# Comprehensive Review Next-Generation Intrusion Prevention System (NGIPS) Based Cyber Attacks Classification and Challenges Using Machine Learning Techniques

**KATIKAM MAHESH [1], AND DR. KUNJAM NAGESWARA RAO [2]**

[1] Scholar at Andhra University College of Engineering, Department of Computer Science and Systems Engineering, India

[2] Professor at Andhra University College of Engineering, Department of Computer Science and Systems Engineering, India

Date of Publication: 24, OCT 2024, Version: 1.0, Volume: 1, Issue: 10

**ABSTRACT** At present, nearly all of international interactions in commerce, economics, culture, social interaction, and government at all level involving individuals, non-governmental organizations, authorities, and governmental institutions take occur online. Cyberattacks and hazards related to technology for wireless communication have become major issues for numerous government agencies and private businesses worldwide in recent times. Today's society relies heavily on electronic technology, and protecting this data against cyberattacks is a challenging issue. The motive behind cyberattacks is to financially harm companies. Next-Generation Intrusion Prevention System (NGIPS) keeps an eye on devices and network traffic for known suspicious tasks, suspect activity by alerting security administrators about known or potential dangers, or by sending alerts to a centralized security tool, an IDS can assist speed up and automate network threat Classification and Detection. In this paper Presenting Cyber Attacks Classification using Various Machine Learning techniques with Datasets and Accuracy.

**KEYWORDS:** *Cyber Attacks, Classification, Next-Generation Intrusion Prevention System, An Intrusion Detection System, Accuracy, Dataset*

## I. INTRODUCTION

The development of harmful software, or malware, presents a significant obstacle to intrusion detection system (IDS) design. software developers have become craftier in their attacks, making it increasingly difficult to recognize unknown and obfuscated software. Utilize various evasion strategies to hide information from an IDS so that it cannot be discovered. Furthermore, there has increased the number of security risks, including zero-day assaults intended specifically for internet surfers. Consequently, With the increasing integration of information technology into our daily lives, computer security has become indispensable. Consequently, a number of nations, including Australia and the The US has been greatly affected by zero-day assaults.

### *A. Types of Cyber Attacks*

- *Attacks with Ransomware*
  In 2024, ransomware assaults will still be a major concern. Cybercriminals are always improving their methods; they use targeted tactics and sophisticated encryption. Organizations may become paralyzed by these attacks, which would cause significant financial losses and harm to their brand. Use focused tactics and cutting-edge encryption Disable businesses and cause large financial losses as well as harm to their reputation Prevent ransomware with frequent security patching, employee awareness training, and strong backup plans. Vulnerabilities related to the Internet of Things The proliferation of IoT devices increases the attack surface available to cybercriminals. IoT vulnerabilities present serious dangers in 2024 since many devices lack sufficient security protections.

- *Vulnerabilities Related to the Internet of Things*
  The proliferation of IoT devices increases the attack surface available to cybercriminals. IoT vulnerabilities present serious dangers in 2024 since many devices lack sufficient security protections. These flaws can be used by hackers to obtain unauthorized access or initiate distributed denial-of-service (DDoS) assaults.

- *Social Engineering and Phishing Attacks*
  In 2024, social engineering and phishing assaults are still very effective. Cybercriminals use

individualized information and advanced methods to trick people. These attacks are more credible since there is a wealth of personal data available on social media and other platforms. Make use of advanced methods and customized data to trick people Take advantage of the wealth of personal information that is accessible on websites and social media Use two-factor authentication, cybersecurity awareness training, and cautious information sharing to thwart phishing and social engineering assaults.

- *Supply Chain Attacks*
  Supply chain attacks are becoming more and more common, and 2024 is no different. Hackers might potentially affect numerous firms by compromising the whole supply chain through the hacking of reliable vendors or suppliers.

- *AI-Powered Cyber Threats*
  Cybercriminals use artificial intelligence (AI) in 2024 to plan complex attacks. AI-generated risks automate attacks, avoid being discovered, and get beyond conventional security safeguards. Utilize artificial intelligence (AI) to plan complex assaults Automate attacks, avoid being discovered, and get beyond conventional security measures to combat hostile AI, implement AI-driven defensive mechanisms and security solutions.

Vulnerability Discovery
DDoS Attacks
Exploitation
AI-POWERED Cyber Threats

Fig 1: AI-Powered Cyber Threats

- *Advanced Persistent Threats*
  Advanced persistent threats, or APTs, are complex cyberattacks that are directed at certain targets, including governments or major corporations. Even in 2024, APTs are still a serious concern because they use cunning tactics to enter networks without authorization and stay there.

- *Zero-Day Exploits*
  Zero-day exploits focus on undiscovered software flaws for which there are no existing fixes or protections. By 2024, state-sponsored hackers and cybercriminals will be heavily interested in zero-day exploits. Target undiscovered software flaws for which there are no existing fixes or protections sought after by hackers with state support and cybercriminals Use intrusion detection systems, apply software patches, and keep an eye on vulnerability databases to protect yourself from zero-day exploits.

- *Cloud Security Risks*
  There is new security vulnerabilities associated with the increased use of cloud services. Misconfigurations, data breaches, and illegal access to cloud systems will be major issues in 2024.growing use of cloud services has led to the introduction of new security threats Important risks include misconfigurations, data breaches, and illegal access to cloud systems.

- *Mobile Security Flaws and Malware*
  Cybercriminals are increasingly focusing on mobile devices because of their broad use and easy access to private data. By 2024, there will be a lot of dangers associated with mobile malware and vulnerabilities, such as identity theft and data breaches.

- *Dangers from Within*
  Insider threats are defined as malevolent or careless acts by people who work for a company. Insider threats are still a major worry in 2024 because personnel with privileged access have the ability to corrupt systems and data, either on purpose or accidentally.

- *Misuse of Artificial Intelligence (AI)*
  Although artificial intelligence (AI) has many useful applications, it can potentially be abused for negative ends. By 2024, there will be a greater risk to cybersecurity due to AI misuse. AI algorithms can be used by cybercriminals to automate assaults, improve their social engineering strategies, or get beyond security measures. The threat posed by the malicious use of AI in cybersecurity is increasing. AI systems have the ability to automate attacks, improve social engineering techniques, and get beyond security measures. Reduce the misuse of AI by putting AI ethics guidelines into place, auditing AI models, and keeping an eye out for questionable activity on AI systems.

- *Violations of Privacy and Data Breaches*
  Data breaches and privacy violations will be a significant cybersecurity concern in 2024. Cybercriminals attack organizations in an attempt to gain sensitive data, which can have a devastating effect on a company's finances and reputation. Because of the legal restrictions on data privacy, businesses need to give data protection first priority. Significant concerns of data breaches and privacy

violations in 2024 Cybercriminals aim to steal confidential information from organizations. Prevent data breaches and privacy violations by implementing strict access controls, frequent security audits, and strong data encryption.

- *Sophisticated Phishing Methods*
  In 2024, phishing assaults have advanced with increasingly complex methods. Cybercriminals deceive people into disclosing critical information by using sophisticated social engineering techniques, skilfully written emails, and convincingly bogus websites. It is imperative to maintain vigilance as these attacks target both persons and organizations.

- *Cyberattacks by Nation-States*
  Nation-state cyberattacks pose a significant threat to governments, corporations, and critical infrastructure by 2024. Well-funded and highly skilled cyber groups plan these attacks with the goal of compromising or breaching networks for financial, military, or political gain.

- *Threats Connected to Cryptocurrencies*
  In 2024, the emergence of cryptocurrencies has brought about fresh cybersecurity risks. Cybercriminals use cryptocurrency wallets, exchanges, and transactions as targets for money theft or to carry out cryptojacking attacks. Because cryptocurrencies are anonymous and decentralized, it is difficult to track down and retrieve stolen property.

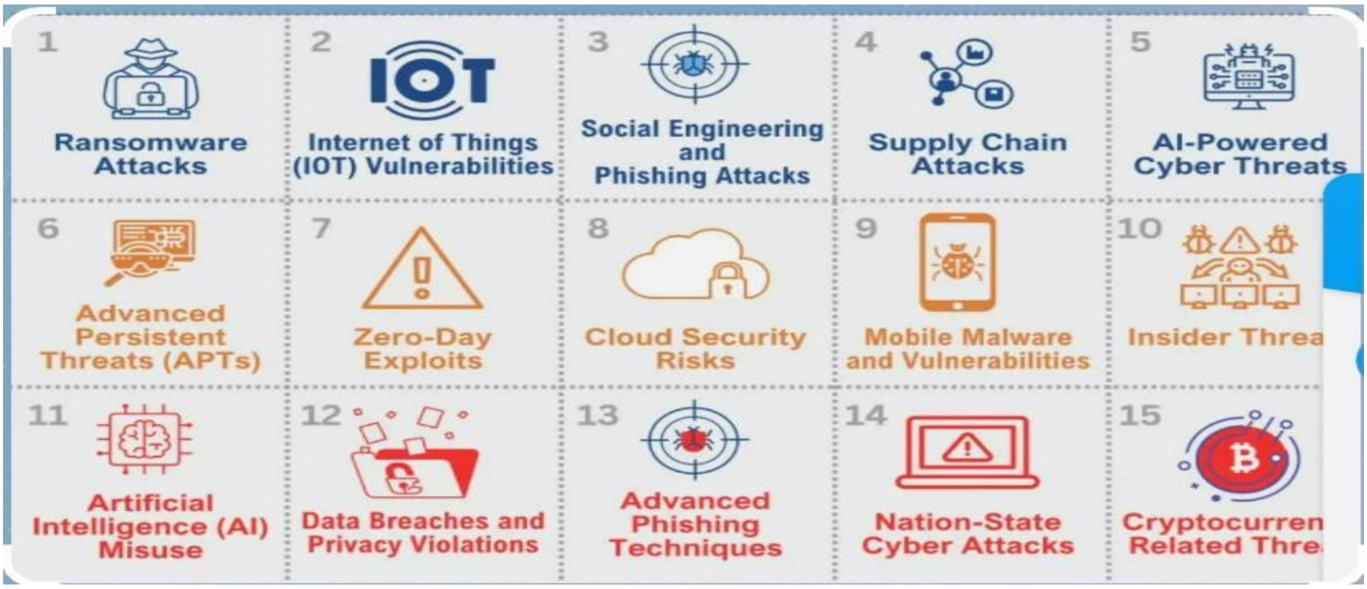

1
Ransomware Attacks
2
IOT
Internet of Things (IOT) Vulnerabilities
3
Social Engineering and Phishing Attacks
4
Supply Chain Attacks
5
AI-Powered Cyber Threats
6
Advanced Persistent Threats (APTs)
7
Zero-Day Exploits
8
Cloud Security Risks
9
Mobile Malware and Vulnerabilities
10
Insider Threa
11
Artificial Intelligence (AI) Misuse
12
Data Breaches and Privacy Violations
13
Advanced Phishing Techniques
14
Nation-State Cyber Attacks
15
Cryptocurren Related Thre

Fig 2: Top 15 Types Cyber Attacks

*B. IDS Classification*

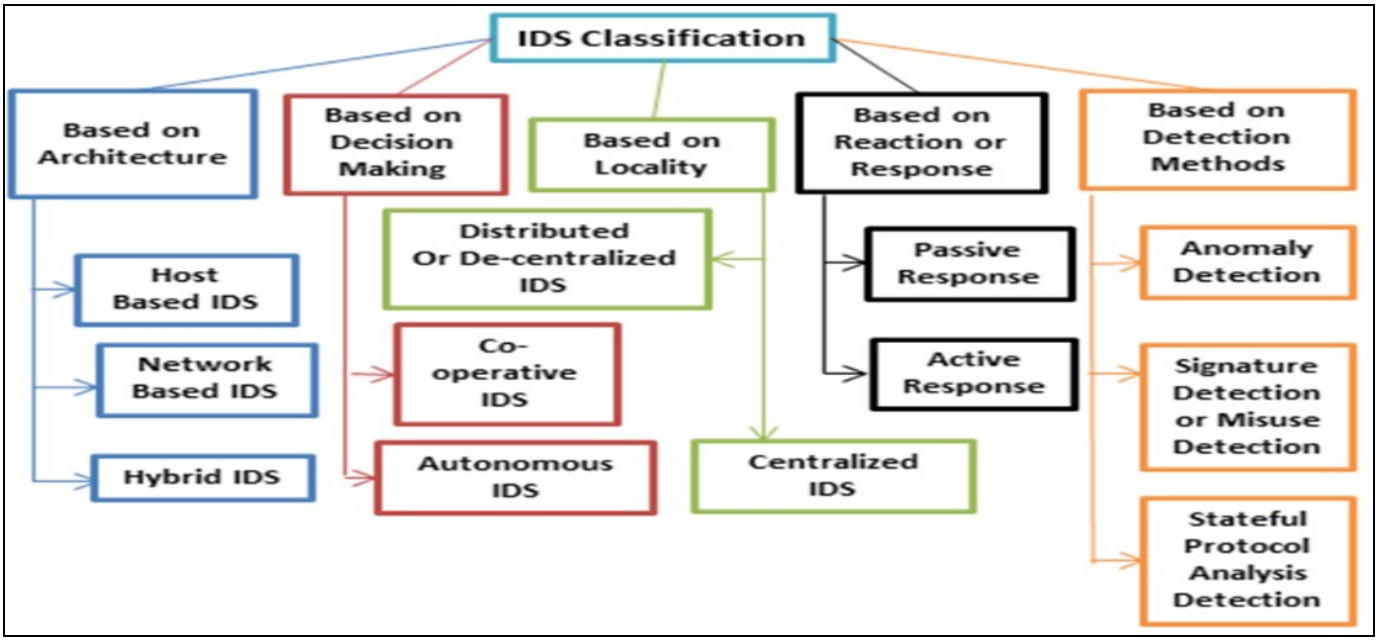


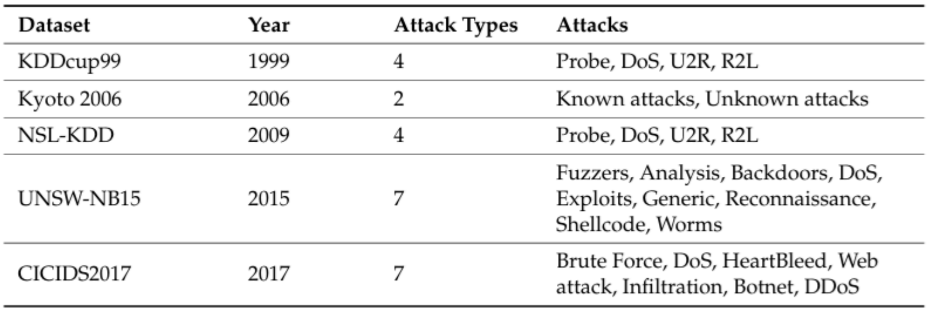
Fig 3: Taxonomy of IDS

## II. RELATED WORKS

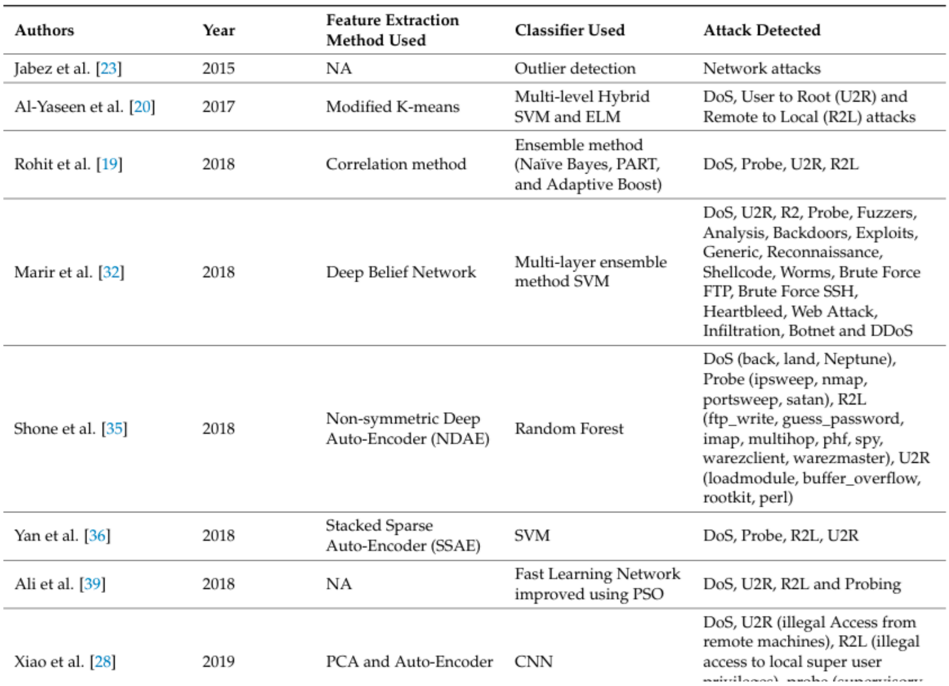
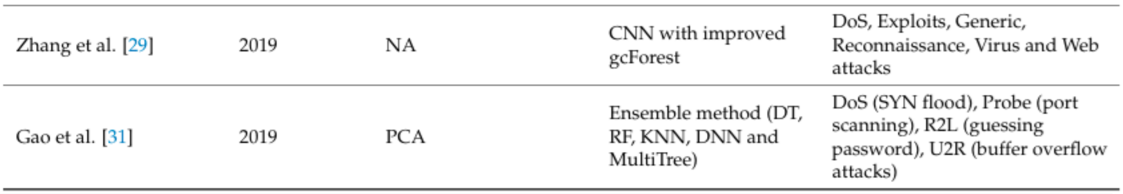
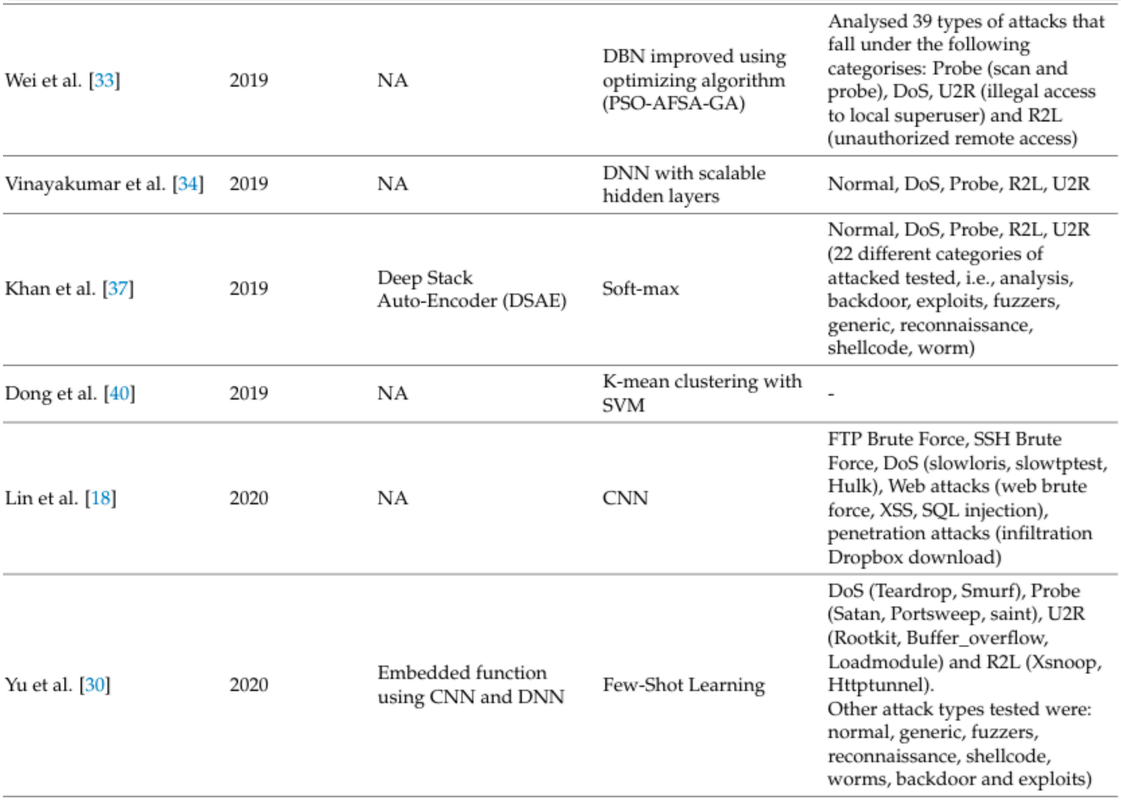
The Convolutional Neural Network (CNN) with a multi-layer perceptron as its model was utilized in the solution put forth by Lirim et al. [2]. A multi-layer perceptron can be thought of as a fully connected network in which each neuron in a layer corresponds to a single layer and is connected to every other layer's neuron. An input layer, hidden layers, and an output layer make up a CNN for neural networks. CNN-based IDS was also proposed by Lin et al. [4]. There are two components to their solution. The first involves offline training with CNN.

Using a maximum pooling layer and a series of convolutional layers, they reduce an input layer of 9 9 to an output layer of 1 1. Their online detection phase, which is the second portion of the system, uses Suricata, an opensource intrusion detection system, to intercept traffic. After that, the packets are pre-processed, and the network traffic is fed through the trained model to determine the detection result. A random forest algorithm-based intrusion detection system for wireless networks was developed by Yiping et al. [7]. Prior to developing the model to identify malevolent nonlinear scrambling intrusion signals, they developed a model for signal identification that captured the salient characteristics of signals. Static feature fusion and reinforcement learning techniques were utilized to provide the best possible detection of malicious traffic in a wireless network after the spectral properties of the malicious signal were extracted using an enhanced random forest algorithm. Their average accuracy was 96.93%. Guet al. [10] proposed a novel method that improves IDS by using SVM. They used the Naïve Bayes technique to choose features in their solution. They then trained the model using the modified data from the feature selection. To test their method, they utilized the CICIDS2017 and UNSW-NB15 datasets. The outcomes are superior than those obtained with the SVM classifier alone when Naïve Bayes is employed for feature extraction first. They really obtained 93.75% accuracy on the UNSW-NB15 dataset and 98.92% accuracy on the CICIDS2017 dataset.

Table 1: Datasets



| Dataset | Year | Attack Types | Attacks |
|---|---|---|---|
| KDDcup99 | 1999 | 4 | Probe, DoS, U2R, R2L |
| Kyoto 2006 | 2006 | 2 | Known attacks, Unknown attacks |
| NSL-KDD | 2009 | 4 | Probe, DoS, U2R, R2L |
| UNSW-NB15 | 2015 | 7 | Fuzzers, Analysis, Backdoors, DoS, Exploits, Generic, Reconnaissance, Shellcode, Worms |
| CICIDS2017 | 2017 | 7 | Brute Force, DoS, HeartBleed, Web attack, Infiltration, Botnet, DDoS |

| Authors | Year | Feature Extraction Method Used | Classifier Used | Attack Detected |
|---|---|---|---|---|
| Jabez et al. [23] | 2015 | NA | Outlier detection | Network attacks |
| Al-Yaseen et al. [20] | 2017 | Modified K-means | Multi-level Hybrid SVM and ELM | DoS, User to Root (U2R) and Remote to Local (R2L) attacks |
| Rohit et al. [19] | 2018 | Correlation method | Ensemble method (Naïve Bayes, PART, and Adaptive Boost) | DoS, Probe, U2R, R2L |
| Marir et al. [32] | 2018 | Deep Belief Network | Multi-layer ensemble method SVM | DoS, U2R, R2, Probe, Fuzzers, Analysis, Backdoors, Exploits, Generic, Reconnaissance, Shellcode, Worms, Brute Force FTP, Brute Force SSH, Heartbleed, Web Attack, Infiltration, Botnet and DDoS |
| Shone et al. [35] | 2018 | Non-symmetric Deep Auto-Encoder (NDAE) | Random Forest | DoS (back, land, Neptune), Probe (ipsweep, nmap, portsweep, satan), R2L (ftp_write, guess_password, imap, multihop, phf, spy, warezclient, warezmaster), U2R (loadmodule, buffer_overflow, rootkit, perl) |
| Yan et al. [36] | 2018 | Stacked Sparse Auto-Encoder (SSAE) | SVM | DoS, Probe, R2L, U2R |
| Ali et al. [39] | 2018 | NA | Fast Learning Network improved using PSO | DoS, U2R, R2L and Probing |
| Xiao et al. [28] | 2019 | PCA and Auto-Encoder | CNN | DoS, U2R (illegal Access from remote machines), R2L (illegal access to local super user privileges), probe (supervisory |
| Zhang et al. [29] | 2019 | NA | CNN with improved gcForest | DoS, Exploits, Generic, Reconnaissance, Virus and Web attacks |
| Gao et al. [31] | 2019 | PCA | Ensemble method (DT, RF, KNN, DNN and MultiTree) | DoS (SYN flood), Probe (port scanning), R2L (guessing password), U2R (buffer overflow attacks) |
| Wei et al. [33] | 2019 | NA | DBN improved using optimizing algorithm (PSO-AFSA-GA) | Analysed 39 types of attacks that fall under the following categorises: Probe (scan and probe), DoS, U2R (illegal access to local superuser) and R2L (unauthorized remote access) |
| Vinayakumar et al. [34] | 2019 | NA | DNN with scalable hidden layers | Normal, DoS, Probe, R2L, U2R |
| Khan et al. [37] | 2019 | Deep Stack Auto-Encoder (DSAE) | Soft-max | Normal, DoS, Probe, R2L, U2R (22 different categories of attacked tested, i.e., analysis, backdoor, exploits, fuzzers, generic, reconnaissance, shellcode, worm) |
| Dong et al. [40] | 2019 | NA | K-mean clustering with SVM | - |
| Lin et al. [18] | 2020 | NA | CNN | FTP Brute Force, SSH Brute Force, DoS (slowloris, slowtptest, Hulk), Web attacks (web brute force, XSS, SQL injection), penetration attacks (infiltration Dropbox download) |
| Yu et al. [30] | 2020 | Embedded function using CNN and DNN | Few-Shot Learning | DoS (Teardrop, Smurf), Probe (Satan, Portsweep, saint), U2R (Rootkit, Buffer_overflow, Loadmodule) and R2L (Xsnoop, Httptunnel).<br>Other attack types tested were: normal, generic, fuzzers, reconnaissance, shellcode, worms, backdoor and exploits) |

| | | | | |
|---|---|---|---|---|
| Andresini et al. [38] | 2020 | Dual Auto-Encoder | Soft-max | - |
| Elhefnawy et al. [42] | 2020 | Naïve Bayes | Hybrid Nested Genetic Fuzzy Algorithm | Probe, DoS, U2R, and R2L. Other attack types tested were: normal, generic, fuzzers, reconnaissance, shellcode, worms, backdoor and exploits) |
| Lirim et al. [17] | 2021 | NA | CNN with multi-layer perceptron | DoS, DDoS, PortScan, Web Attack, Heartbleed, Benign, Infiltration, Brute Force, SSH, FTP |
| Kanimozhi et al. [21] | 2021 | Logistic Regression | Oppositional tunicate fuzzy C-mean | - |
| Kurniawan et al. [24] | 2021 | Correlation-based features selection | Modified Naïve Bayes | Normal, DoS, Probe, R2L, U2R |
| Gu et al. [26] | 2021 | Naïve Bayes | SVM | - |
| Pan et al. [27] | 2021 | NA | KNN using PM-CSCA for optimization | DoS, Sniffing (Probe), U2R and R2L |

Table 2: Survey of Various Literatures

| Authors | Year | Feature Extraction Method Used | Classifier Used | Attack Detected |
|---|---|---|---|---|
| Wisanwanichthan et al. [41] | 2021 | ICFS and PCA | Naïve Bayes and SVM | Employed Double Layered Hybrid Approach (DLHA) for detecting DoS, Probe, R2L and U2R |
| Yiping et al. [22] | 2022 | NA | Improved random forest algorithm | Wireless network attacks |

## III. CHALLENGES OF IDS

### *A. Ensuring a Successful Implementation*

Organizations must make sure that the intrusion detection system they have chosen is properly deployed and optimized in order to get a high degree of threat visibility. Some intrusion detection technologies may not be feasible to incorporate throughout an IT environment due to financial and monitoring constraints. Deploying these solutions properly can be challenging, and if done incorrectly, it may leave important assets vulnerable. This is because many organizations do not have a comprehensive understanding of their IT network.

### *B. Handling the Large Number of Alerts*

For internal teams, the large volume of alerts produced by intrusion detection systems can be somewhat taxing. Organizations seldom have the time to investigate system alarms that are false positives

### *C. Comprehending and Examining Alerts*

It can take a lot of time and resources to investigate alarms found by intrusion detection systems, and additional data from other systems may be needed to assess the seriousness of an alarm. System output interpretation requires specialized knowledge, and many organizations lack the assistance of committed security professionals who can carry out this vital task.

### *D. Being able to React to Dangers*

A prevalent issue encountered by organizations striving to integrate intrusion detection systems is the absence of a suitable incident response capacity. Half the battle is won when an issue is recognized, but it also takes resources and knowledge to respond correctly. Good incident response necessitates both strong protocols to handle problems without interfering with regular operations and knowledgeable security professionals who know how to quickly neutralize threats. It might be challenging to accomplish quick remediation in many organizations because of the significant divide between the individuals in responsibility of monitoring warnings and those in charge of infrastructure management.

## IV.NEXT-GENERATION INTRUSION PREVENTION SYSTEMS (NGIPS)

A state-of-the-art cybersecurity tool called NextGeneration Intrusion Prevention System (NGIPS) is made to proactively identify and stop sophisticated threats in computer networks. Its main job is to provide real-time threat analysis, detection, and quick response capabilities. It also detects, notifies, and discourages malware attacks, unauthorized access, and data breaches. Protecting digital assets, vital infrastructure, and sensitive data from everchanging cyber threats is made possible in large part by NGIPS. Because cyberattacks are becoming more sophisticated and allow for the exploitation of weaknesses in networks and systems, NGIPS is critical.

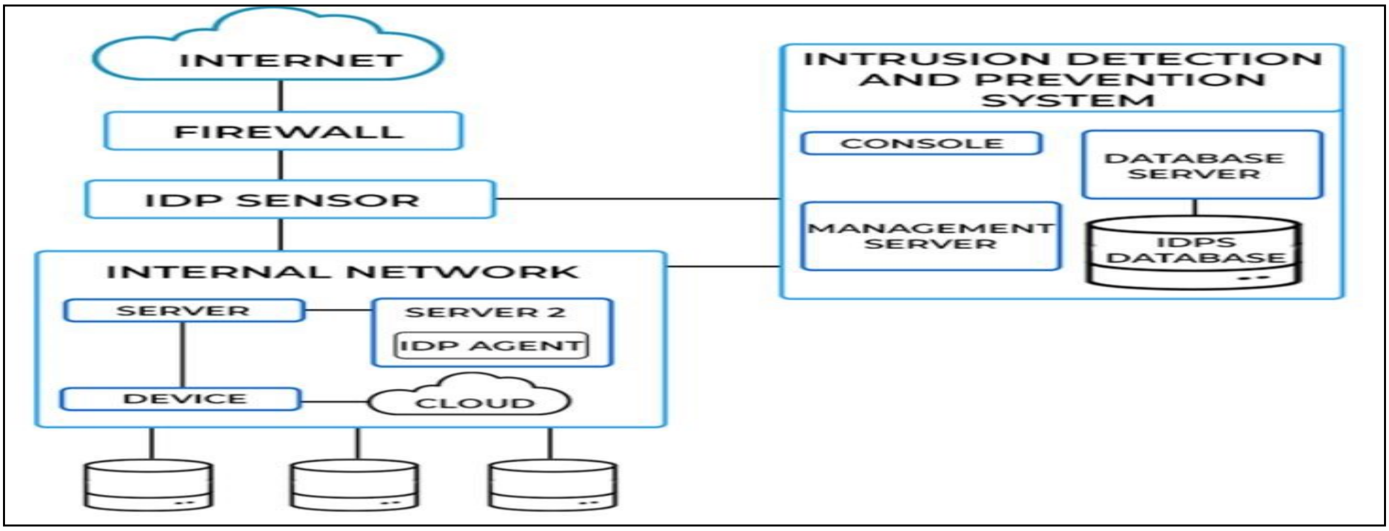


Fig 4: IDPS Working

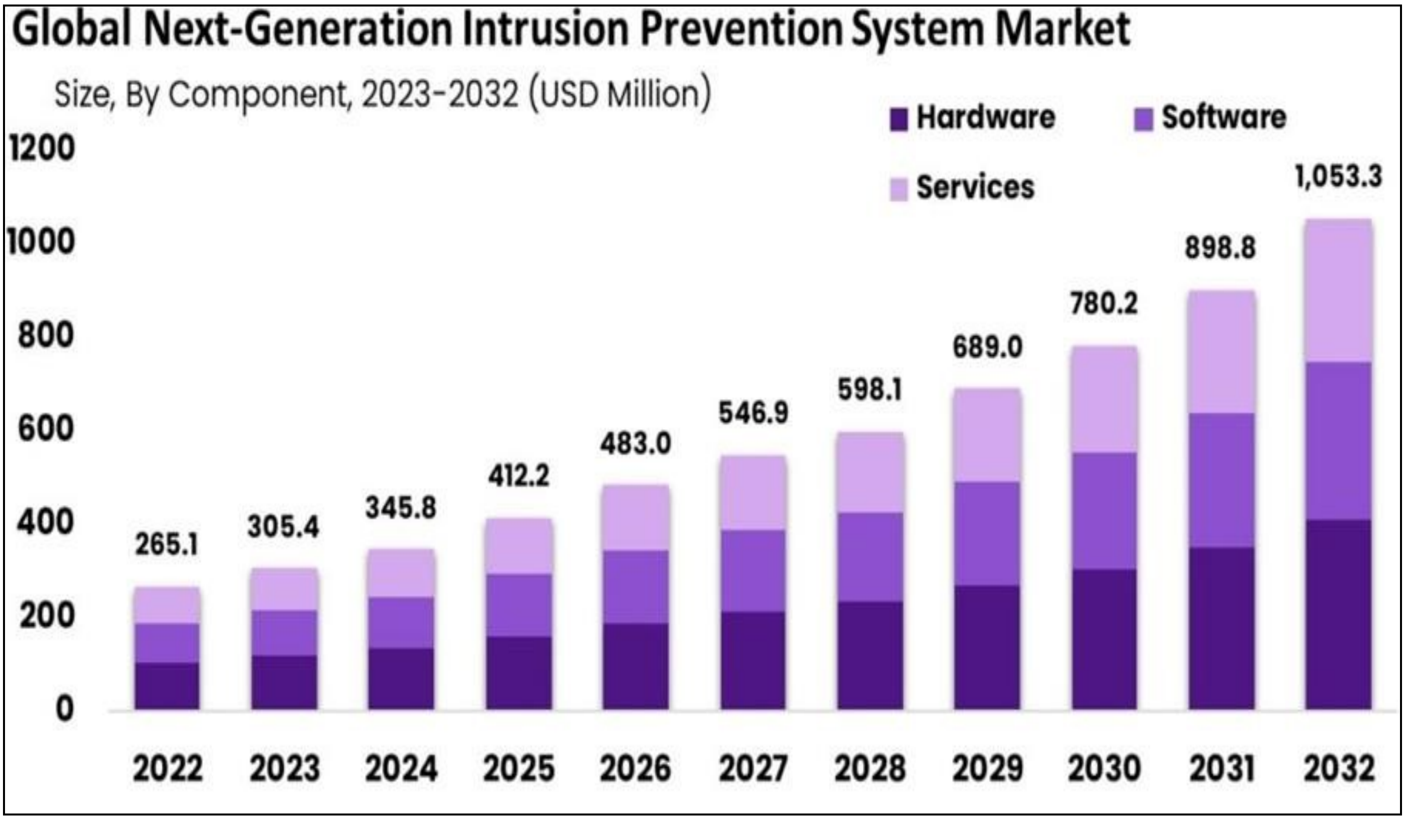


Fig 5: Bar Graph

## CONCLUSION

Nowadays, almost every international connection involving people, non-governmental organizations, authorities, and governmental institutions as well as commerce, economics, culture, social interaction, and government at all levels happens online. In recent years, cyberattacks and the risks associated with wireless communication technologies have grown to be significant concerns for many public and private organizations across the globe. Electronic technology plays a major role in modern life, and safeguarding this data from cyberattacks is a difficult problem. The goal of cyberattacks is to cause financial damage to businesses. An IDS can help speed up and automate network processes by monitoring devices and network traffic for known suspicious tasks. NextGeneration Intrusion Prevention System (NGIPS) alerts security administrators about known or potential dangers, or by sending alerts to a centralized security tool. This paper gives classification of different Recent and future possible Cyber Attacks.

## ACKNOWLEDGEMENT

I would like to express my profound gratitude to Dr. Kunjam Nageswara Rao Professor Department of Computer Science and System Engineering in Andhra University Andhra Pradesh, Visakhapatnam India, for giving Guidance and Support to Review and Given suggestion.

## AUTHOR CONTRIBUTION

All authors contributed to the study conception and design. Material preparation, data collection and analysis were performed by Katikam Mahesh, Dr Kunjam Nageswara Rao, and all authors commented on previous versions of the manuscript.

## CONFLICTS OF INTEREST

The authors declare no conflicts of interest

## REFERENCES

[1] Chen, Y.; Yuan, F. Dynamic detection of malicious intrusion in wireless network based on improved random forest algorithm. In Proceedings of the 2022 IEEE Asia-Pacific Conference on Image Processing, Electronics and Computers (IPEC), Dalian, China, 14–16 April 2022; pp. 27–32.

[2] Gu, J.; Lu, S. An effective intrusion detection approach using SVM with naïve Bayes feature embedding. Comput. Secur. 2021, 103, 102158. [CrossRef]

[3] Chen, L.; Kuang, X.; Xu, A.; Suo, S.; Yang, Y. A Novel Network Intrusion Detection System Based on CNN. In Proceedings of the 2020 Eighth International Conference on Advanced Cloud and Big Data (CBD), Taiyuan, China, 5–6 December 2020; pp. 243–247. [CrossRef]

[4] Sharafaldin, I.; Lashkari, A.H.; Ghorbani, A. Toward Generating a New Intrusion Detection Dataset and Intrusion Traffic Characterization; Canadian Institute for Cybersecurity (CIC): Fredericton, NB, Canada, 2018; pp. 108–116.

[5] Manu Bijone, and Jitendra Dangra, "A Survey of Signature Based & Statistical Based Intrusion Detection Techniques", IJSRD - International Journal for Scientific Research & Development, Vol. 4, Issue 08, pp. 583-585, 2016.

[6] A. Sawant, J. Yadav, A. K. Arora, J. Deo, and N. Dhange, "Intrusion Detection System using Data Mining," vol. 4, no. 2, pp. 4–7, 2015

[7] S. Sharma and R. K. Gupta, "Intrusion Detection System: A Review," vol. 9, no. 5, pp. 69–76, 2015.

[8] Kuang, F., Xu, W., and Zhang, S., "A novel hybrid KPCA and SVM with GA model for intrusion detection", Applied Soft Computing, vol. 18, pp.178-184, 2014.

[9] Ahmad, I., Hussain, M., Alghamdi, A., and Alelaiwi, A., "Enhancing SVM performance in intrusion detection using optimal feature subset selection based on genetic principal components" Neural Computing and Applications, 24(7-8), pp.1671-1682, 2014.

[10] F.N. Sabri, N.M. Norwawi, K. Seman, "Identifying false alarm rates for intrusion detection system with Data Mining", IJCSNS International Journal of Computer Science and Network Security, vol.11, 2011.

[11] Zorana Bankovic, Slobodan Bojanic, Octavio Nieto-Taladriz, and Atta Badii, "Increasing Detection Rate of User-to-Root Attacks Using Genetic Algorithms", International Conference on Emerging Security Information, Systems, and Technologies, IEEE, 2007.

[12] Jian P., Shambhu U., Faisal F., Venugopal G., "Data Mining for Intrusion Detection – Techniques, Applications and Systems", Data Mining Techniques for Intrusion Detection and Computer Security, University at Buffalo, New York, 2004.