IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

A COMPREHENSIVE ANALYSIS FOR CYBERSECURITY: EXISTING CHALLENGES, RESEARCH POTENTIALS, AND FUTURE DIRECTIONS

Renuga K
Assistant Professor
Department of Computer science
Karpagam Academy of Higher Education,
Deemed to be University
Coimbatore-641021

Dr.A. Faritha banu
Assistant Professor
Department of Computer Technology
Karpagam Academy of Higher Education
Deemed to be University
Coimbatore-641021

ABSTRACT

Cyber security has become a serious concern that requires the attention of researchers, academicians, and industries to secure information systems. With the world ever digitizing and out of various people and organizations trying to adapt to this new ecosystem for sustenance, we are inevitably being faced with newer cyber threats. AI assists cybersecurity professionals in automating basic tasks, hastening threat detection and response, and fine-tuning their actions. It improves the security stance to face multiple threat vectors and types of cyberattacks. This is one example for safer online behavior of end users through comprehensive training programs. This paper illuminates the trends and future research on generative AI application in cybersecurity. In enjoying the promise of stronger security that could be made possible through generative AI methods, it also warned about the importance of "robust defenses" against perpetrators relying on them. Show more, it further notes the ethical considerations of using generative AI for malicious activities and underlines best practices of responsible and ethics-driven application.

Keywords: Secure digital infrastructure, Reliable systems, Improving security frameworks, and system protection, Security models, Information security, Data-driven innovation.

I. INTRODUCTION

Cyber threats are significant, and growing strategic risks facing a wide range of private and public organizations. These are damage to brand or reputation, theft or corruption of sensitive information and direct financial losses all the way up to stealing valuable intellectual property and data. As cybersecurity is emerging as a key issue when it comes to organizations investing in protections. Protecting networks, systems, and data from online threats while promoting responsible and sustainable technological usage is known as cybersecurity. In modern times, where everything is connected, cybersecurity not only protects information but also helps the environment by stopping people from wasting resources and misusing systems. Cyberattacks may be very bad for businesses, causing them to lose money, damage their reputation, and even kill people in industries with important infrastructure system, including healthcare and energy. Small businesses, government agencies, the military, healthcare providers, schools, energy companies, and transportation systems all use cyber security to protect personal data,

keep important systems safe, and make sure that sensitive information is kept private and safe.

A. Types of Cybersecurity

- **Network Security**: Networks connect devices and let people share information. This enables companies, educational institutions, governmental organisations, and other groups to carry out their regular tasks. An organization's computer networks are protected from hackers, unauthorised access, and other threats by network security.
- **Information security:** Prevents unauthorised access, theft, or destruction to everything from employee documents to sensitive corporate plans and customer credit card information. Identity theft, financial fraud, and significant harm to a company's reputation or competitive edge can result from this type of confidential information falling into the wrong hands.
- **Application security:** Everything you need to know about protecting the software people and companies use on a daily basis. This can include corporate software, web apps, and mobile apps. These apps are crucial to a business's ability to do things like manage its money and assist customers. One of the most important tools for keeping applications safe from possible threats is static analysis, which analyzes an application's code to find security holes.
- **Cloud computing:** By enabling simple access to data storage, software tools, and the processing power required to run complicated apps without having to buy costly on-site hardware, cloud computing revolutionised the way organisations of all sizes work.
- **Endpoint security**: Any devices that connect to a company's network. This includes laptops that employees use, smartphones that employees use to check business emails, and servers that hold important data. Endpoint security is becoming a primary priority because more people are working from home and utilizing different devices to access their company's systems.
- **Operational security** (OpSec): It highlights the shortcomings in a company's routine digital functions, such as the way staff manage sensitive data. It ensures that critical data, including as company plans, client information, and intellectual property, are protected from misuse, loss, and illegal access.
- **Website Security**: By doing this, websites are protected from online risks. Programs for website security will safeguard the database, files, apps, and source code of the website. Identity theft, downtime, financial loss, harm to one's reputation and brand image, and more have all been caused by data breaches.

B. Types of Security Attacks

A security attack is any action that puts information and/or computer systems at risk, whether it was planned or not. Examples include copying information, analyzing traffic, changing original data, or making new data, like replaying or interrupting data.

Physical attacks: A physical attack occurs when attackers gain direct access to hardware devices and alter or damage them to steal data or disrupt operations. These kinds of attacks happen more commonly since IoT devices are generally in open or remote areas.

Software attacks: Software attacks hunt for security holes in operating systems, programs, or firmware so they can get in without authorization or destroy computers.

Network attacks: Try to steal, modify, or block data that is being sent by targeting the communication channels between devices.

Encryption attacks: Try to breach around cryptographic systems to get to protected data.

Distributed Denial of Service (DDoS) Attack: It poses a major threat to online systems, web services, network devices, and both conventional and contemporary networks like SDN. The target's resources are exhausted by adversaries assaulting it with heavy network traffic. For an extended length of time, this results in the system slowing down, crashing, or becoming completely unavailable to authorised users.

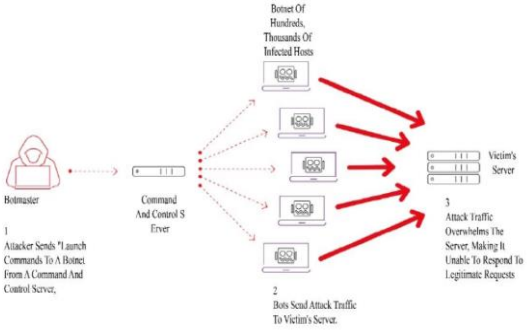

Figure 1: Attack

Therefore, it is necessary to implement thorough detection techniques for DDoS attacks in Big Data Distributed Processing Frameworks in order to handle the difficulties in DDoS. In order to emphasise the necessity of creating efficient defense mechanisms, a crucial area for future research for emerging DDoS attacks are examined.

C. AI IN CYBER SECURITY

With the rise of AI it is also able to analyze historical threat patterns and detect anomalies in real time which a human would not have been able to manage It may also automate filtering out bad traffic and patching vulnerabilities, leaving humans with trickier threats. Predictive analytics provided by Machine Learning (ML) can identify these possible threats and enable preventive measures. Here, AI-based security can draw on its knowledge of earlier attacks or other businesses undergoing similar assaults, enabling us to adapt much faster to emerging vulnerabilities.

This paper is arranged in this way: section 1 Introduction to cybersecurity. In Section 2, we review related work that pertains to our research. Section 3 reviews on a gap in previous research. In Section 4 & 5, various spanning ML approaches and Deep Learning (DL) techniques applied in the cybersecurity domain (the relevant constraints). In Section 6, a wide range of research on top of cyber security is reviewed. The paper is finally concluded in Section 7, which also explores potential future research directions.

II. LITERATURE SURVEY

With the growth of cyberattacks towards critical infrastructure system and commercial environments, a cybersecurity domain has emerged. At first, the entire cybersecurity stuff revolved around perimeter defenses are just a firewall and antivirus with access control over some resources. These strategies were simple, but largely reactive and not terribly expansive. As networks grew and digital transformation took off, these academics pushed for a security-tightening paradigm that was more adaptive to the context. With the rise of distributed systems as well as mobile computing & cloud computing, the attack surface has increased tremendously. So researchers began applying new threat models and defensive frameworks.

In order to improve DDoS attack detection, Alamgir Hossain and Saiful Islam (2024) devised an approach that combines hybrid feature selection (FS) technique paired with an ensemble-based classifier. This hybrid FS method integrates several methods to find the most pertinent features. With an ensemble-based classifier, those features are combined. To improve classification accuracy and decrease overfitting through model robustness, the ensemble method-building strategy combines many decision trees (DT). FS uses principal component analysis (PCA), correlation analysis, and mutual information to identify the best attributes in detecting attacks. However, the Random Forest (RF) classifier based on an ensemble of other classifiers provides the highest detection rates when optimal features are utilised. The recommended framework is assessed using a number of DDoS attack detection datasets. The results demonstrate that it performs better than current approaches in metrics, including accuracy (ACC), recall, precision (PRE), f1-score, and False Positive (FP) rate. The ACC rate of the suggested method is 99.945%; the True Positive (TP) rate is calculated as 100%, and error rate is as low as 0%. That makes it a good candidate to look for DDoS attacks.

To detect malware-infected apps and illegally distributed data in the IoT background, the hybrid DL technique was proposed by Markkandeyan et al. [5] in [2025]. In contrast, SC is the best approach because it continues to seek illegal material while displaying source code where IPSO is superior for deeper networks with few read missing data points. Advantages of new approach This state-of-the-art hybrid strategy blends up-to-date DL with optimization methods to improve cyber security. This allows for more effective and accurate detection. This allows the model to handle the complexity of cyber threats in today's connected world, as it has a robust method for detecting threats in real time. To remove the noisy input and represent how important a proxy is for the SC duplication, the tokenization and weighting feature techniques are applied. In the second part, a DL method is used to maintain SC duplicates GCJ FAQ collection Used Google Code Jam (GCJ) to collect the dataset to study software piracy. Additionally, anomalous behavior in the IoT background was identified using the Enhanced (LSTM) Long Short-Term Memory (E-LSTM), which was highlighted using colour visuals. When collected malware samples needed for

testing using the Maling dataset. Test results indicate that the proposed solution to evaluate cyber security threats in IoT is superior than traditional evaluation techniques at certain classification.

A new hybrid FS-based unsupervised (IDS) Intrusion Detection System called HYbrid and Robust Intrusion DEtection (HYRIDE) was presented by Srivastav et al. [6] [2025]. To extract the fewest optimal features possible, it uses many FS methods. To automatically identify abnormal network data, these features are modelled in the local outlier factor, elliptic envelope, and histogram-based outlier score. As a result, HYRIDE can differentiate between intrusions and normal events more easily and accurately. The suggested method is verified using common datasets, including the University of New South Wales-Network Benchmark (UNSW-NB15), the Canadian Institute of Cybersecurity's IDS (CICIDS 2017), operating systems datasets of Windows and Linux, network traffic (TON, IoT), and telemetry datasets of IoT services.

A new hybrid quantum-classical DL model for cybersecurity applications : botnet detection based on domain generation algorithms (DGA), and it was suggested by Suryotrisongko and Musashi [7] [2022]. Evaluating the performance of the hybrid model with that of its classical model equivalent in order to determine whether a quantum circuit was a useful building block in a DL model. MinREBotnets, CharLength, TreeNewFeature, and nGramReputation_Alexa are the four components from the Botnet DGA dataset that are utilised. Pennylane's embedding (Angle Embedding and IQP Embedding) and layers circuit (Basic Entangler Layers, Random Layers, and Strongly Entangling Layers) make up the hybrid model's quantum circuit. To ascertain whether the model might be used with current Noisy Intermediate Scale Quantum (NISQ) devices, researchers also constructed noise models. We found that under best case scenarios, the hybrid approach excelled. We discovered that Angle Embedding and Strongly Entangled complement each other well in addition to providing the best results of the standard deep learning model, through testing with n=100. However, in other conditions the overall performance is still weak compared with that of standard deep learning model.

In the context of IIoTs, a Leveraging Sparrow Search Optimisation Algorithm for a DL-Based Cybersecurity (LSSOA-DLBC) technique was suggested by Alrayes et al. [8] [2025]. This method automatically searches the IIoT environment for cybersecurity. Z-score normalisation is the initial stage of the data normalisation procedure for the LSSOA-DLBC model. For FS, the recommended framework employs the sine cosine algorithm (SCA). Furthermore, cybersecurity in the IIoT scenario is automatically detected by the deep belief network (DBN) model. In the end, the DBN model's hyperparameter tuning is enhanced by the sparrow search algorithm (SSA) model. The benchmark dataset is used to assess the experimental outcomes of the LSSOA-DLBC technique. In comparison to current approaches, the LSSOA-DLBC methodology's performance validation shows an enhanced accuracy rate of 99.29% across numerous evaluation metrics.

In IoT network, the Hybrid Dung Beetle Optimization-based Dimensionality Reduction with DL-based Cybersecurity Solution (HDBODR-DLCS) technique was created by Alkhalifa et al. [9] [2025] to reduce the dimension count. The purpose of this technique is to reduce the number of dimensions while also tweaking hyperparameters to improve detection outcomes. In the first step of the HDBODR-DLCS approach, the input dataset was determined using Z-score normalisation. By identifying the crucial elements and eliminating the unimportant ones, the HDBO model helps in reducing dimensional count. To identify intrusions, the attention bidirectional recurrent neural network (ABiRNN) model is also employed. At last, a hyperparameter tuning process based on artificial rabbits optimization (ARO) is done, which improves the overall performance of the classification. The benchmark IDS dataset is used to empirically evaluate the HDBODR-DLCS method. The outcomes of the test showed that this recommended method is better than other approaches that are already in use.

A Zero Trust (ZT)-based cybersecurity system with secure MQTT communication, AI-driven intrusion detection, and automated remediation in a layered architecture was suggested by Kabir et al. [10] [2026] for critical infrastructure. Three layers make up the suggested framework: perception, network, and application. A secure message broker ensures that messages are sent

securely, a Zero Trust enforcement mechanism continuously monitors traffic, and trusted edge devices gather data in real time. For detecting both short- and long-term temporal dependencies in network traffic, the hybrid GRU+LSTM DL model was used by the core of the detection engine. This enables it to accurately discern between desired and unwanted behavior. A multi-class MQTT intrusion dataset comprising real traffic, DoS traffic, flood traffic, malformed traffic, brute force traffic, and SlowITe traffic was used for the experiments. The suggested model has an ACC of 89.21%, PRE:0.90, recall:0.91, F1 Score value of 0.89, and AUC = 0.99. Both traditional ML models and advanced DL models with faster inference times were outperformed by the recommended approach. This framework uses secure application layer response approaches to enable automated problem solving and real-time monitoring. These outcomes show that hybrid deep learning automatically implements a strong and flexible defense mechanism for vital infrastructure system against growing cyber assaults, all while simultaneously enabling secure network modernization and the reinforcement of Cybersecurity posture by using different schemes in accordance with the Zero Trust environment.

Al-Quayed [11] [2026] proposed a new paradigm hierarchical security architecture, called FE-ACS (Fog-Edge Adaptive Cybersecurity System), that aims to maximize the efficiency of security measures and respect latency allocations at both processing levels by directing AI-based anomaly detection modules toward the fog/edge or cloud layers. In comparison to cloud-centered architecture (152.3 ms) and fog-only infrastructure (34.5 ms), FE-ACS requires much reduced end-to-end latency (18.7 ms) and attains high detection efficiency (AUC-ROC of 0.985 and F1-score of 0.923). The solution is 67x more scalable with native cloud-based approach supporting at-least 38,000 devices (logarithmic performance degraded).

The architecture identifies 12,400 events per second at an energy cost of just 12.3 mJ per inference, according to the computational efficiency studies. With a very high system dependability score (94.0%) and a low patient safety score (14.7%), FE-ACS has outstanding overall operational viability in healthcare risk assessment. The recommended model offers a scalable, privacy-preserving, and real-time solution for defending healthcare IoT networks against changing cyber threats. It provides a major breakthrough in distributed security designs.

Alamri et al [12] [2026] suggested an edge-enabled cybersecurity solution that uses deep ensemble learning and edge analytics to prevent image-based malware in healthcare networks and provide low-latency data source inference. VGDense-DeepEnsemble (VGGDenseNet-DeepEnsemble) is a novel stacked deep learning model that uses ensemble learning with a meta-model to improve detection efficacy by integrating VGG16, VGG19, DenseNet121, and Dense Using Explainable AI (XAI) and Grad-CAM on sample photographs, we determined how the AI made decisions. A separate test dataset for final evaluation and the Blended Malware Image Dataset with 31 malware families were used to test the proposed approach. The suggested model has 96% accuracy, 97% macro precision, 96% macro recall, and 96% macro F1 score. These results outperform each backbone individually (VGG16: 88%, VGG19: 94%, DenseNet121: 93%, DenseNet169: 94%). All classes are robust and separable, according to the ROC and precision-recall studies. Misclassifications in hard families (Neshta, Sality, Agent, and Injector) dramatically decrease, according to the confusion matrices. Grad-CAM explanations indicate that malware-relevant structures drive predictions, not background noise. These findings demonstrate that transparent edge-centric deep ensemble models can effectively, precisely, and explicably secure healthcare networks against image-based malware attacks.

For the challenging issue of SQL injection (SQLi) identification, a Bi-directional LSTM (BiLSTM) architecture [2026] was suggested by Hassan et al. [13]. In order to learn thoroughly with high generalization, we designed a composite dataset consisting of 244,112 records aggregated from seven mainstream benchmarks and further beefed up with manually created adversaries queries that closely simulate real-world exploitation scenarios. Our model was rigorously tested against five of the best classifiers; AdaBoost, XGBoost, CatBoost, Naive Bayes and LightGBM. A 15% test partition split in stratified manner was created. * CyberBiLSTM: The attention-based sequential feature extraction and attention clustering aims to leverage bi-directional sequence processing for successful detection. New large-scale

dataset, vigorous benchmarking showing it is efficient and performant. The newly proposed CyberBiLSTM achieved best results with 98.43% and precision, F1-score and recall reached each other at 98%. Final notes This is easier to simplify than all-optimal gradient-boosting frameworks. The results reveal that, indeed, sequence-aware deep architectures are effective in detecting the underlying semantics behind harmful payloads. It sets a precedent for an innovative treatment of intelligent SQL injection (SQLi) defense in the domain of computer science research.

Table 1: COMPARISON OF CYBERSECURITY TECHNIQUES

Author	Algorithms	Merits	Demerits
Hossain and Islam [4] [2024]	Hybrid FS and ensemble-based classifier	provides exceptional performance and nearly flawless accuracy across a variety of parameters.	Supports only DDoS attacks
Markkandeyan et al [5] [2025]	Novel hybrid DL with Improved Particle Swarm Optimization	More reliable cybersecurity decision-making	Implementation difficulty in large-scale cybersecurity systems
Srivastav et al [6] [2025]	HYRIDE	Easily detects the normal events and intrusions	Restricted to cyberthreats that are always changing
Suryotrisongko and Musashi [7] [2022]	Hybrid quantum-classical DL model	Demonstrates improved performance when using the noise model	Leading to interoperability and compatibility challenges.
Alrayes et al [8] [2025]	Leveraging Sparrow Search Optimization Algorithm with DL (LSSOA-DLBC)	Automatically identifies cybersecurity in the IIoT environment.	Need to focus on more dynamic datasets.
Alkhalifa et al [9] [2025]	HDBODR-DLCS	Utilizes hyperparameter tuning to do dimensionality reduction for better detection results.	The algorithm may prematurely converge to less-than-ideal solutions in intricate cybersecurity contexts with dynamic attack patterns.
Kabir et al [10] [2026]	ZT-based critical infrastructure cybersecurity framework	Offers a reliable and expandable way to protect vital infrastructure from changing cyberthreats.	Characteristics of network traffic might differ greatly based on communication patterns, device configurations, and deployment conditions.
Al-Quayed [11] [2026]	FE-ACS (Fog-Edge Adaptive Cybersecurity System)	Scalable and privacy-preserving	Maintenance complexity due to distributed network
Alamri et al [12] [2026]	Edge-enabled cybersec	Defend healthcare	Increased management

	urity framework	networks from image-based malware effectively	complexity and security risks due to distributed edge devices
Hassan et al [13] [2026]	CyberBiLSTM model	Good at identifying the hidden meanings of harmful payloads	To get high detection accuracy, CyberBiLSTM models need a lot of annotated cybersecurity datasets.

III. RESEARCH GAP

While a lot of progress in cybersecurity technologies, there are still important research areas that need to be studied and analyzed further. The current generation of cybersecurity systems lacks dependable, real-time threat detection and response capabilities, which is made even more problematic by sophisticated persistent threats and zero-day exploits. Security models using artificial intelligence and DL based methods aren't feasible in resource-constrained scenarios, such as embedded systems, edge devices and IoT. Moreover, the lack of large and relevant and high quality up-to-date cybersecurity datasets is a major concern that complicate training machine learning models for accuracy and generalizability. Another major concern lies within the opacity and inherent difficulty of use with which AI-driven cybersecurity systems are created. Most models operate as “black boxes,” providing no insight into how decisions are made. In addition, many legacy cybersecurity solutions focus on point solutions rather than integrated, multi-layered defense systems that can prevent, detect and respond to threats. The article demonstrates the imperative of innovative and scalable solutions in light of security vulnerabilities in cloud and distributed computing environments, as well as a failure to advance autonomous and self-healing cybersecurity software. Consequently, future research endeavors should concentrate on cybersecurity frameworks that are lightweight, easily understandable, and adaptable to large-scale, dynamic networks.

IV. MACHINE LEARNING IN CYBERSECURITY

ML is very important in the fight against cyber risks and attacks. It may help find malware, phishing, spam, and fraud. This review will analyze spam, IDS, and virus detection. In order to harm a particular machine and jeopardise the confidentiality, integrity, and availability of computer resources and services, malicious code operates on it. In the future, machine learning will be the best way to find things. Training approaches for finding malware should not cost too much. Additionally, malware analysts ought to be effective in understanding ML techniques for malware identification. One of the most important problems with the security system is that the average user, who doesn't know much about security, usually decides how reliable the computing resources are. Replay attacks, man-in-the-middle (MiTM) attacks, impersonation, credential leakage, password guessing, session key leakage, unauthorised data updates, malware injection, flooding, denial of service (DoS), and DDoS attacks are just a few of the ways that connected systems can be targeted in cyberspace. A security standard of some kind is necessary to identify and stop these threats. ML models can learn about different cyberattacks in both offline and online contexts because of the pre-processed dataset that is provided. In online mode, the ML algorithms can immediately detect any indications of an incursion (a cyberattack).

V. DEEP LEARNING IN CYBERSECURITY

In the last several years, researchers in cybersecurity have been looking into a branch of ML called DL. This is because DL can automatically look through and organize through a lot of internet data. Cybersecurity solutions that leverage DL methods automatically identify and forecast cyberattacks. Over time, their skills get better and better. DL architectures have been highly helpful in solving severe cybersecurity problems since they have a lot of advantages over prior ML methods. More precisely, the data that comes from the security sector is growing more varied because it comes from a lot of various sources, such as logs and sensors on networks. They also follow different formats and have complex interactions. Because of this, many problems are now too hard or too much

effort for typical ML approaches like Support Vector Machines (SVM). These methods can't handle input with a lot of dimensions and don't grow better with more data. Big data, on the other hand, makes DL better by getting rid of domain expertise and leveraging hierarchical feature extraction. In short, DL methods can learn feature representations by using a multitude of nonlinear hidden layers. This makes feature engineering automatic. It doesn't cost as much money or time to hire staff to fix things when a new sort of hack, like zero-day malware, comes out. When it comes to cybersecurity, people in both the public and private sectors are starting to trust DL apps more because of these advantages.

CHALLENGES OF CYBERSECURITY

In the digital age, cybersecurity is a big worry for consumers, businesses, and governments. As technology and digital devices become more common, it is more important than ever to protect networks, electronic devices, and data against theft, damage, and unwanted access. As technology gets better, defending a business, its people, and its most important assets from cyber threats becomes harder. This article will talk about the problems that the cybersecurity sector is facing and the steps that can be taken to solve them in the future.

DATASET AVAILABILITY

There are several cybersecurity datasets based on research that were produced explicitly to train intrusion detection systems, notably for machine learning approaches. IDS datasets not only record actual network traffic but also employ techniques such as data replay, data synthesis, simulation, and emulation datasets [13]. These datasets have pros and cons, such as differences in how well they can grow, how private they are, how well they cover the topic, and how realistic they are.

One important tool for researching and creating methods for identifying and classifying DDoS attacks is the CIC-DDoS2019 dataset. It closely resembles real-world data with both benign traffic and the most current, common DDoS attacks.

Network traffic analysis findings, including source and destination IP timestamp protocols, ports, and attack kinds, are also included in this dataset. The total number of records in the dataset is 50,063,112. Here, the amount of malicious data is shown by the 50,006,249 DDoS attacks and the 56,863 normal (benign) traffic. There are 86 features (variables or attributes) in each record that can be utilised for traffic analysis.

Table 2: Various attacks in CIC-DDoS2019 dataset

S.No	Attacks	Description
1.	NTP-based attack	UDP traffic is amplified by Network Time Protocol (NTP) servers to overwhelm a target, causing disruption and making its infrastructure unavailable.
2.	DNS-based attack	An inordinate amount of resolution requests is sent to a certain IP address by the attacker using a botnet.
3.	LDAP-based attack	generates amplified responses that are subsequently sent to the target server by using a vulnerable, publicly available LDAP server.
4.	MSSQL-based attack	Actors can submit requests to susceptible servers using the Microsoft SQL Server Resolution Protocol (MC-SQLR) by using spoof IP addresses. This gives a perception that the requests come from the target's IP address instead of the attacker's
5.	NetBIOS-based attack	All NetBIOS network traffic is restricted when an

		attacker sends fake "Name Conflict" or "Name Release" notifications to the target system, disrupting service.
6.	NetBIOS-based attack	To overload the target's network, attack volumes of hundreds of gigabits per second are generated using the Simple Network Management Protocol (SNMP).
7.	SSDP-based attack	More traffic can be sent to a particular target by using Universal Plug and Play (UPnP) protocols.
8.	UDP-Lag-based attack	IP packets known as UDP datagrams are transmitted with the intention of slowing down or stopping the target host.
9.	WebDDoS-based attack	To attack and interfere with a web server or service, people utilise legitimate HTTP GET or POST queries.
10.	SYN-based attack	The network server under assault becomes unusable due to the consumption of resources during the TCP three-way handshake process.
11.	TFTP-based attack	The victim server returns data to the attacker when the attacker makes queries to TFTP servers via the Trivial File Transfer Protocol (TFTP).
12.	PortScan-based attack	A remote server's active services can be discovered by an attack that scans ports on a single computer or the entire network to verify network security.

VI. EVALUATION METRICS

This metrics supports in identifying the potential of recommended method for DDoS attacks with minimal FP and high accuracy. ACC, recall, PRE, F1-score, FP rate (FPR), and TP rate (TPR) are the evaluation metrics for the suggested DDoS attack detection model. The experimental findings of the CIC-DDoS2019 dataset are covered in this section.

A confusion matrix shows how many of the model's forecasts were right and how many were wrong when contrasted to the actual results (or true labels) in the test data. Usually, the table is a square matrix with the actual class labels in the rows and the expected class labels in the columns. In a binary classification task, the four possible outcomes are TP, FP, true negatives (TN), and false negatives (FN).

- TP: The framework correctly forecasts the positive class.
- FP: The framework forecasts the positive class incorrectly.
- TN: The framework correctly forecasts the negative class.
- FN: The framework incorrectly forecasts the negative class.

The CIC-DDoS2019 dataset makes it easy to classify different sorts of DDoS assaults into multiple classes and helps figure out how well different algorithms work in terms of ACC, PRE, recall, F1-score, and detection delay.

Table 3: Performance Comparison of DL and ML algorithms on CICDDoS2019 dataset.

Methods	Accuracy	Precision	Recall	F1-score
LR	87%	84%	90%	86%
RF	95%	86.84 %	60.8 7%	71.5 8%
SVM	96%	95%	97%	96%
Bi-LSTM	96%	97%	96%	96%
RNN	97%	97%	96%	97%

Traditional ML methods like LR, RF, and SVM do fairly well in terms of recognition accuracy, according to the data displayed in Table 3. Nevertheless, their total performance is comparatively lower than DL algorithms. On the other hand, DL-based models such basic RNN and Bi-LSTM successfully meet the requirements of anomaly traffic recognition since they have greater recall rates in addition to outstanding recognition accuracy. Additionally, when representing long-range dependencies, transformer networks show notable advantages over RNN.

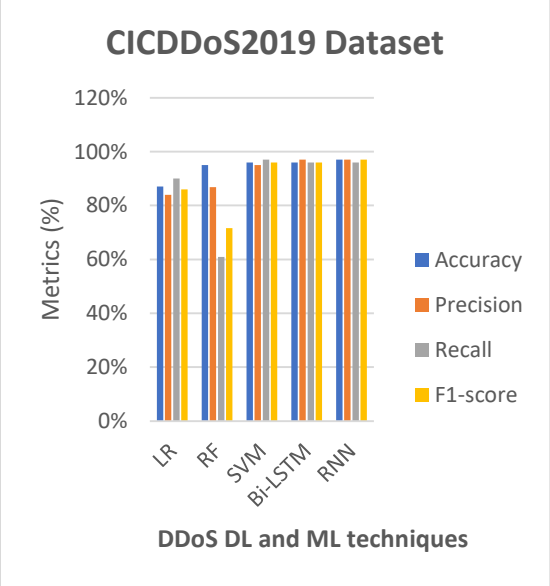

Figure 3: Performance Metrics of DL and ML techniques using CICDDoS2019 dataset.

In this survey, the typical machine-learning performance changes based on the dataset, whereas the RNN classifier gives fantastic results. The RNN did a better job of finding DDoS attacks than typical machine-learning classifiers. Another interesting thing about the figure is that different classifiers regularly get high accuracy.

VII. CONCLUSION

Cybersecurity is an ongoing process that involves regular training, keeping security policies up to date, and being aware of the newest threats and flaws. consumers who work for the company and consumers who utilize the service should also learn how to spot and stay away from risks. To sum up, the approaches discussed are a great way to halt cyberattacks, but they should only be one aspect of a complete security plan that addresses both technical and human flaws. Since DDoS attacks are evolving at a rapid pace, traditional rule-based methods have been able to offer a limited solution for preventing it thereby making deep learning based solutions and approaches very attractive. Deep learning models, particularly Convolutional and LSTM architectures, outperform traditional methods in identifying DDoS attacks with detection rates greater than 98%. These models include data from the real world and can change themselves to new attack patterns, so they are very well at preventing attacks before this happens. In this paper, we addressed some of these gaps and the need to further research DDoS detection systems to make them stronger and easier to interpret. In summary, applying DL to the paradigm of DDoS attack detection has improved network defense from a retrospective viewpoint to an offensive one. Where we are required to do constant research and find innovative solutions just to be ahead of the ever-evolving DDoS attack scenario and keep essential communication networks secure.

REFERENCES

1. Alshuaibi, A., Almaayah, M. and Ali, A., 2025. Machine learning for cybersecurity issues: A systematic review. Secur Challenges, 1(2).

2. Sehrawat, S., Sehrawat, H. and Siwach, V., 2026, January. Enhancing Cybersecurity Through Effective. In Proceedings of International Conference on Recent Trends in Computing: ICRTC 2025, Volume 2 (Vol. 2, p. 74). Springer Nature.

3. Jagtap, S., Kavitkar, V., Jain, M., Ingle, A., Tamkhade, J.P. and Kshirsagar, K., 2025, January. Enhancing Cyber Security Against DDoS Attacks: A Comprehensive Review and Future

Directions. In 2025 1st International Conference on AIML-Applications for Engineering & Technology (ICAET) (pp. 1-6). IEEE

4. Hossain, M.A. and Islam, M.S., 2024. Enhancing DDoS attack detection with hybrid feature selection and ensemble-based classifier: A promising solution for robust cybersecurity. Measurement: Sensors, 32, p.101037.

5. Markkandeyan, S., Ananth, A.D., Rajakumaran, M., Gokila, R.G., Venkatesan, R. and Lakshmi, B., 2025. Novel hybrid deep learning based cyber security threat detection model with optimization algorithm. Cyber Security and Applications, 3, p.100075.

6. Srivastav, S., Shukla, A.K., Kumar, S. and Muhuri, P.K., 2025. HYRIDE: HYbrid and Robust Intrusion DEtection approach for enhancing cybersecurity in Industry 4.0. Internet of Things, 30, p.101492.

7. Suryotrisongko, H. and Musashi, Y., 2022. Evaluating hybrid quantum-classical deep learning for cybersecurity botnet DGA detection. Procedia Computer Science, 197, pp.223-229.

8. Alrayes, F.S., Nemri, N., Mansouri, W., Alshuhail, A., Almukadi, W.S., Al-Sharafi, A.M., Aljabri, J. and Nafie, F.M., 2025. Leveraging sparrow search optimization with deep learning-based cybersecurity detection in industrial internet of things environment. Alexandria Engineering Journal, 121, pp.128-137.

9. Alkhalifa, A.K., Alruwais, N., Mansouri, W., Arasi, M.A., Alliheedi, M., Alallah, F.S., Khadidos, A.O. and Alshareef, A., 2025. Hybrid dung beetle optimization based dimensionality reduction with deep learning based cybersecurity solution on IoT environment. Alexandria Engineering Journal, 111, pp.148-159.

10. Kabir, M.H., Razib, M., Jahin, Z. and Jesan, Z., 2026. Zero Trust Based Critical Infrastructure Cybersecurity Framework with AI-Driven Threat Detection and Secure Network Modernization. Journal of Computer Science and Technology Studies, 8(5), pp.01-14.

11. Al-Quayed, F., 2026. AI-Powered Anomaly Detection and Cybersecurity in Healthcare IoT with Fog-Edge. Computer Modeling in Engineering & Sciences (CMES), 146(1).

12. M. Alamri, Z. Ahmad, M. Humayun, M. Alshammeri, A. Munshi and J. Rasheed, "Cybersecurity Framework for Proactive Detection of Image-Based Malware in Healthcare Networks Using Explainable Deep Ensemble Learning and Edge Analytics," in IEEE Transactions on Consumer Electronics,doi: 10.1109/TCE.2026.3665641.

13. Hassan, M.M., Chowdhury, A.R., Ahammed, R. and Hossen, M.A., 2026, January. CyberBiLSTM: A Bidirectional LSTM Architecture for Cybersecurity via High-Precision SQL Injection Attack Detection. In 2026 5th International Conference on Electrical, Computer & Telecommunication Engineering (ICECTE) (pp. 1-6). IEEE.

14. Zhang, Z., Turnbull, B., Kermanshahi, S.K., Pota, H. and Hu, J., 2025. UNSW-MG24: A heterogeneous dataset for cybersecurity analysis in realistic microgrid systems. IEEE Open Journal of the Computer Society.

15. Abdulrahman, N.F. and Singh, M.J., 2025. Deep learning approaches for DDoS attack detection in communication networks and iot: A comprehensive review. Jurnal Kejuruteraan, 37(1), pp.323-333.

16. Qureshi, R. and Koo, I., 2026. A Comprehensive Survey of Cybersecurity Threats and Data Privacy Issues in Healthcare Systems. Applied Sciences, 16(3), p.1511.

17. Alamir, R., Noor, A., Almukhalfi, H., Almukhlifi, R. and Noor, T.H., 2026. AI-Enhanced Cybersecurity in Edge

Computing: Threats, Solutions, and Future Directions. ACM Computing Surveys.

18. Hjaiji, C., Ouni, B. and Alouini, M.S., 2026. Cybersecurity of High-Altitude Platform Stations: Threat Taxonomy, Attacks and Defenses With Standards Mapping–DDoS Attack Use Case. IEEE Open Journal of the Communications Society.

19. Afzal, M., Capriglione, D., Cerro, G., Ferrigno, L., Masone, B., Miele, G., Nardone, A. and Tari, L., 2026. Measurements in Cybersecurity: Recent Trends and Examples of Application [Roadmap for Measurement and Applications]. IEEE Instrumentation & Measurement Magazine, 29(1), pp.21-29.

20. Afzal, M., Capriglione, D., Cerro, G., Ferrigno, L., Masone, B., Miele, G., Nardone, A. and Tari, L., 2026. Measurements in Cybersecurity: Recent Trends and Examples of Application [Roadmap for Measurement and Applications]. IEEE Instrumentation & Measurement Magazine, 29(1), pp.21-29.

21. Srivastav, S., Shukla, A.K., Kumar, S. and Muhuri, P.K., 2025. HYRIDE: HYbrid and Robust Intrusion DEtection approach for enhancing cybersecurity in Industry 4.0. Internet of Things, 30, p.101492.

22. Suryotrisongko, H. and Musashi, Y., 2022. Evaluating hybrid quantum-classical deep learning for cybersecurity botnet DGA detection. Procedia Computer Science, 197, pp.223-229.

23. J. Ispahany, M. R. Islam, M. Z. Islam, M. A. Khan, Ransomware detection using machine learning: a review, research limitations and future directions, IEEE Access, 2024, 12, 68785-68813.

24. P. Sharma, K. Chaudhary, M. Wagner, M. G. M. Khan, A comparative analysis of malware anomaly detection, Advances in Computer, Communication and Computational Sciences, Springer Singapore, Singapore, 2020, 35-44, doi: 10.1007/978-981-15-4409-5_3.

25. A. Dahiya, S. Singh, G. Shrivastava, Android malware analysis and detection: a systematic review, Expert Systems, 2025, 42, e13488, doi: 10.1111/exsy.13488

26. Karthick.N, Yogeshwaran.M "Hybrid Deep Neural Network Framework for Early and Accurate Alzheimer's Disease Detection," *2025 5th International Conference on Evolutionary Computing and Mobile Sustainable Networks (ICECMSN)*, Coimbatore, India, 2025, pp. 1724-1732, doi: 10.1109/ICECMSN68058.2025.11382838.

27. Karthikeyan, M.M., Dalin, G (2021). Dynamic Congestion Control Routing Algorithm for Energy Harvesting in MANET. In: Smys, S., Balas, V.E., Kamel, K.A., Lafata, P. (eds) Inventive Computation and Information Technologies. Lecture Notes in Networks and Systems, vol 173. Springer, Singapore. https://doi.org/10.1007/978-981-33-4305-4_2

28. A.Krishnaveni and S. Balamurugan, "Phishing Attack Prediction using Several Machine Learning Techniques," *2024 4th International Conference on Sustainable Expert Systems (ICSES)*, Kaski, Nepal, 2024, pp. 484-489, doi: 10.1109/ICSES63445.2024.10763142.

29. V. S. Mohammed and M. M. Karthikeyan, "Enhancing Mobile Network Security Through Blockchain Technology: A Zero Trust Approach Utilizing PoW, PoS, and BFT Algorithms," *2025 International Conference on Multi-Agent Systems for Collaborative Intelligence (ICMSCI)*, Erode, India, 2025, pp. 223-230, doi: 10.1109/ICMSCI62561.2025