*Research Journal of Computer and Information Technology Sciences* _____ISSN 2320 – 6527
Vol. **14(1),** 1-10, June **(2026)** *Res. J. Computer and IT Sci.*

***Review Paper***

# A comprehensive review of Network Attacks with Emphasis on DoS and DDoS Detection and Mitigation strategies

**Deepak Kumar Deshmukh* and Sanjay Kumar**
School of Studies in Computer Science & I.T., Pt. Ravishankar Shukla University, Raipur, Chhattisgarh, India
deepakdeshmukh.bit@gmail.com

**Available online at: www.isca.in**
Received 30th November 2025, revised 16th March 2026, accepted 6th April 2026

## Abstract

*This paper presents a comprehensive review of major network attacks and their mitigation strategies, emphasizing the growing threat of Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks. It examines essential cyber security principles—confidentiality, integrity, availability, authenticity, and non-repudiation—and outlines vulnerabilities, exploits, and classifications of active and passive attacks. The study reviews prominent attack vectors such as malware, ARP spoofing, IP spoofing, and Man-in-the-Middle (MITM) attacks, alongside conventional defense mechanisms including cryptographic algorithms, access control, and authentication protocols. Through an extensive literature survey, various mitigation frameworks based on statistical, cryptographic, and machine learning techniques are analyzed. The review identifies persistent challenges in detecting and mitigating DDoS attacks, particularly their distributed nature and stealth characteristics that evade conventional Intrusion Detection Systems (IDS) and firewalls. Findings highlight the necessity for adaptive, intelligent, and mathematically robust defense mechanisms, improved datasets, and standardized evaluation metrics to enhance resilience against evolving cyber threats.*

**Keywords:** Cyber security, DoS attack, DDoS mitigation, network security, spoofing, machine learning.

## Introduction

The Internet has emerged as an indispensable element for individuals across diverse sectors of society. It has facilitated interactions within the community, functioning not only to address economic requirements but also to fulfill social and cultural aspirations. The Internet has evolved into a formidable instrument that empowers individuals to augment their competencies. Nevertheless, in conjunction with its advantages, it has also introduced certain disadvantages that have yielded detrimental consequences.

Mr. Nitin Bansal articulates in his article in 'The Hindu' dated June 19, 2019, that India exhibits the highest average data consumption per smartphone, achieving 9.8 GB monthly by the end of 2018, as per a recent analysis by Ericsson. This statistic is anticipated to escalate to 18 GB monthly per smartphone by the conclusion of 2024[1].

In this regard, it is of utmost significance to ensure the protection of user data. Numerous conventional static approaches are available that provide solutions for data safeguarding; however, in the contemporary epoch of smartphones, where data threats are escalating at an alarming velocity, it becomes essential to formulate intelligent security solutions that can offer dynamic surveillance against data threats[1].

The concepts of Cyber Security and Network Security are often employed interchangeably. Cyber security can be delineated as the practice of ensuring the safety of cyberspace from damage or threats[2].

To commence, we must scrutinize the characteristics of cyber security, which are delineated as follows[2]:

**Confidentiality:** This characteristic aims to avert unauthorized users from accessing sensitive information. Cryptography operates as the mechanism through which data confidentiality is upheld[2].

**Integrity:** This principle assures that only authorized users are permitted to alter or obliterate data within cyberspace[2].

**Availability:** This aspect mandates that resources and information within cyberspace must be accessible in a prompt and dependable manner[2].

**Authenticity:** This provides assurance that the parties involved in communication are legitimate[2].

**Non-Repudiation:** This term pertains to the evidence that no entities engaged in communication can refute their actions of transmitting and receiving data[2].

The aforementioned characteristics contribute to the safeguarding of cyberspace. It is equally crucial to contemplate the potential threats to cyberspace so that suitable measures can be instituted to attain security for any system. Numerous threats are extant; nevertheless, some of the principal threats are encapsulated as follows:

**Vulnerability:** A vulnerability signifies a deficiency in system design, configuration, or process that renders the system open to attacks[2].

**Exploit:** An exploit constitutes a specific technique devised to capitalize on a vulnerability within a system to undermine its security[2].

**Attack:** An attack represents an endeavor by a threat actor to obtain unauthorized access to a system's services, resources, or information, or to compromise the system's integrity or its data. Attacks can be further categorized based on the nature of their operation[3].

Attacks can be classified into two primary categories: Active Attacks and Passive Attacks, each of which can be further subdivided into various types[3].

Active Attacks & Passive Attacks, where both can again encompass several types under them.

**Malware:** Malware is a kind of software that takes advantage out of vulnerabilities within a system by executing unauthorized functions or processes. Various manifestations of malware include viruses, worms, bots, adware, and Trojans.

William Stallings proposes several security mechanisms in his scholarly work , which are imperative to examine here, as these mechanisms are meticulously developed to deliver security services that ensure the safeguarding of a system, network, or cyberspace. He recommends the following security mechanisms[3]:

**Encipherment:** The utilization of mathematical algorithms to transmute data into an unintelligible format. The procedure of modification and ensuing retrieval of the data depends on a designated algorithm and one or several encryption keys[3].

**Digital Signature:** Data that is appended to, or a cryptographic modification of, a data unit which allows the recipient of the data unit to authenticate the provenance and integrity of the data unit, thus providing protection against counterfeiting.(for example, by the recipient)[3].

**Access Control:** A collection of mechanisms that enforce access rights to various resources[3].

**Data Integrity:** An assortment of mechanisms utilized to guarantee the integrity of a data unit or a sequence of data units[3].

**Authentication Exchange:** A mechanism designed to verify the identity of an entity through the means of information exchange[3].

**Traffic Padding:** The insertion of bits into voids within a data stream to hinder attempts at traffic analysis[3].

**Routing Control:** Facilitates the selection of specific physically secure paths for particular data and permits routing alterations, particularly when a security breach is suspected[3].

**Notarization:** The engagement of a trusted third party to ensure specific properties of a data exchange[3].

## Literature Review

For a substantive research endeavor, the formulation of research design is of paramount significance. As articulated by C. R. Kothari[4], the literature review serves a critical function in the establishment of a hypothesis pertinent to the specified research problem domain. The various phases of research are illustrated in Figure-1[4]. In the course of the literature survey, the literature was meticulously classified into three distinct categories; initially, those research papers were examined that provided a review of the chosen research domain, specifically addressing contemporary challenges in cyber security. Secondly, we analyzed those studies that propose data collection methodologies and instruments pertinent to the selected domain, and finally, individual security concerns along with their proposed solutions were systematically surveyed.

Jagpreet Kaur and K. R. Ramkumar[5], in their scholarly work titled "The Recent Trends in Cyber Security: A Review," conducted an extensive and meticulous examination of the prevailing body of literature pertinent to research endeavors situated within the domain of cyber or network security, prioritizing at the outset the critical task of recognizing and delineating the contemporary security challenges that currently confront both individuals and organizations in this rapidly evolving digital landscape. They systematically classified various types of cyber attacks and engaged in an in-depth discourse regarding security frameworks. The authors conducted an analytical evaluation of conventional cryptographic techniques, including RSA, DES, and AES, appraising their respective advantages and disadvantages, while simultaneously exploring emerging security paradigms.

Moreover, the authors conducted a survey of the scholarly contributions made by other researchers within the domain of cyber security. In conclusion, they presented a tabulated summary of their findings[5].

With the emergence of innovative Information and Communication Technology (ICT), the deployment of ICT products has experienced a significant escalation, thereby resulting in a corresponding increase in cyber attacks. This document elucidates the importance of the Common Criteria (CC), which stands as an international standard (ISO/IEC 15408) aimed at achieving cyber security certification[6].

The researchers endeavor to execute a comprehensive review of the Cyber Criteria (CC), elucidating its applications by synthesizing the existing body of literature alongside empirical findings obtained from the recent Development of Australian Cyber Criteria Assessment (DACCA) initiative[6]. i. A comprehensive and meticulous analysis of the prevailing trends concerning the adoption of the CC is undertaken. In

consideration of the challenges identified in the adoption of the CC, impediments to its implementation, both at the international and national levels, are critically examined[6]. ii. Recommendations, best practices, and potential future directions emerging from the analysis, along with solutions designed to address the challenges encountered in specifying security requirements within the framework of the CC, are articulated[6].

Lin et al. have elucidated methodologies and instruments pertinent to data collection technologies in their scholarly publication titled "A Survey on Network Security-Related Data Collection Technologies." In the process of conceptualizing a security model, algorithm, or data collection strategy, the authors propose various methodologies and tools for the execution of security analysis[7].

Initially, they define security-related data and conduct a comprehensive analysis of the methodologies, mechanisms, and technologies relevant to the collection of network data, employing the proposed criteria and objectives to evaluate their effectiveness in attaining high-quality network security-related data collection[7].

This manuscript encapsulates unresolved research dilemmas and advocates for prospective research trajectories within the realm of network security-related data collection, underpinned by a rigorous literature review and analytical discourse.

The primary aims associated with the collection of network data predominantly encompass 1) intrusion detection, 2) network management, 3) traffic accounting, 4) network forensics, and 5) malware detection.

Madhu K. Shankarapani et al.[8] have authored a paper entitled "Malware detection using assembly and API call sequences," which addresses the detection of malware through their proposed methodology predicated on API call sequences. The manuscript delineates malware as a significant security threat, accentuating the proliferation of malicious software as a consequence of increased internet utilization.

It examines various methodologies for malware detection, concentrating on signature-based and data mining techniques. The literature underscores the critical role of data mining within malware detection systems. It highlights persistent research challenges, particularly in the identification of malware exhibiting evolving signatures. The paper serves as a comparative reference for scholars and developers engaged in malware detection[8].

In their esteemed scholarly article titled "A prototype implementation and evaluation of the malware detection mechanism for IoT devices utilizing processor information," Takase et al.[9] put forth an innovative malware detection framework that skillfully capitalizes on values procured from the intricate activities of processors. The primary aim of their research is to effectively transition the crucial functionality of malware detection from software systems to hardware implementations, thereby aiming to achieve a significant reduction in the consumption of valuable hardware resources that are often strained in resource-constrained environments. To enhance the robustness of their framework, data extracted from processor activity is further enriched with supplementary information obtained through the utilization of the CBP Emulator, which serves as a pivotal tool in their experimental setup. The resultant Trace Data, which encapsulates the operational behavior of the processor, is meticulously directed towards a classifier that is specifically designed to fulfill the essential task of identifying the presence of malware within the system. In their classification scheme, the researchers categorize the various instructions into five distinct and well-defined categories, which include NOP (No Operation), LOAD, STORE, JUMP, and Other OP (Other Operations). By executing simulations of these operational commands, they are able to derive pertinent processor information, particularly emphasizing aspects such as locality, which can play a crucial role in identifying potential threats. The instruction set employed in their framework translates the commands NOP, LOAD, STORE, JUMP, and Other OP into corresponding numerical representations of 0, 1, 2, 3, and 4 respectively, thus facilitating a systematic approach to data interpretation. Furthermore, the proposed framework harnesses advanced machine learning methodologies to effectively classify malware instances, utilizing the Trace Data as an essential feature set that enables the detection process to be both efficient and accurate within the context of Internet of Things (IoT) devices.

Shaohua LV et al.[10] have introduced an innovative framework in their scholarly article titled "Intrusion Prediction with System-Call Sequence-to-Sequence Model," which articulates a sequence-to-sequence model meticulously crafted for the purpose of intrusion prediction. They elucidated a model grounded in system-call sequence-to-sequence prediction paradigms. This methodology encompasses two fundamental components. Firstly, it endeavors to mitigate the constraints inherent in extant anomaly detection systems while simultaneously addressing the short-term dependency challenges prevalent in contemporary system-call prediction algorithms through the deployment of a sequence-to-sequence system-call prediction model. Secondly, it aspires to augment the performance of baseline intrusion detection classifiers by assimilating the predicted sequence as an ancillary component alongside the invoked sequence, thereby producing an enhanced input. The sequence-to-sequence model fundamentally constitutes an application of Recurrent Neural Networks (RNNs) within the encoder-decoder framework. The training dataset is formulated utilizing the ADFA-LD, which is provided by The University of New South Wales, Australian Defense Force Academy.

Dinil Mon Divakaran et al.[11] have developed a comprehensive framework articulated in the paper entitled "Evidence gathering

for network security and forensics," which is adept at collecting evidentiary materials relevant to diverse categories of cyber attacks and malicious activities. Their investigation tackles the issue of evidentiary collection through a thorough analysis of network traffic. The evidences signify foundational patterns correlated with suspicious behaviors, accomplished by employing regression models to examine network traffic data and discern patterns indicative of questionable activities. The anomalous patterns, which constitute the evidences, are systematically correlated and scrutinized to enhance the efficacy of detecting traffic associated with attacks and malevolent activities, where efficacy is quantified in terms of detection accuracy and the prevalence of false positives.

Y. Li et al.[12] encapsulate the entirety of the methodology under the overarching theme "Framework for evidence gathering," wherein they introduce the framework dedicated to evidentiary collection[12]. The techniques based on regression modeling and analytical processes for the identification of anomalous patterns are expounded in the section titled "Regression analysis for detection of anomalous patterns[12]." The ultimate criteria for decision-making concerning the anomalous nature of one or more traffic flows are grounded in the evidences amassed, which is elaborated upon in the section "Decision making based on evidences gathered[12]." Finally, the experiments conducted are presented alongside a discussion of the resultant findings in the section Performance evaluations.

Marcin Gregorczyk[13] and collaborators developed a methodology based on machine learning and network traffic probing for the identification of sniffing attacks, which are categorized as a form of passive attack. Passive attacks present considerable difficulties with respect to their detection; nonetheless, certain mechanisms are available that may aid in the forecasting of such incidents. Sniffing is typically executed utilizing specialized software referred to as sniffers, with notable instances being TcpDump and Wireshark. These instruments confront the menace of sniffing within the cybersecurity paradigm of the Internet of Radio-Light (IoRL) system, which is presently under construction as part of the Horizon 2020 initiative. The proposed detection methodology specifically targets the sniffing application.

This methodology encompasses five discrete phases: 1. Identification of Suspicious Machine 2. Continuous dispatch of network probes 3. Documentation of responses 4. Periodic imposition of artificial load 5. Application of ML techniques to discern sniffing activities.

Hossein Hadian Jazi et al.[14] investigated the detection of application layer Denial of Service (DoS) attacks. In this research endeavor, a more expansive detection framework was utilized, employing CUSUM (Cumulative Sum)-based methodologies to tackle various manifestations of DoS attacks, including flooding attacks, at the application layer. The authors executed thirteen distinct sampling techniques for the purpose of anomaly detection, which are delineated as follows: Systematic packet sampling, Random n-out-of-N sampling, Random packet sampling, Adaptive random sampling, Random flow sampling, Smart sampling, Sample-and-hold sampling, Sketch-guided sampling, IP flow-based sampling, Adaptive weighted sampling, algorithm, Fast filtered sampling, Selective flow sampling, Adaptive traffic sampling.

Ismail et al. composed a scholarly article titled "A Machine Learning-Based Classification and Prediction Technique for DDoS Attacks"[15], wherein they introduced a machine learning approach aimed at the classification and forecasting of diverse categories of DDoS attacks. To substantiate their research, they outlined an exhaustive framework designed for the prediction of DDoS incidents. For their empirical analysis, the UNWS-np-15 dataset was obtained from a GitHub repository, with Python serving as the primary tool for simulation. Data manipulation was executed using both Python and Jupyter Notebook. Additionally, the dataset was categorized into two separate classes: the dependent class and the independent class. The framework is comprised of the following essential steps[15]. i. The preliminary phase entails the selection of an appropriate dataset for implementation[15]. ii. The following phase involves the identification of relevant tools and programming languages[15]. iii. The third phase is dedicated to the execution of data preprocessing techniques aimed at eliminating extraneous data from the dataset. In the fourth phase, feature extraction and labeling are performed[15]. iv. Encoding is conducted to transform categorical data into numerical representations[15]. v. The fifth stage encompasses the segmentation of data into training and testing sets for the model. During this stage, the proposed model is developed and trained. Additionally, model optimization is performed on the trained model, focusing on kernel scaling and hyper-parameter tuning to enhance model performance. Upon completion of optimization, the model will produce output results15[15].

Rana Abubakar et al.[16] proposeda methodology for an Intrusion Prevention System (IPS) that allows traffic deemed legitimate to navigate through the network, whilst concurrently flagging suspicious traffic for further examination via an identification system. We furnish the algorithm along with empirical results that illustrate enhanced performance when compared to the fundamental Snort IPS, Probabilistic Neural Network (PNN), Back Propagation (BP), Chi-square, and Particle Swarm Optimization – Support Vector Machine (PSO-SVM) in terms of accuracy, exposure, and specificity.

Steven Simpson et al.[17] present Antidose, a mechanism designed to enhance the interaction between a susceptible peripheral service and an indirectly linked Autonomous System (AS), thereby enabling the AS to proficiently conduct localized filtering with discretion as guided by the remote service. Antidose comprises a variety of packet formats, protocols, and functions that an AS may selectively implement to differing extents, thereby allowing it to mitigate a Distributed Denial of

Service (DDoS) attack on a target of which it lacks direct awareness. This paper outlines multiple contributions: it motivates and articulates the proposal of Antidose; it elucidates the structure and computation of proofs and cookies (the essential components of Antidose) as well as the interactions among ASes (nodes) for their interchange; it operationalizes the principal Antidose element as a data-plane function to be integrated within the network switching architecture; and it clarifies the influence of Antidose on recognized 'good' traffic in contrast to other traffic, demonstrating that false positives (i.e., 'other' traffic mistakenly permitted) remain at minimal levels, even amidst numerous distinct 'good' flows.

Khalaf et al.[18] in their paper entitled "Comprehensive Review of Artificial Intelligence and Statistical Approaches in Distributed Denial of Service Attack and Defense Methods" examines the leading defense mechanisms against DDoS attacks that leverage artificial intelligence and statistical methods. Additionally, the review classifies and clarifies the various types of attacks, testing attributes, evaluation techniques, and datasets utilized within the scope of the proposed defense methodologies. Ultimately, this review offers recommendations and potential areas for the development of improved solution frameworks related to DDoS attack defense mechanisms. The authors have conducted a comparative evaluation of DDoS attack solutions based on various criteria set forth by multiple researchers, presenting their conclusions in a structured tabular format. The review encompasses a thorough total of 129 scholarly articles, six network security publications, ten dataset references, and six review articles. It is relevant across web applications, web servers, web services, cloud computing, and any internet-enabled device. The review provides a complete and meticulously thorough analysis of the statistical and artificial intelligence techniques utilized in the detection and mitigation of DDoS attacks[18].

James Halladay et al.[19] present and scrutinize the efficacy of 25 time-based features aimed at detecting and classifying 12 distinct types of DDoS attacks through the utilization of both binary and multiclass classification methodologies. The authors have conducted a comparative assessment of existing literature concerning DDoS traffic detection.

Daliya Nashat et al.[20] present a novel detection framework for HTTP flooding attacks, utilizing the Susceptible-Infective-Susceptible (SIS) model, which is conventionally employed in the examination of infectious diseases within dynamic systems. Throughout any specified temporal interval, the server is equipped to quantify diverse user attribute metrics, encompassing the aggregate number of connections, the enumeration of active connections, and the summation of terminated connections. These metrics can be utilized to discern any irregular behavior or compromised connections within the server by correlating these attributes with the SIS model. As a result, it becomes viable to detect suspected and infected connections during each designated time period.

Ghaben et al.[21] executed a thorough analysis and assessment of twenty-two pre-existing mechanisms for DDoS attack detection, incorporating all classifications of DDoS attack mitigation strategies, in order to elucidate the fundamental reasons for the persistent efficacy of DDoS attacks. This investigation posits two hypotheses concerning the observed discrepancy: Firstly, there exists an insufficient application of mathematical functions within the extant detection mechanisms. The functions that are utilized are predominantly restricted to logical, statistical, or probabilistic operations, thereby diminishing the comprehensive effectiveness of detection. Secondly, researchers may inadvertently miscalculate the accuracy rate of these mechanisms by employing quantitative metrics in a partial manner.

Xin Wang et al.[22] In their academic article, by simulating link flooding attacks alongside corresponding defensive strategies, we address a series of inquiries pertaining to the practical challenges associated with LFAs. The primary aim of LFAs is to inundate the target link, thereby severing the intended victim's network from the larger network. The presented formulation demonstrates that LFAs can be effectively countered through traffic engineering techniques examined from a game-theoretic perspective.

Marinos Dimolianis and colleagues[23], in their 2021 research publication, introduce an innovative framework for the classification and filtering of Distributed Denial of Service (DDoS) traffic that operates independently of source IP addresses, which they refer to as a source IP-agnostic approach. This framework employs advanced supervised Machine Learning techniques to effectively identify the unique signatures of malicious packets, a critical step in developing robust cybersecurity measures, and subsequently establishes protocols for filtering based on these identified signatures in a manner that is both efficient and adaptive to evolving threats. In contrast to traditional DDoS defense mechanisms, which typically depend on statistical data gleaned from source IP addresses or overall network flows in an effort to detect and counteract harmful traffic, this new methodology presents a significant advancement in the field. Their proposed system is designed to provide DDoS protection that is not reliant on the identification of source IPs, thereby enhancing its effectiveness in classifying various types of network attacks and mitigating them based solely on the distinctive packet signatures, which are defined as unique combinations of values found within packet fields. This innovative approach not only broadens the scope of DDoS defense strategies but also marks a pivotal shift towards a more nuanced and sophisticated understanding of network security challenges. By embracing this source IP-agnostic framework, network administrators may significantly improve their ability to thwart malicious activities and safeguard their infrastructure against increasingly sophisticated DDoS threats.

Arwa Badhib et al.[24] presented a scholarly paper titled "A Robust Device-to-Device Continuous Authentication Protocol

for the Internet of Things," which introduces a swift and secure device-to-device continuous authentication protocol predicated on device characteristics (token, battery, and location) and mitigates DoS attacks through the implementation of shadow IDs and emergency keys. Furthermore, it takes into account the mobility of sensors while ensuring the maintenance of privacy. To evaluate the robustness and validate the security of the proposed protocol, both informal and formal analyses were conducted utilizing Scyther. Additionally, performance assessments were performed to ascertain computational costs in relation to system counterparts. The findings indicate that the protocol demonstrates robust defenses against security threats while incurring acceptable computational expenses.

Abdulrahman Alhothaily et al.[25] propose a highly efficient and practical user authentication framework that employs personal devices utilizing a diverse array of cryptographic primitives, including encryption, digital signatures, and hashing techniques. This innovative approach capitalizes on the widespread integration of ubiquitous computing alongside various intelligent portable and wearable devices, thereby empowering users to implement a secure authentication protocol. The proposed framework obviates the necessity for an authentication server responsible for managing static username and password databases, which are traditionally employed for the identification and verification of legitimate users attempting to log in. It is meticulously designed to be resilient against password-related attacks and demonstrates a capacity to withstand replay attacks, shoulder-surfing incidents, phishing attempts, and occurrences of data breaches.

Daemin Shin et al.[26] present a comprehensive route optimization protocol meticulously crafted for smart home systems that utilize Device Mobility Management (DMM). The proposed security framework, which encompasses both the initialization and handover phases of route optimization, is expertly designed to facilitate mutual authentication, enable key exchange, maintain perfect forward secrecy, and ensure privacy protection. The robustness of its security architecture has been thoroughly assessed through the application of two formal security analysis tools, specifically BAN-logic and Automated Validation of Internet Security Protocols and Applications (AVISPA). Comparative evaluations indicate that the proposed protocol considerably surpasses other existing protocols in terms of efficiency.

Suhail Hussain et al.[27] promote the utilization of Message Authentication Code (MAC) algorithms, particularly Hash-based Message Authentication Code (HMAC) and Advanced Encryption Standard-Galois Message Authentication Code (AES-GMAC), to ensure the integrity of GOOSE messages. Controlled laboratory experiments are performed to assess the timing efficiency and practicality of these algorithms for deployment in GOOSE scenarios. A software library has been established to support the secure generation of GOOSE messages utilizing HMAC and GMAC-based MAC algorithms. The packet dimensions and timing efficiencies of these algorithms are rigorously evaluated to ascertain their appropriateness for enhancing cybersecurity for GOOSE messages. Laboratory results reveal that all algorithms are capable of maintaining secure communication effectively. Additionally, the detected avalanche effect suggests that truncated versions with minimized Protocol Data Unit (PDU) sizes may represent the most advantageous approach for achieving a balance between security and timing requirements.

Nivedita Mishra et al.[28] provide an extensive review that tackles a multitude of security issues faced across the different layers of the Internet of Things (IoT): the perception layer, network layer, support layer, and application layer, with a specific emphasis on Distributed Denial of Service (DDoS) attacks. DDoS attacks pose considerable risks within the cybersecurity landscape due to their ability to disrupt targeted entities. The discussion includes an examination of various forms of DDoS attacks, their effects on IoT devices, and potential countermeasures. The review rigorously assesses Intrusion Detection and Prevention systems designed to combat DDoS attacks, with a particular focus on Intrusion Detection systems. Moreover, it investigates the categorization of Intrusion Detection Systems, a range of anomaly detection methods, different models of Intrusion Detection Systems based on datasets, and the utilization of various machine learning and deep learning techniques for data preprocessing and malware identification[28].

Yasmine Harbi et al.[29] aim to provide a modern synthesis of the key research topics concerning the security of the Internet of Things (IoT). To begin, the essential elements and protocols associated with IoT are outlined to elucidate the sources of threats in this domain. Following this, a categorization of IoT attacks is presented, along with an analysis of the security vulnerabilities present at different levels of IoT infrastructure. Subsequently, a comparative evaluation of current security frameworks based on innovative solutions—including fog computing, edge computing, software-defined networking (SDN), block chain technology, lightweight cryptography, homomorphic and searchable encryption, as well as machine learning—is conducted. In conclusion, the paper addresses existing security challenges and delineates potential future directions for researchers in this field.

Zaman et al.[30] undertook an in-depth, comprehensive analysis that meticulously examined the multifaceted security threats associated with the Internet of Things (IoT) on a layer-by-layer basis, while also introducing various security models that leverage the power of artificial intelligence (AI) to effectively mitigate and address these pressing threats. In addition to this, the manuscript goes on to provide a thorough elucidation of the myriad challenges currently faced within the realm of IoT, as well as delineating promising research pathways that are intended to significantly enhance the protective measures surrounding IoT networks. The authors conducted a rigorous assessment of a diverse array of existing security

methodologies, while simultaneously outlining a range of unresolved issues that remain pertinent, alongside identifying potential areas for further academic investigation that could yield valuable insights. Given that the foundational theoretical constructs underpinning AI and machine learning (ML) are still in a state of relative underdevelopment, it becomes increasingly evident that specific strategies aimed at optimizing the operational performance of AI and ML models require additional thorough clarification and exploration. Furthermore, a variety of emerging learning methodologies, along with innovative visualization techniques, are poised to play a crucial role in achieving an accurate and comprehensive understanding of data, thereby facilitating enhanced data interpretation and analysis. In this context, the imperative for ongoing research and development in these fields cannot be overstated, as advancements in technology continue to evolve at a rapid pace. As such, it is essential for scholars and practitioners alike to remain vigilant and proactive in addressing the dynamic challenges posed by IoT security. The interplay between AI, ML, and IoT represents a fertile ground for innovation, necessitating a concerted effort to explore new solutions that can effectively safeguard these interconnected systems. Ultimately, the pursuit of knowledge in this area is not only beneficial but essential for the advancement of secure and resilient IoT infrastructures.

## Comparative Analysis

In order to deliver a comprehensive and structured overview of the current research landscape that exists in the field, a meticulously crafted comparative summary of the works that have been surveyed is presented in the form of Table 1. This table serves the dual purpose of providing a thorough comparison of the various methods that have been suggested in the relevant academic papers. Within this table, significant details pertaining to each referenced work are consolidated, which includes essential information such as the title of the paper, the names of the authors, the venue of publication along with the year of publication, and the specific reference number that is employed throughout this study. Furthermore, the table delineates the fundamental methodology that has been adopted in each of the works analyzed, accompanied by a succinct indication of its overall effectiveness in addressing the respective research questions. This comparative analysis not only elucidates the diverse methodologies that have been utilized to tackle pressing network security issues, but also encompasses critical areas such as malware detection and the mitigation of Distributed Denial of Service (DDoS) attacks. The structured format of the table significantly facilitates the identification of shared strengths and weaknesses, as well as the limitations and research gaps that currently exist, particularly with respect to the challenges posed by advanced DDoS attacks and the larger scope of network threats that can impact organizations. Through this thorough examination, researchers and practitioners can gain valuable insights into the current state of the art in network security methodologies, enabling them to build upon existing frameworks and address unresolved issues in future research endeavors. Ultimately, this detailed comparative summary serves as a vital resource for anyone looking to deepen their understanding of the methodologies employed in the realm of network security research.

**Table-1:** Comparison of Methods suggested in papers.

| Ref. No. | Methodology Used | Effectiveness / Conclusions |
|---|---|---|
| 5 | Systematic literature review of cyber/network security; classification of attacks and security frameworks; analysis of RSA, DES, AES and emerging paradigms. | Provides structured taxonomy of attacks/frameworks and highlights current cybersecurity challenges; no quantitative performance metrics. |
| 6 | Systematic review of Common Criteria (CC) applications; synthesis of literature plus empirical insights from DACCA project on CC adoption. | Explains role of CC in cybersecurity certification, identifies adoption barriers, and proposes recommendations and best practices; no detection metrics. |
| 7 | Survey defining "security-related data"; comparative analysis of methods, mechanisms, technologies for network data collection against quality/requirement criteria. | Clarifies strengths and limitations of data collection techniques; identifies open research problems and future directions. |
| 8 | Proposed malware detection using assembly and API call sequences; compares signature-based and data-mining approaches. | Shows that sequence-based features are effective for malware detection; highlights difficulty of handling malware with evolving signatures. |
| 9 | Hardware-oriented framework using processor activity traces (NOP/LOAD/STORE/JUMP/Other) and machine learning classifier over trace data. | Demonstrates feasibility of malware detection on IoT devices using processor information with minimal extra hardware resources. |
| 10 | RNN encoder–decoder (seq2seq) model to predict system-call sequences; uses ADFA-LD dataset; combines predicted + invoked sequences as IDS | Improves performance of baseline intrusion detection classifiers and mitigates short-term dependency issues in earlier models. |

| | | |
|---|---|---|
| | features. | |
| 11 | Framework for evidence collection using regression models on network traffic to detect anomalous patterns, correlate evidences, and make decisions. | Achieves effective detection of malicious traffic; performance expressed in terms of detection accuracy and false positive rate. |
| 12 | Literature-based analysis proposing a five-stage situational awareness framework (Factor Acquisition, Model Representation, Measurement, Evolution, Prediction). | Provides conceptual framework to overcome limitations of IDS and structure situational awareness research; no empirical performance given. |
| 13 | Active network probing plus machine learning to detect sniffing (passive) attacks in IoRL; steps: identify suspicious machine, probe, log responses, add artificial load, classify. | Shows that sniffing attacks can be detected via probing and ML even though they are passive; your text does not quote exact rates. |
| 14 | CUSUM-based detection framework using 13 different packet/flow sampling strategies for anomaly detection at application layer. | Demonstrates that proper sampling combined with CUSUM can detect HTTP DoS/flooding under sampling; compares effectiveness of sampling methods. |
| 15 | ML pipeline on UNSW-NB15-like dataset using Python/Jupyter: preprocessing, feature extraction & labeling, encoding, train/test split, hyperparameter tuning and kernel scaling. | Provides accurate classification and prediction of DDoS attack types; optimization improves efficiency of the trained model. |
| 16 | Intrusion Prevention System (IPS) mechanism that forwards legitimate traffic and flags suspicious traffic; experimental comparison vs Snort IPS, PNN, BP, Chi-square, PSO-SVM. | Shows superior accuracy, exposure, and specificity over baseline IPS/ML approaches for real-time DDoS mitigation. |
| 17 | "Antidose" protocol and packet formats enabling collaboration between vulnerable service and remote ASes; data-plane implementation in switching fabric. | Enables remote ASes to filter DDoS traffic while keeping false positives minimal even with many distinct legitimate flows. |
| 18 | Large-scale survey of 129 papers + reports/datasets; comparative analysis of AI and statistical DDoS defenses across environments and evaluation setups. | Exhaustive synthesis of AI/statistical DDoS defenses; provides guidelines and research directions rather than new experimental results. |
| 19 | Evaluates 25 time-based traffic features with binary and multiclass classifiers to detect and classify 12 DDoS attack types. | Identifies effective time-based features and demonstrates strong detection and classification performance; exact metrics not quoted in your text. |
| 20 | Uses SIS epidemic model; server measures user attributes (total, open, closed connections) over time to detect suspicious/infected connections. | Allows identification of suspected and infected connections during each time interval for HTTP flooding attacks; quantitative results not detailed in your text. |
| 21 | Analytical evaluation of 22 DDoS detection mechanisms, focusing on mathematical functions and metric usage. | Concludes that limited mathematical rigor and partial use of metrics can overestimate accuracy, explaining why DDoS attacks still succeed; calls for better metrics. |
| 22 | Simulation-based study of link flooding attacks and defenses; formulates traffic engineering defenses from a game-theoretic viewpoint. | Shows that properly designed traffic engineering can mitigate LFAs and discusses practical deployment challenges. |
| 23 | Supervised ML to learn malicious packet signatures (field combinations); implements signature-based filtering in programmable data planes. | Provides IP-agnostic DDoS mitigation with fine-grained filtering; improves upon traditional IP/flow-based approaches. |
| 24 | Continuous authentication protocol using device token, battery, location; employs shadow IDs and emergency keys; verified with Scyther plus performance evaluation. | Demonstrates robust protection against security threats (including DoS) with acceptable computational cost,even with sensor mobility. |
| 25 | Authentication framework leveraging personal/wearable devices and cryptographic primitives (encryption, signatures, hashing) without traditional password DB server. | Resilient to password attacks, replay, shoulder-surfing, phishing, and data breaches; improves usability and practical security. |
| 26 | Route-optimization security protocol covering initialization and handover; ensures mutual authentication, key exchange, forward secrecy, privacy; | Outperforms existing protocols in security features and effectiveness for DMM-based smart home IoT networks. |

| | | |
|---|---|---|
| | verified via BAN-logic and AVISPA. | |
| 27 | Implements HMAC and AES-GMAC MAC algorithms for securing GOOSE messages; lab tests on timing and packet size; software library for secure GOOSE. | All algorithms sustain secure communication; truncated MACs with smaller PDUs provide best balance between security and timing. |
| 28 | Systematic review of IoT applications and security; layer-wise discussion of attacks (esp. DDoS) and IDS/IPS models, anomaly detection, ML/DL-based approaches. | Offers comprehensive view of IoT security challenges and IDS solutions; identifies gaps and future research needs rather than new metrics. |
| 29 | Survey of IoT components/protocols; proposes taxonomy of IoT attacks; analyzes vulnerabilities and compares emerging security frameworks (fog, edge, SDN, blockchain, etc.). | Summarizes current IoT security trends and frameworks; highlights open challenges, no new quantitative evaluation. |
| 30 | Layer-wise survey of IoT threats and AI-based security models; evaluates security strategies and outlines open issues and research directions. | Shows potential and limitations of AI/ML for IoT security; stresses need for stronger theoretical foundations and optimization techniques. |

## Conclusion

This comprehensive review has explored major network attacks, with a particular focus on Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks, alongside their detection and mitigation strategies. The paper highlights the critical importance of cybersecurity principles such as confidentiality, integrity, availability, authenticity, and non-repudiation in safeguarding cyberspace. It also categorizes attack vectors, including malware, ARP spoofing, IP spoofing, and Man-in-the-Middle (MITM) attacks, and discusses conventional defense mechanisms like cryptographic algorithms and access control.

**Persistent Challenges in DDoS Detection:** Despite advancements, persistent challenges remain in effectively detecting and mitigating DDoS attacks, primarily due to their distributed nature and stealth characteristics. Traditional Intrusion Detection Systems (IDS) and firewalls often prove insufficient against these sophisticated threats. The literature review underscores the need for adaptive, intelligent, and mathematically robust defense mechanisms, improved datasets, and standardized evaluation metrics to enhance resilience against evolving cyber threats. Several studies reviewed emphasize the limitations of current approaches and the need for more dynamic solutions.

**Advancements in Detection and Mitigation Techniques:** The survey identifies various methodologies for addressing network security issues, including malware detection and DDoS mitigation. Machine learning techniques, for instance, have shown promise in classifying and predicting DDoS attacks, with some frameworks demonstrating improved performance over baseline methods. Other approaches include hardware-oriented frameworks for malware detection on IoT devices, CUSUM-based detection for application layer DoS attacks, and Intrusion Prevention Systems (IPS) that leverage machine learning for real-time DDoS mitigation. The paper also discusses the importance of secure authentication protocols and robust route optimization in smart home systems to enhance overall security.

**Future Directions and Research Gaps:** The review collectively points to several research gaps and future directions. There is a continuous need for stronger theoretical foundations and optimization techniques for AI/ML-based security models. The complexity of IoT environments introduces unique security challenges, necessitating specialized solutions for DDoS attacks and other threats across various layers of the IoT infrastructure. Overall, the paper serves as a valuable resource by providing a structured overview of the current research landscape, highlighting the strengths and limitations of existing methods, and identifying areas for future investigation to combat the ever-evolving landscape of cyber threats.

## References

**1.** Report (2022). At 9.8 GB per month, India has the highest data usage per smartphone. *The Hindu*, Jun. 19, 2019. Accessed: Jul. 11, 2022. Available: https://www.thehindu.com/

**2.** T. W. Edgar and D. O. Manz (2017). *Research methods for cyber security*. Cambridge, MA: Syngress, an imprint of Elsevier.

**3.** W. Stallings (2011). *Network security essentials: applications and standards.* 4th ed. Boston: Prentice Hall.

**4.** C.R. Kothari (2004). *Research methodology: methods & techniques*. New Delhi: New Age International (P) Ltd., Publishers.

**5.** J. Kaur and K. . R. Ramkumar (2021). The recent trends in cyber security: A review. *J. King Saud Univ. - Comput. Inf. Sci.*, p. S1319157821000203.

**6.** Sun, N., Li, C. T., Chan, H., Le, B. D., Islam, M. Z., Zhang, L. Y., ... & Armstrong, W. (2022). Defining security

requirements with the common criteria: Applications, adoptions, and challenges. *IEEE Access*, 10, 44756-44777.

**7.** Lin, H., Yan, Z., Chen, Y., & Zhang, L. (2018). A survey on network security-related data collection technologies. *IEEe Access*, *6*, 18345-18365.

**8.** Shankarapani, M. K., Ramamoorthy, S., Movva, R. S., & Mukkamala, S. (2011). Malware detection using assembly and API call sequences. *Journal in computer virology*, 7(2), 107-119.

**9.** Takase, H., Kobayashi, R., Kato, M., & Ohmura, R. (2020). A prototype implementation and evaluation of the malware detection mechanism for IoT devices using the processor information. *International Journal of Information Security*, 19(1), 71-81.

**10.** Lv, S., Wang, J., Yang, Y., & Liu, J. (2018). Intrusion prediction with system-call sequence-to-sequence model. *IEEE Access*, 6, 71413-71421.

**11.** Divakaran, D. M., Fok, K. W., Nevat, I., & Thing, V. L. (2017). Evidence gathering for network security and forensics. *Digital Investigation*, 20, S56-S65.

**12.** Li, Y., Huang, G. Q., Wang, C. Z., & Li, Y. C. (2019). Analysis framework of network security situational awareness and comparison of implementation methods. *EURASIP Journal on Wireless Communications and Networking*, 2019(1), 205.

**13.** Gregorczyk, M., Żórawski, P., Nowakowski, P., Cabaj, K., & Mazurczyk, W. (2020). Sniffing detection based on network traffic probing and machine learning. *IEEE Access*, 8, 149255-149269.

**14.** Jazi, H. H., Gonzalez, H., Stakhanova, N., & Ghorbani, A. A. (2017). Detecting HTTP-based application layer DoS attacks on web servers in the presence of sampling. *Computer Networks*, 121, 25-36.

**15.** Mohmand, M. I., Hussain, H., Khan, A. A., Ullah, U., Zakarya, M., Ahmed, A., ... & Haleem, M. (2022). A machine learning-based classification and prediction technique for DDoS attacks. *IEEE Access*, 10, 21443-21454.

**16.** Abubakar, R., Aldegheishem, A., Majeed, M. F., Mehmood, A., Maryam, H., Alrajeh, N. A., ... & Jawad, M. (2020). An effective mechanism to mitigate real-time DDoS attack. *IEEE Access*, *8*, 126215-126227.

**17.** Simpson, S., Shirazi, S. N., Marnerides, A., Jouet, S., Pezaros, D., & Hutchison, D. (2018). An inter-domain collaboration scheme to remedy DDoS attacks in computer networks. *IEEE Transactions on Network and Service Management*, *15*(3), 879-893.

**18.** Khalaf, B. A., Mostafa, S. A., Mustapha, A., Mohammed, M. A., & Abduallah, W. M. (2019). Comprehensive review of artificial intelligence and statistical approaches in distributed denial of service attack and defense methods. *IEEE Access*, 7, 51691-51713.

**19.** Halladay, J., Cullen, D., Briner, N., Warren, J., Fye, K., Basnet, R., ... & Doleck, T. (2022). Detection and characterization of DDoS attacks using time-based features. *IEEE Access*, 10, 49794-49807.

**20.** Nashat, D., Khairy, S., & Hassan, M. M. (2021). Detection of application layer DDoS attack based on SIS epidemic model. *IEEE Access*, 9, 159827-159832.

**21.** Ghaben, A., Anbar, M., Hasbullah, I. H., & Karuppayah, S. (2021). Mathematical approach as qualitative metrics of distributed denial of service attack detection mechanisms. *IEEE Access*, *9*, 123012-123028.

**22.** Wang, X., Ma, X., Peng, J., Li, J., Xue, L., Hu, W., & Feng, L. (2021). On modeling link flooding attacks and defenses. *IEEE Access*, 9, 159198-159217.

**23.** Dimolianis, M., Pavlidis, A., & Maglaris, V. (2021). Signature-based traffic classification and mitigation for DDoS attacks using programmable network data planes. *IEEE Access*, 9, 113061-113076.

**24.** Badhib, A., Alshehri, S., & Cherif, A. (2021). A robust device-to-device continuous authentication protocol for the internet of things. *IEEE Access*, 9, 124768-124792.

**25.** Alhothaily, A., Hu, C., Alrawais, A., Song, T., Cheng, X., & Chen, D. (2017). A secure and practical authentication scheme using personal devices. *IEEE access*, 5, 11677-11687.

**26.** Shin, D., Yun, K., Kim, J., Astillo, P. V., Kim, J. N., & You, I. (2019). A security protocol for route optimization in DMM-based smart home IoT networks. *IEEE Access*, 7, 142531-142550.

**27.** Hussain, S. S., Farooq, S. M., & Ustun, T. S. (2019). Analysis and implementation of message authentication code (MAC) algorithms for GOOSE message security. *IEEE Access*, 7, 80980-80984.

**28.** Mishra, N., & Pandya, S. (2021). Internet of things applications, security challenges, attacks, intrusion detection, and future visions: A systematic review. *IEEE Access*, 9, 59353-59377.

**29.** Harbi, Y., Aliouat, Z., Refoufi, A., & Harous, S. (2021). Recent security trends in internet of things: A comprehensive survey. *IEEE Access*, 9, 113292-113314.

**30.** Zaman, S., Alhazmi, K., Aseeri, M. A., Ahmed, M. R., Khan, R. T., Kaiser, M. S., & Mahmud, M. (2021). Security threats and artificial intelligence based countermeasures for internet of things networks: a comprehensive survey. *Ieee Access*, 9, 94668-94690.