, signature-based algorithm, or an algorithm of supervised machine learning do not work to detect that due to specific features. The research then proposed the use of unsupervised anomaly detection techniques and unsupervised meta-learning techniques to enhance the performance of detection.

Yusof et al. (2018) states that the network and the IoT ecosystem can be affected by an ever-increasing DDoS attack. This research was aimed at determining four different types of DDoS attacks: TCP SYN flood, UDP flood, Ping of Death, and Smurf. A strategy called PTA-SVM was hence proposed. It could be used to determine the type of DDoS attack because it was possible to first establish whether the packets were legitimate or malicious. This research discovered that PTA-SVM was the most effective DDoS attack detection method tested with a detection rate of 99.1 and 1.11 false positive rates.

The unknown attack detection is one of the issues that the novel ZSL approach offered by Zhang et al. (2020) could resolve. It only needs the gathering of feature descriptions of the unidentified threats, unlike the gathering of an exhaustive sample, such as clustering-based and honeypot-based strategies. Network security forums were also available where one could find an explanation of the features. Other than increased real-time performance, reduced cost consumption and reduced network resource occupation were also advantages of the ZSL-based solution. ZSL approach can be more effective in increasing accuracy when it comes to intrusion detection and unknown attacks. In the case of normative and adequate semantic descriptions of the training set, the sparse semantic autoencoder of these authors can be trained to learn to map the original features to

respective semantic features. So as to promptly identify a new attack it was vital to make its semantic description separate.

2.4 Observations Due to Literature

Difficulty of Zero-Day Attacks: According to the literature review, the sophistication and complexity of the zero-day attacks have been on the rise, bypassing the conventional cybersecurity protection at the expense of using an unknown vulnerability. This explains why sophisticated detection and prediction methods are required that can detect emerging threats in real time.

Dynamic and Continuously Changing Cybersecurity Environment: According to the literature, the cybersecurity environment is dynamic and undergoing changes in terms of new attack vectors and methods. The signature-based techniques are typically not effective in tackling the zero-day attacks, and this is why new methods based on the ML and DL techniques should be explored.

Role of ML and DL: the ML and DL algorithms have been used in the research of cybersecurity as a result of the possibility to analyze large amounts of data and identify minor patterns that are likely indicative of malicious activity. The literature highlights the possibilities of such techniques to improve the effectiveness and accuracy of the zero-day attack detection and prediction systems.

Significance of Feature Selection: Feature selection comes out as a decisive point in zero-day attack detection and prediction, and the literature focuses on identifying the prominent features that play significant roles in the correct classification of malicious activity. Random forest and logistic regression are some of the techniques that have been used to select features to enhance the performance of a model.

Approach to Comparative Analysis: Although there are many studies that suggest different ML and DL algorithms to detect and predict zero-day attacks, the comparative analysis of the algorithms has not yet been conducted widely, and it is recommended that such studies should be performed to help to choose the best approach to cybersecurity defenses.

Table 2.6 Comparison Table for Existing Works in each Zero-Day Attack

Year	Author	Title	Method	Parameters Used	Observation
2018	Kostas	ML-Based Anomaly Detection in Networks	Anomaly Detection	ML Algorithms, Network Traffic Data	Proposes anomaly detection in networks using ML algorithms.
2021	Kumar and Sinha	A robust, intelligent, zero-day cyber-attack detection technique	Intelligent Cyber-Attack Detection	ML , DL	Introduces a technique for robust detection of zero-day cyber-attacks using intelligent methods.
2021	Kunang et al.	Attack classification of an intrusion detection system using DL and hyperparameter optimization	Intrusion Detection System Classification	DL , Hyperparameter Optimization	Utilizes DL and hyperparameter optimization for attack classification in IDS.
2018	Yang and Zhao	DDoS Attack Identification and Defense Using SDN Based on ML Method	DDoS Attack Identification	ML , SDN (Software-Defined Networking)	Proposes a method for DDoS attack identification and defense using SDN and ML.
2021	Babu and Veena	A Survey on Attack Detection Methods For IoT Using ML And DL	Attack Detection in IoT	ML , DL	Provides a survey on attack detection methods in IoT utilizing ML and DL.

2.5 Research Challenges and Gaps Identified

Imbalance in Data: The initial drawback is the presence of imbalance in the data in datasets which are used in the detection and prediction of zero-day attacks. The number of zero-day attacks is very large, usually greatly exceeded by the number of benign cases, so that biased models one of which will be quite unable to correctly classify rare events will be produced. In order to counter this challenge, oversampling, undersampling, or special algorithms to handle imbalanced data are all the methods that can be used.

Scalability and Efficiency: The other issue is the scalability and efficiency of additional ML and DL models in particular in large-scale network environments. Complex models, which are trained with big data, can be computationally demanding and time consuming and not practically applicable in real time threat detection. The answer to this dilemma is to develop algorithms that can be scaled, as well as parallel processing to make the model more efficient.

Generalization across Domains: Since there are no numerous studies performed, the majority of that focus on specific datasets or network contexts, thus limiting the generalizability of the findings to other domains and settings. The robust zero-day attack detection and prediction models that are generalized over the different network infrastructures are a big problem to have. To address this vacuum, there is need to research the methods of TL and devise elastic models which could be in a position to be responsive to alterations in network architecture.

Interpretability and Explainability: Although different ML and DL models are reported to have high accuracy in detection, the black-box quality is a major limitation of the models due to its grave limitation on the interpretability and explainability, which is a crucial requirement in the field of cybersecurity. Security analysts should understand why a particular network activity has been marked a zero-day attack that alerts can be verified, attack behavior can be investigated and mitigation measures that informed. The absence of clear decision-making procedures reduces trust and impairs forensic analysis and puts such models into practice of the real-life clouds.

To address this concern, in different chapters, the proposed research incorporates both the model-level and decision-level interpretability mechanisms. Chapter 4 introduces the model of probabilistic attack path, and graph representation, which have inherent explainability in that demonstrate the patterns of the attack progression. The fifth chapter also presents a Bi-LSTM framework that is built based on game theory, and a payoff can be understood as the way to analyze the strategies of attacker and defender and equilibrium states. In chapters 6 and 7, feature contribution and ensemble decision fusion are applied to interpret the model predictions by determining the important features and model confidence scores. The combination of these mechanisms enhances transparency, develops trust on the analysts and decision-making in zero-day attacks detection.

Evaluation Metrics and Benchmarking: There is no standard evaluation metrics and benchmark data sets to evaluate the performance of zero-day attack prediction and detection model. It is therefore difficult to compare when comparing results between various studies and establish the effectiveness of the proposed methodologies. It would be more appropriate to create standardized assessment procedures and benchmark data sets to make more significant comparisons and identify the state-of-the-art methods.

2.6 Phase-Wise Literature Mapping and Comparison

Chapter 3 suggests and elaborates a four-step model that combines the many ML, DL and optimization methods of identifying, predicting, detecting and refining instances of zero-day attacks. The phase is befriended by the previous research, and the substantial literature pertinent to the approaches applied at every stage is outlined below.

Phase 1: Identification of Attack Paths

In this phase, Enhanced Back Propagation Neural Network (BPNN) with a probabilistic graph model is used to determine zero-day attack traces in a simulated cloud setting.

- **Relevant Works**:
    i. Xie et al. (2014) introduced the attack graph-based modeling of the threat propagation analysis.
    ii. The neural network theory presented by Haykin formed the basis of the training techniques of BPNN.
    iii. CloudSim has also been developed by Buyya et al. (2009) and is deployed here to simulate attack environments.
- **Comparison:** The proposed phase improves upon prior work by incorporating probabilistic weights and dynamic graph expansion for zero-day path identification.

Phase 2: Prediction of Attacker Behavior

This phase presents Modified Bi-LSTM with Game Theory that predicts the actions of attackers based on the behavioral patterns and the payoff modeling.

- **Relevant Works**:
    i. Zhang et al. (2019) proved the applicability of LSTM to cyber threats forecasting in terms of temporal sequences.
    ii. Alpcan and Başar (2011) used game-theoretic methods in the assignment of security resources and the model of attackers.
- **Comparison:** This phase, in contrast to current models, which use standalone LSTM, improves temporal modeling, and in addition to that, strategic interaction, to predict threats in advance.

Phase 3: Detection of Real-Time Threats

This phase uses a profound hybrid architecture DC-nZDA that comprises ResNet50 and LSTM to classify a zero-day threat in real-time.

- **Relevant Works**:
    i. ResNet, proposed by He et al. (2015), improves the work of CNN with residual learning.
    ii. Vinayakumar et al. (2018) proposed using CNN and LSTM as IDS models that add value to the detection using a DL.
- **Comparison:** The proposed architecture will be superior to the previous systems of DL-based IDS because it is able to incorporate residual learning and temporal dynamics, specifically with regard to the adversarial zero-day threats.

Phase 4: Optimization for Performance Enhancement

Phase 4 captures more accurate detection and a lower optimization of false positives with an Optimized Levy Flight-based Methods (OLFFOA).

- **Relevant Works**:
    i. Pan (2012) proposed FFOA to solve problems of optimizing functions.
    ii. Metaheuristic and swarm intelligence Yang (2010) and Wang et al. (2020) investigated Levy Flight.
- **Comparison:** FFOA and Levy Flight hybridization are better when compared to conventional methods of optimization in terms of convergence rate and detection accuracy.

All stages of the proposed research are grounded on and contrasted with the prior work. The consolidated model presents progressive innovations through the combination of the tested ideas with the new combinations applied to zero-day attacks detection, expectation, identification, and optimization. This is explained in the subsequent chapters.

2.7 Chapter Summary

This chapter is a critical examination of the existing literature on the issue of the detection and prediction of the threat of the zero-day which involved the enhanced severity of the zero-day and the inefficiency of the existing signature-based security systems. ML, DL, game theory and strategies built on optimization and benefits and downside by nature in terms of generalization, interpretability and real-time application have been discussed and benefits and shortcomings have been reviewed. It is based on this analysis that critical research issues and gaps were identified such as the need to have powerful, explicable and scalable detection frameworks that would be able to cope with previously unseen attacks. The lessons acquired in this chapter form a specific motivation which lies at the back of the hybrid and optimization based strategy which is developed in the subsequent chapters.

Publications

- S. A. M and P. G, A Survey on Various Intrusion Detection System Tools and Methods in Cloud Computing, 2019 6th International Conference on Computing for Sustainable Global Development (INDIACom), New Delhi, India, 2019, pp. 439-445. (Scopus)

- M, Swathy Akshaya and G, Padmavathi, A Study on Zero-Day Attacks (2019). Proceedings of International Conference on Sustainable Computing in Science, Technology and Management (SUSCOM), Amity University Rajasthan, Jaipur – India.