Results in Engineering 26 (2025) 105521

Contents lists available at ScienceDirect

Results in Engineering

journal homepage: www.sciencedirect.com/journal/results-in-engineering

Adaptive distributed honeypot detection network for enhanced cybersecurity against DoS and DDoS attacks

V. Selva Kumar [a], K.R. Mohan Raj [b], S. Gopalakrishnan [c], G. Vennila [d], D. Dhinakaran [e,*], P. Kavitha [f]

[a] Department of Computer Science and Engineering, P.S.R. Engineering College, Sivakasi, India
[b] Department of Information Technology, Velammal Engineering College, Chennai, India
[c] Department of Computer Science & Engineering (Data Science), Madanapalle Institute of Technology & Science, Andhra Pradesh, India
[d] Department of Artificial Intelligence and Machine Learning, School of Computing, Mohan Babu University, Tirupati, India
[e] Department of Computer Science and Engineering, Vel Tech Rangarajan Dr. Sagunthala R&D Institute of Science and Technology, Chennai, India
[f] Department of Computer Science and Engineering, R.M.K. Engineering college, Chennai, India

ARTICLE INFO

Keywords:
Denial of service
Distributed denial of service
Intrusion detection systems
Generative adversarial networks
Real-time attack detection
Deep learning

ABSTRACT

The increasing prevalence and sophistication of Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks present significant challenges in ensuring the security and stability of modern networked systems. These attacks, characterized by their ability to disrupt services and compromise resources, require innovative and robust detection mechanisms to safeguard highly interactive environments such as honeypot systems. Traditional detection techniques often fall short in addressing the complexities posed by dynamic traffic patterns, diverse attack types, and real-time processing demands. This study introduces the Adaptive Distributed Honeypot Detection Network (ADHDN), a novel framework that leverages deep learning and probabilistic modeling to address the limitations of existing solutions. ADHDN employs a combination of Deep Generative Adversarial Networks (DGANs) and Discrete Hidden Markov Models (DHMMs) to achieve superior detection precision across various DoS attack types, including application-level, protocol-level, and data volume attacks. Implemented in a highly interactive honeypot environment with distributed server and virtual machine configurations, ADHDN demonstrates remarkable adaptability and resilience. Performance evaluation using the IoTID20 dataset reveals that ADHDN consistently outperforms contemporary models, such as RBMD, BNDH, and AHDL. ADHDN achieves a true positive rate of 99.7% for protocol-level attacks, 99.4% for application-level attacks, and 97.5% for data volume attacks under low attack volumes, maintaining robust performance even as attack intensity scales. These results underscore ADHDN's potential to redefine DoS detection in dynamic and high-interaction environments, offering a scalable and efficient solution to contemporary cybersecurity challenges.

1. Introduction

In the rapidly evolving landscape of cybersecurity, Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks have emerged as persistent and sophisticated threats [1]. These attacks are designed to disrupt the availability of services by overwhelming target systems or networks with illegitimate requests. DoS attacks may originate from a single malicious machine, while DDoS attacks leverage a network of compromised devices, commonly known as botnets, to launch large-scale, coordinated attacks [2–4]. Botnets are created by infecting victim systems with malware that transforms them into bots, which then execute commands from the attacker. The collection of these bots forms a botnet that can be used to initiate high-impact attacks on targeted systems [5].

1.1. Challenges in detecting DoS and DDoS attacks

The variety and complexity of DoS attacks are vast, with primary categories including application-level, protocol-level, and data capacity-level attacks. Application-level attacks target web servers and their underlying protocols, disrupting transaction processes and online services. Protocol-level attacks exploit vulnerabilities in IP fragments,

* Corresponding author.
E-mail addresses: selvakumarv@psr.edu.in (V. Selva Kumar), mohanraj@velammal.edu.in (K.R. Mohan Raj), gopal.pgsk@gmail.com (S. Gopalakrishnan), drvennilam@gmail.com (G. Vennila), drdhinakarand@veltech.edu.in (D. Dhinakaran), pka.cse@rmkec.ac.in (P. Kavitha).

https://doi.org/10.1016/j.rineng.2025.105521
Received 19 April 2025; Received in revised form 22 May 2025; Accepted 27 May 2025
Available online 27 May 2025

connection setups, firewalls, and load balancers, undermining the foundational infrastructure of networks [6–8]. Meanwhile, data capacity-level attacks focus on degrading network throughput and bandwidth, leading to reduced performance and service availability. This diversity of attack vectors makes it imperative to develop detection systems capable of identifying and mitigating these threats across multiple levels. Based on the understanding that DDoS attacks are targeted at network services, highly interactive honeypots have become an invaluable tool to understand and mitigate DoS attacks [9]. Some of these systems are aimed at replicating real-world environments and putting attackers through active engagement to collect detailed information about attacker interactions. Unlike low-interaction honeypots that just log basic attack attempts, such advanced honeypot systems simulate real services and protocols, giving a more realistic environment to attackers. With this approach, security systems can gain a deeper view of how attackers are behaving and how they're doing it.

However, such an active nature of highly interactive honeypots brings some unique challenges [10]. Although these systems need tons of resources to be realistic and are very solicitous in nature, the need for real-time detection and analysis is twice as important because these systems are very targeted by attackers. Even though traditional detection mechanisms have the potential, they are not very appropriate for high-interaction honeypot environments when the DoS attacks are dynamic. Yet signature-based detection methods are based on pattern and rule predefined, and are thus ineffective against the novel and adaptive attack strategies [11]. Heuristic approaches and rule-based systems are few, and typically cannot scale to the complexity of modern vector attacks. Potential solutions were already analyzed through the use of machine learning (ML) and deep learning (DL) techniques that were able to analyze large datasets and detect complex patterns [12]. Unfortunately, these include Random Forest, Recurrent Neural Networks (RNN), and Multi-Layer Perceptrons (MLP), which do not sufficiently adapt to the requirements of real-time and distributed environments of honeypot systems [13]. With the sophistication of DoS and DDoS attacks growing and the shortcomings of traditional detection techniques, the need for creative and aware techniques is clearly demonstrated. However, advanced detection mechanisms capable of dealing with large amounts of traffic, during distributed networks and highly dynamic attack patterns, are needed in such advanced honeypot systems, which will become effective in engaging attackers [14]. Recent advancements in adaptive control mechanisms have shown promise in addressing the complexities of dynamic attack patterns. For example, secure adaptive sampled-data control strategies have demonstrated efficacy in mitigating the effects of uncertainty and DoS attacks in multi-agent systems through synchronized communication and neural network-based estimation techniques [15]. Inspired by these approaches, our research seeks to adapt similar principles to high-interaction honeypot systems, focusing on distributed, real-time detection and mitigation in the face of modern attack vectors.

1.2. Motivation and objectives

This work addresses the research problem defined by these challenges. The main objective is to create a scalable, adaptable, and efficient detection system for a highly interactive honeypot environment. At a minimum, it entails figuring out how to create a tough mechanism for leaning in awesome and hidden threats, and contrasting legitimate traffic with malicious practices, while it remains incidental to distribute them around. The research addresses these challenges in order to increase the security and resilience of honeypot systems against evolving DoS and DDoS attack strategies. In order to accomplish these objectives, this research proposes a novel detection model for Adaptive Distributed Honeypot Detection Network (ADHDN) that couples state-of-the-art deep learning with the probabilistic framework. To detect the DoS and DDoS attacks, the proposed system utilizes Deep Generative Adversarial Networks (DGAN) and Discrete Hidden Markov Models (DHMM) to present a complete and adjustable one. With DGAN it is possible to synthesize synthetic attack data that is subsequently used to train the detection model in a wide range of environment configurations and finally with DHMM probabilistic modeling is used to predict malicious events from observed traffic patterns. Taken together, these techniques establish a robust and scalable detection mechanism that can operate with high levels of dynamicness.

However, highly interactive honeypots augment the problem of detection by their active engagement with attackers. These systems generate very large amounts of interaction data volume and variability and real-time analysis is highly challenging. Furthermore, when any modern honeypot deployments are distributed in nature, with multiple Virtual Machines (VMs) present on single or multiple physical systems, such detection mechanisms need also to be scalable in a widely distributed setting. Using distributed processing capabilities, the ADHDN mode responds to such challenges by providing detection at multiple points in the network. With DGAN and DHMM analytical agents installed in each VM, each can be processed in parallel and detected in real-time. In addition to improving detection accuracy, this architecture makes the system more robust to attacks because the model is distributed and thus less susceptible to failure on any single point. Besides the detection, the proposed system looks at prevention. ADHDN furnishes real-time alerting as well as response mechanisms that allow identified threats to be minimized before they can do extensive harm. In highly interactive honeypot environments, where the system is inherently active, such a proactive approach is crucial since the risk of impact of successful attacks has increased.

1.3. Contributions and innovations

This research presents significant advancements in the field of cybersecurity, specifically tailored for highly interactive honeypot environments. The key contributions and innovations of this study are outlined as follows:

Proposed ADHDN Framework: Introduced the adaptive distributed honeypot detection network, a novel and scalable framework designed to address the complexities of detecting and preventing DoS and DDoS attacks in highly interactive honeypot systems.
Integration of Advanced Analytical Techniques: Leveraged deep generative adversarial networks for synthesizing diverse attack scenarios and discrete hidden Markov models for probabilistic modeling, enabling real-time detection and prediction of malicious activities.
Distributed Processing Capabilities: Designed a distributed architecture where detection agents based on DGAN and DHMM operate independently across multiple Virtual Machines (VMs). This ensures scalability, robustness, and reduced susceptibility to single-point failures.
Real-Time Alert and Response Mechanism: Implemented proactive measures that provide real-time alerts and immediate response actions to mitigate threats, reducing the risk and impact of potential attacks on critical systems.
Bridging the Gap in Existing Solutions: Addressed limitations of traditional honeypot detection methods by creating a dynamic, adaptive system that meets the demands of highly interactive honeypot environments, particularly in the context of evolving attack strategies and distributed deployments.
Enhanced Detection Accuracy: Demonstrated improved detection accuracy and reduced false positives through the integration of synthetic data generation and probabilistic traffic analysis, achieving superior performance compared to existing methodologies.
Security and Resilience of Honeypot Systems: Contributed to the advancement of honeypot systems by enhancing their security and resilience against evolving attack vectors, providing a robust solution for modern cybersecurity challenges.

The significance of this research lies in its ability to bridge the gap between traditional detection methods and the unique requirements of highly interactive honeypot systems. By integrating advanced analytical techniques and leveraging the distributed nature of honeypot environments, the proposed model represents a significant advancement in the field of cybersecurity. It provides a scalable, adaptive, and efficient solution to the challenges posed by DoS and DDoS attacks, ensuring the security and resilience of critical systems and networks. The structure of this article is as follows: Section 2 provides an in-depth analysis of recent and relevant research, offering a comprehensive overview of the existing landscape. Section 3 delves into the technical aspects and intricacies of the proposed Deep Generative Adversarial Networks based Honeypot (DGAN-H) system, highlighting its innovative features and addressing associated complexities. Section 4 presents the operational framework, detailed outcomes, and a comparative analysis of the proposed system with existing methodologies. Finally, Section 5 concludes the study, summarizing key findings and proposing insightful directions for future research.

2. Related works

Cyber security has developed to a great degree that can guard systems and networks from vicious danger. Nevertheless, the DoS and DDoS attacks persisted and remained sophisticated. Because they are focused on denying the availability of resources and services by overwhelming systems with illegitimate requests, these attacks can be incredibly damaging to sensitive and critical infrastructures. However, the techniques of detection and mitigation have not fully closed all of the gaps, especially the gap of adapting to the highly dynamic, interactive nature of honey pot environments of modern times. Highly interactive honeypots are a sine qua non for mimicking real-world systems to entice and analyze malicious activities. However, challenges for them are inherent such as scalability problems, real-time detection, and the differentiation between legitimate and malicious traffic. To develop more robust solutions, first, these challenges need to be addressed.

The domain is flagged as one of the major challenges, especially given the fact that one of the most complicated attack vectors is hard to detect using traditional rule-based and signature-based systems. What is always present is advanced techniques such as distributed botnets, polymorphic malware, and zero-day exploits and static detection models do not work. To address these, recently, the research has shifted to the application of ML and DL techniques. Anomaly detection has also been attempted using algorithms like Random Forest, Naive Bayes, MLPs, and RNNs. Besides that, hybrid techniques that incorporate probabilistic models in DL paradigms have also been explored to increase precision and flexibility. Nevertheless, the current solutions are still limited in the implementation of real-time threats in highly interactive environments using honeypots, and there is still room for the development of more scalable and context-aware ones.

Overview of Research in Intrusion Detection and Honeypots: The field of intrusion detection and honeypot systems has seen substantial advancements over the years, with a focus on detecting and mitigating a wide range of cyberattacks. Mishra et al. [16] explored the use of KDD Cup'99 and DARPA datasets for identifying and classifying intrusions, particularly zero-day attacks, through the SNORT-XSS algorithm. Their method integrated fuzzy reasoning for rule categorization and a feed-forward neural network with backpropagation to enhance system training, validation, and testing. This approach successfully minimized false positives and true negatives, showcasing its effectiveness for real-time intrusion detection. Despite its merits, the system's reliance on predefined rules limits adaptability to novel attack vectors. Darzi et al. [17], on the other hand, tackled DoS attack challenges by examining post-quantum security measures and integrating AI-driven mechanisms. Their study emphasized the need for federated learning and collaborative frameworks, pointing out the gaps in privacy, authentication, and transparency in existing approaches. These foundational works illustrate the evolving nature of cyber threats and the importance of innovative strategies to counteract them effectively.

Advancements in Honeypot and DoS Detection Technologies: Significant contributions have been made in optimizing honeypot systems and detecting distributed DoS attacks. Akshay et al. [18] provided a detailed analysis of intrusion detection and prevention systems within honeypot environments, focusing on honey trap techniques and constructing Network Intrusion Detection Systems (NIDS). Their work highlighted effective honeypot security measures while addressing the challenges of resource allocation and system robustness. Altulaihan et al. [19] proposed an anomaly-based Intrusion Detection Systems (IDS) for Internet of Things (IoT) networks using classifiers like Decision Tree, Random Forest, and Support Vector Machine, combined with feature selection techniques such as Genetic Algorithm and Correlation-based Feature Selection. This approach showcased the potential of hybrid techniques in improving IoT network security. However, its reliance on computationally intensive processes poses challenges for deployment in low-resource environments. Similarly, Khan et al. [20] developed a reputation-based IDS tailored for IoT systems, focusing on energy efficiency and computation optimization. By analyzing routing and Medium Access Layer (MAC) layer protocols, the system effectively detected intrusions, although it struggled to adapt to dynamic network environments. Madison et al. [21] introduced a centralized honeypot sensor system for detecting DoS and packet capturing attacks. While the use of honeypot sensors improved detection rates, the centralized architecture created vulnerabilities, such as single points of failure, necessitating a shift towards distributed solutions.

Movva et al. [22] introduced an innovative honeypot system inspired by the Venus flytrap mechanism, focusing on extracting an attacker's tools and techniques while efficiently shutting them down. By leveraging the intelligent prey-catching behavior of Venus plants, the study proposed the use of a Venus flytrap optimization algorithm for designing a honeypot integrated with an IDS. The approach introduced a new fitness function to dynamically determine the attacker's size, improving the honeypot's interaction capabilities. This intelligent design enables the system to interact effectively with attackers, providing valuable insights into their strategies while minimizing risks. However, the study primarily emphasizes attack identification and lacks scalability considerations in highly interactive network environments. Ozkan et al. [23] presented a robust hybrid attack detection model, Signature- and Anomaly-Based Attack Detection Technique (SABADT), supported by a novel Feature Selection Approach (FSAP). The FSAP enhances the feature extraction process, optimizing the performance of attack detection algorithms. The SABADT model integrates signature-based and anomaly-based techniques, offering comprehensive detection capabilities. The research tested the FSAP and SABADT methods on benchmark datasets, including KDD'99, UNSW-NB15, and CIC-IDS2017, demonstrating superior results in detection accuracy and reduced false-alarm rates. While the methods achieved state-of-the-art performance, they predominantly focused on static datasets and did not address the challenges of real-time, adaptive, and distributed attack detection systems in dynamic environments.

Deep Learning and Hybrid Models for Attack Detection: Recent developments have centered on employing deep learning and hybrid models to enhance attack detection capabilities. Imamverdiyev et al. [24] explored Restricted Boltzmann Machines (RBM) for detecting DoS attacks, utilizing Gaussian and Bernoulli techniques to train neural networks with multilayer architectures. This approach demonstrated superior detection rates compared to traditional ML techniques such as Support Vector Machines and Decision Trees, although its reliance on controlled network assumptions limited its practical applicability. Banerjee et al. [25] applied honeypot-based network traffic analysis for botnet detection, using classifiers like Random Forest and Decision Tree. Their analysis highlighted the effectiveness of these classifiers in diverse honeypot environments but noted the lack of runtime attack analysis, which restricted its deployment in dynamic systems. Feng et al. [26]

proposed an anomaly detection framework using deep learning techniques like Deep Neural Network (DNN), Convolutional Neural Network (CNN) and LSTM (Long Short-Term Memory-RNN) in ad-hoc networks. This system effectively detected DoS and SQL injection attacks while generating real-time alerts. However, its implementation was restricted to low-interactivity wireless systems, limiting scalability to highly interactive networks. These efforts underscore the importance of adaptive, real-time solutions for evolving attack scenarios, setting the stage for the proposed ADHDN to address these critical gaps.

Emerging Strategies in Intrusion Detection and Honeypot Systems: Recent studies have delved deeper into novel techniques for detecting and mitigating cyber threats. Lopes et al. [27] proposed an innovative early detection strategy for DoS attacks using Horizontal Visibility Graphs (HVG) and Natural Visibility Graphs (VG) derived from network flows. This method demonstrated the ability to detect DoS attacks within 70ms using just 30 packets, showcasing exceptional efficiency and speed. The strategy's reliance on graph-based methodologies offered a promising direction for real-time detection, though its scalability and adaptability to varying network conditions require further exploration. Similarly, Alazawi et al. [28] employed convolutional neural networks (CNNs) to analyze system behavior and detect intrusion attacks. Their method demonstrated superior classification results compared to traditional SVM techniques, particularly when combined with feature selection methods. However, the reliance on predefined datasets highlighted the need for generalized approaches that cater to diverse and unpredictable attack scenarios.

Insights into Practical Honeypot Deployments: Sehgal et al. [29] documented real-world experiences of honeypot deployments at the Indian Institute of Technology, Kanpur, providing valuable insights into the practical aspects of honeypot setup and management. This work offered guidance on implementing extensible honeypot architectures while addressing operational challenges, such as resource optimization and maintenance. The detailed documentation underscored the potential of honeypots as effective tools for intrusion detection and system analysis. However, the study highlighted challenges in handling high-volume attack data and ensuring long-term sustainability of honeypot environments.

Despite extensive efforts in intrusion detection and prevention, several key challenges persist in addressing sophisticated cyber threats like DDoS attacks. The existing approaches are often based upon predefined rules, centralized architecture, or in isolation anomaly detection techniques that require a predefined rigid system to be applied. The real-time adaptability and scalability of these systems are difficult in highly interactive and dynamic environments. Also, privacy-preserving mechanisms, effective data handling, as well as collaborative frameworks are either not well explored or implemented sufficiently. In addition, many of these methods also suffer from limitations in dealing with different attack cases which include data volume attack cases, application level, and protocol level intrusion attacks. It also does not help matters when the different attack detection strategies are unable to be effectively integrated into a single framework for a collective attack detection solution. Additionally, runtime adaptability and proactive defense measures are often constrained, leaving systems vulnerable to emerging attack techniques. These gaps underscore the need for an adaptive, scalable, and robust intrusion detection solution capable of overcoming the limitations of current methodologies.

Our proposed ADHDN strategy addresses these critical challenges by introducing a dynamic and distributed framework that enhances detection accuracy and scalability. The system integrates real-time monitoring with collaborative anomaly detection to effectively identify and mitigate diverse attack types. Its distributed architecture eliminates single points of failure, while privacy-preserving mechanisms ensure secure and ethical data handling. ADHDN leverages advanced learning algorithms to dynamically adapt to emerging threats, addressing the limitations of static and rule-based approaches. By providing comprehensive attack detection across data volume, application-level, and protocol-level intrusions, the system ensures robust protection against sophisticated cyber threats. This holistic and adaptive design represents a significant advancement in the field, bridging the gaps in existing solutions and offering a reliable defense framework for modern networks.

3. Proposed adaptive distributed honeypot detection network

The adaptive distributed honeypot detection network is a comprehensive and advanced framework designed to detect and mitigate DoS and DDoS attacks in highly interactive honeypot environments as shown in Fig. 1. This framework leverages the synergistic capabilities of distributed systems and deep learning models to create an adaptive and collaborative detection mechanism. By integrating sophisticated statistical techniques, machine learning models, and distributed event handling, ADHDN ensures precise and efficient attack detection across a network of VMs within honeypot systems. The proposed ADHDN framework comprises multiple components, each serving a critical role in the distributed detection and mitigation process. These components collectively create a robust and dynamic system to counteract cyber threats.

The ADHDN process begins with the traffic reception and distribution stage, which is managed by the Honeypot Server Manager (HSM). The HSM acts as the central node responsible for receiving traffic events from internal and external clients. It ensures that incoming traffic is forwarded to the Asynchronous Random Event Distribution (ARED) model for processing. The ARED model facilitates the efficient distribution of random and asynchronous traffic events among the physical honeypot machines. ARED is a vital component, ensuring balanced and asynchronous distribution of legitimate and attack traffic events. This model employs discrete and continuous random event handling mechanisms, which allow the efficient forwarding of incoming traffic to the appropriate honeypot machines based on the system's workload. At the Event Handling in Honeypot Machines stage, the traffic distributed by ARED is delivered to individual honeypot machines. These machines, equipped with multiple VMs, serve as distributed detection points. Events are queued within the VMs for further analysis. Each VM is designed to handle both internal and external traffic events through separate event queues managed using a Poisson distribution model. This ensures that incoming traffic is processed systematically, minimizing any processing delays and improving the framework's efficiency.

The core intelligence of ADHDN is embedded within the Event Processing in VMs stage. Here, the DHMM operates to analyze the sequences of incoming traffic events. DHMM classifies traffic into observable legitimate events and hidden attacker events, leveraging its statistical capabilities to predict potential attacks. The DHMM outputs are then forwarded to the DGAN. DGAN, which is split into a Generator (G^{DGAN}) and Discriminator (D^{DGAN}), performs anomaly detection by creating and analyzing random samples of legitimate and attack events. The generator synthesizes random traffic samples based on the patterns identified by DHMM, while the discriminator evaluates these samples against real-time traffic to distinguish between legitimate and anomalous events. The Attack Detection and Alerts phase consolidates the findings from the detection components. Detection results from D^{DGAN} are forwarded to the Alert Manager, which acts as the central repository for all detected anomalies and attack patterns. The Alert Manager aggregates the results, generates alerts for detected DoS and DDoS attacks, and communicates them to the HSM for centralized monitoring. Additionally, the Alert Manager informs relevant stakeholders, such as network administrators, to take necessary action against ongoing attacks. This communication loop ensures timely response and updates to protect the system from further threats.

ADHDN employs a highly collaborative and distributed architecture. The coordination between its components enhances the framework's capability to detect complex attack patterns while reducing false

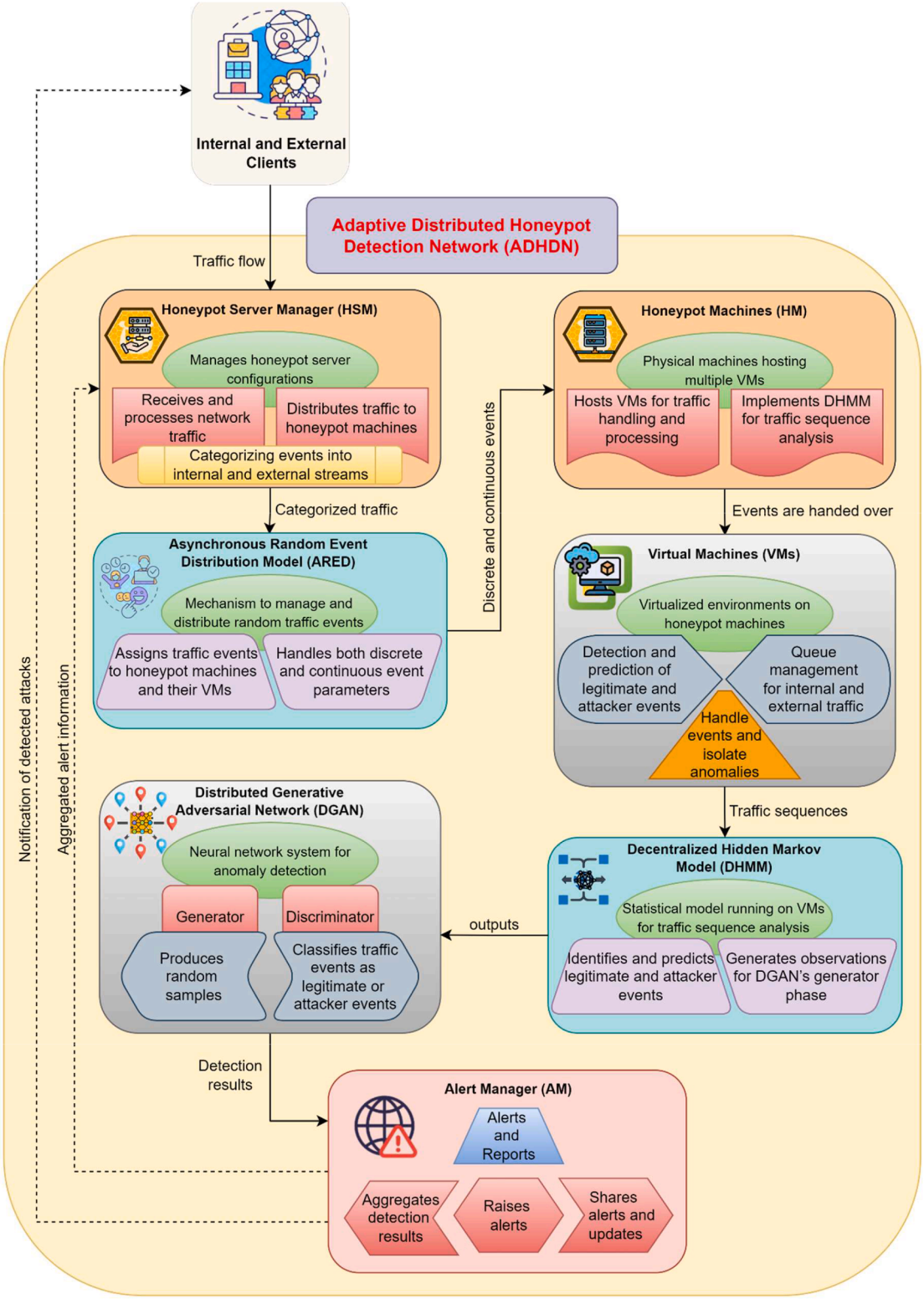

Fig. 1. Flow of proposed adaptive distributed honeypot detection network.

positives. By integrating ARED's asynchronous traffic distribution with DHMM's statistical traffic analysis and DGAN's advanced anomaly detection capabilities, ADHDN creates a comprehensive mechanism to identify and isolate threats effectively. The distributed nature of the system, supported by cooperative VMs and physical machines, ensures scalability and adaptability to varying traffic loads and attack scenarios. Moreover, the dynamic event handling facilitated by ARED and the continuous learning enabled by DHMM and DGAN contribute to the adaptive nature of ADHDN. The integration of real-time updates from detection results allows the system to refine its detection capabilities iteratively. This ensures that the ADHDN framework remains resilient against evolving attack strategies and provides robust protection to the network infrastructure. In conclusion, the ADHDN represents a significant advancement in cybersecurity for honeypot environments. Its

modular design, distributed processing capabilities, and integration of advanced detection models make it a powerful tool for mitigating DoS and DDoS attacks. By effectively combining asynchronous event distribution, statistical traffic analysis, and machine learning-based anomaly detection, ADHDN achieves an unparalleled level of adaptability and accuracy. This framework not only ensures real-time attack detection but also provides a scalable and reliable solution for securing highly interactive honeypot systems. The notation and semantics used in the proposed work are shown in Table 1. The integration of DGAN and DHMM within the ADHDN framework brings several significant advantages:

a) **Dynamic Adaptation:** The use of DGAN enhances the system's ability to dynamically adapt to new and evolving attack patterns, including zero-day attacks, by generating realistic adversarial scenarios to train the detection models effectively.
b) **Improved Detection Accuracy:** DGAN's adversarial training mechanism helps reduce false positives and negatives, ensuring precise differentiation between legitimate traffic and malicious activities.
c) **Sequential Pattern Recognition:** DHMM enables the modeling of sequential patterns in network behaviors, which is particularly useful in detecting complex, multi-stage attacks that span over time.
d) **Probabilistic Decision-Making:** The probabilistic framework of DHMM allows for better handling of uncertainties in detection, making the system robust in scenarios with incomplete or noisy data.
e) **Comprehensive Detection:** By coupling DGAN's learning capabilities with DHMM's sequential analysis, the ADHDN achieves a holistic approach to identifying and mitigating DoS and DDoS attacks, ensuring both real-time responsiveness and long-term adaptability.

These advantages collectively make the ADHDN framework a robust and innovative solution for securing distributed environments against advanced cyber threats.

3.1. Asynchronous random event distribution model

The asynchronous random event distribution model is an essential component of the adaptive distributed honeypot detection network. It plays a pivotal role in efficiently managing and distributing network traffic events across a highly interactive honeypot system. The ARED model addresses the challenges of asynchronous traffic reception and distribution in a distributed environment by implementing systematic mechanisms to classify, manage, and forward events within the honeypot infrastructure. This approach ensures balanced resource utilization and effective handling of both legitimate traffic and attack attempts such as DoS and DDoS [30]. The process begins with the initialization of parameters, which include the number of honeypot machines, their associated VMs, and honeypot servers as shown in Fig. 2. These servers act as the entry point, receiving traffic events from internal and external clients. The incoming events are classified into two main types: discrete events, which represent a fixed number of identifiable activities, and continuous events, which are streams of traffic without a predefined count. This classification allows the system to apply targeted handling strategies for each event type.

Discrete events are distributed across the timeline, ensuring that honeypot physical machines receive them in a structured manner. Continuous events, on the other hand, are distributed as streams to maintain consistent flow and prevent overloading of resources. This dual

Table 1
Notation and meanings.

Notation	Explanation
H^{HI}	Highly Interactive Honeypot
S^R	Honeypot Server
e^i	Traffic Parameter
T	Time
R^{SE}	Random Traffic Events
AR^{Ei}	*Individual Traffic*
AR^E	ARED
V^R	Number of VMs
$P(L)$	Legitimate Events
$P(A)$	Attacker Events
X	Markov Process
Y	Unobservable States
V^R	Physical Machine
$V(e^I)$ *and* $V(e^E)$	Traffic Events
N^C, T^C and n^C	Traffic Features

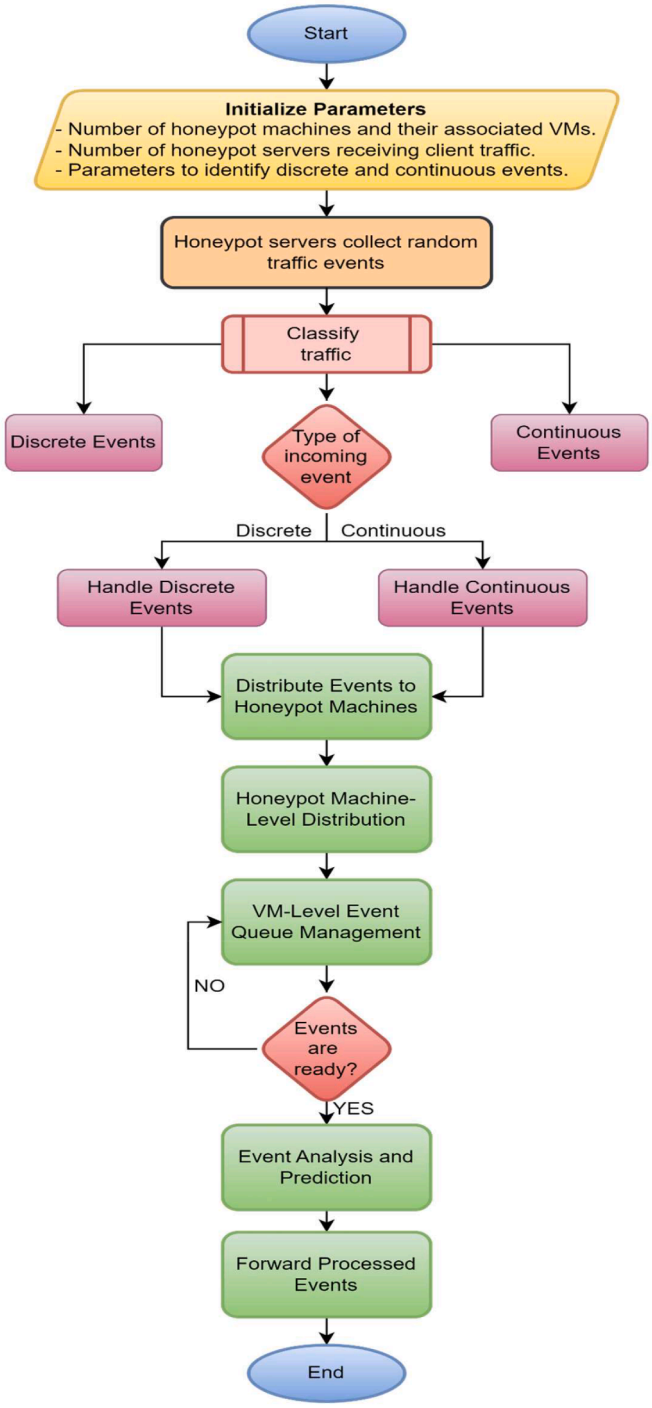

Fig. 2. Process flow of asynchronous random event distribution model.

strategy provides a robust mechanism for handling varying traffic patterns and attack scenarios. Once the events are categorized, the ARED model distributes them asynchronously and asymmetrically across honeypot machines. This distribution is determined based on the utility rate of each machine, ensuring an optimal load-balancing approach. As the traffic reaches the honeypot machines, it is further disseminated to the associated VMs. Each VM is equipped with internal and external event queues, which manage the received events with precision. This queue management is crucial for maintaining order and enabling subsequent analytical processes. After being queued, the events undergo a thorough analysis to identify patterns or sequences indicative of malicious activity. This analysis involves predicting trends and highlighting potential threats, forming the foundation for advanced anomaly detection in subsequent stages. By incorporating this predictive capability, the ARED model not only distributes traffic effectively but also prepares the system for proactive threat management.

3.1.1. Mathematical foundations

Let assume, a highly interactive honeypot, H^{HI} is implemented with R homogeneous physical honeypot machines. In each machine, V VMs are running to detect DoS and DDoS attacks. Each physical machine is connected with S^Rhoneypot server machines to receive the network traffic from internal and external clients. According to ARED model, each distributed server receives R^{SE}random traffic events at time, T. ARED determines discrete and continuous random events for each iteration. Besides, it helps servers to distribute the random events to honeypot machines. ARED model is given below. E is a randomly varying event, the ARED, AR^E for E is determined as given in eq. (1).

$$AR^E = P(E = e^i) = AR^{Ei} \tag{1}$$

AR^{Ei} denotes individual traffic, e^i denotes real valued traffic parameter. The range of AR^E for all active network traffic events, $0 \leq AR^{Ei} \leq 1$. This ARED model determines number of honeypot events as discrete parameter and sequence of event as continuous parameter. The discrete and continuous ARED determinations are illustrated in eqs (2) and (3). Let assume in a honeypot, the discrete events determined over timeline as, n^{e1}, n^{e2}.....n^{eN} . Then ARED is formulated as $AR^E = AR^{Ei}(n^{eN})$, then the real valued event function, R^E must be equivalent to randomly distributed variables. The discrete ARED is determined as below.

$$R^E = AR^E = P(E \leq e^i) = S^R \sum AR^{Ei}(n^{eN}) = S^R.AR^{Ei} \tag{2}$$

The continuous ARED is determined as given in eq. (3).

$$R^E = S^R \int AR^{Ei}(n^{eN}) \tag{3}$$

Eq. (3) is determined for continuously generated network traffic events at S^Rhoneypot servers. The discrete and continuous random events are modelled for S^R number of servers in a honeypot. Then the servers receive events and distribute them to all honeypot physical machines in the network. This distribution is initiated asynchronously and asymmetrically based on the utility rate of each machine. Once the machine receives distributed events from server, it shares among VMs. Each VM in a real machine is implemented to handle both internal and external traffic events. In order to do this activity, it maintains both internal and external queues. The VM queues maintain poison distribution models for event handlings as represented in eq. (4).

$$VH^P = V^R.\ e^{-TE^e}\frac{(TE^e)^L}{N!} \pm x \tag{4}$$

Where, L-Number of honeypots, x-Traffic event deviations, and V^R-Number of VMs in a machine. In this case both ARED and poison distribution models are implemented at different locations. Event receiving servers and honeypot physical machines use ARED techniques. At the next level, VMs use poison distribution. This dual distribution model helps to improve the event distribution and handling efficiency. The discrete and continuous events collected from the servers are given to DHMM running at each physical honeypot machine. DHMM runs at different machines to predict the traffic sequences delivered to all VMs running in a machine. In summary, the ARED model streamlines the reception, classification, and distribution of traffic events in a highly interactive honeypot system. By employing both discrete and continuous event handling mechanisms, it ensures efficient resource utilization and prepares the system for advanced attack detection. This model forms a critical backbone of the ADHDN, enabling real-time adaptability and resilience against sophisticated cyber threats.

3.2. Discrete hidden Markov model

The discrete hidden Markov model serves as a cornerstone in analyzing and predicting traffic events within the highly interactive honeypot environment. Derived from the foundational principles of the Hidden Markov Model (HMM), DHMM focuses on extracting hidden (unobservable) attacker events from observable legitimate traffic sequences. Each virtual machine in the honeypot system incorporates DHMM to process incoming traffic events and classify them into legitimate (observable) and attacker (hidden) states. This classification enhances the identification of DoS and DDoS attacks while predicting subsequent traffic events as shown in Fig. 3. At any given time T, traffic events flow into honeypot VMs, encompassing internal and external sources. These events are queued and processed sequentially, categorizing them into observable and hidden states. The DHMM model operates by identifying legitimate traffic patterns while isolating and analyzing anomalous behaviors indicative of attacks. Its statistical foundation enables it to model and predict hidden attacker events based on observable event sequences. The DHMM implementation involves several critical steps, as illustrated in the following process flow. Initially, the DHMM receives internal and external traffic events from the VMs.

The model is initialized for each VM in the network to ensure localized and distributed event analysis. Furthermore, it is configured for all honeypot physical machines, ensuring the scalability and extensibility of the detection system. A cooperative function is established between internal and external traffic processing points within the honeypot environment. This collaboration facilitates efficient handling of both legitimate and attacker events, enabling accurate probability estimations for legitimate events $(P(L))$ and attacker events $(P(A))$. Once the initialization is complete, the model processes incoming traffic events to compute these probabilities. This involves iterative evaluation of traffic sequences to isolate hidden attacker behaviors. The results are consolidated into discrete sequences representing legitimate $(DHMM(Q^{eI}))$ and attacker $(DHMM(Q^{eE}))$ events. These outputs serve as a foundation for generating predictive insights into the next possible traffic events. The predictive capability of DHMM plays a crucial role in preemptive security measures. By analyzing recent traffic patterns and event probabilities, the system predicts future events, enabling proactive responses to potential threats. This prediction mechanism significantly enhances the adaptive nature of the honeypot system, aligning with the overall objectives of the ADHDN framework.

3.2.1. Mathematical foundations

HMM is a statistical analysis technique being designed by Markov process, x and the unobservable states, y. HMM always attempts to extract the events in unobservable states, y by recognizing observable events at the state, y. DHMM is initiated in each VM of honeypot environment to extract unobservable events or attacks in the sequence of y states. At time T, traffic events are coming into honeypot VM. It handles the sequence of events under two categories like legitimate (observable) and attacks (hidden) states. DHMM is illustrated as given in eqs (conditional probability model). The probability of observing attacker events,

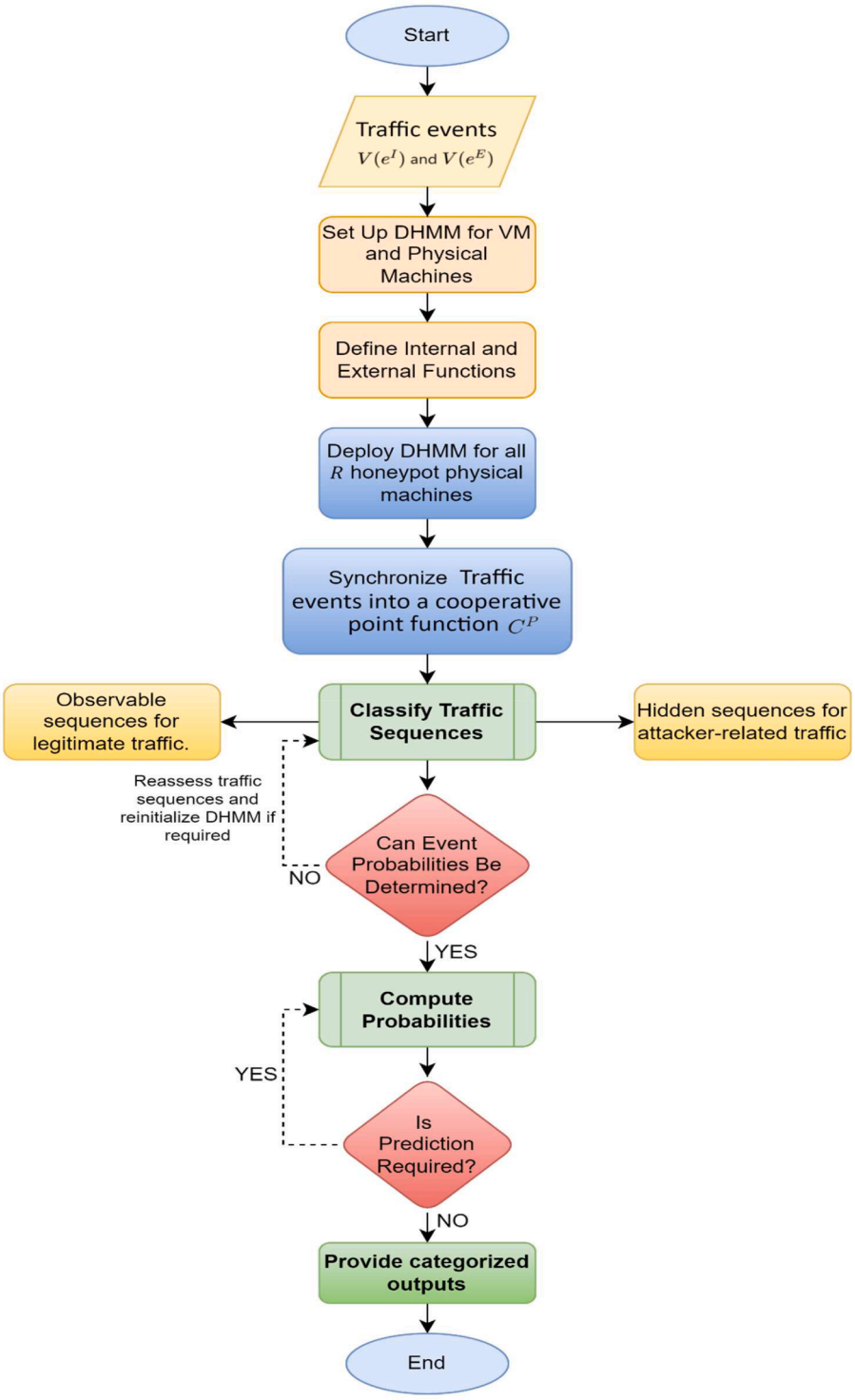

Fig. 3. Process flow of discrete hidden Markov model.

$$H^{PA} = a(0),\ a(1),\ a(2).....a(N-1) \tag{5}$$

Where, N - Sequence length, and now, the sequence becomes

$$P\left(H^{PA}\right) = \sum_{L}^{N} P(A|L)P(L) \tag{6}$$

Here, $L = l(0),\ l(1),\ l(2)...l(N-1)$, $P(L)$= Probability of legitimate events. This model uses recent events to observe or predict next event in the traffic sequence. It has limited complexity rate. Algorithm 1 illustrates DHMM on DoS identification and prediction.

The techniques discussed such as ARED, poison distribution and DHMM are providing prior event management activities. The techniques create distributed event management scenario for highly interactive honeypot system. In addition, the procedures and algorithm deliver distributed and queued events. DHMM is the model try to understand and predict both $P(A)$ *and* $P(L)$. This probability determination procedures enrich the proposed DGAN-H system. DGAN-H system uses the event distribution models at honeypot distribution points. It uses DHMM in each VM to process the event sequences. The next section discusses DGAN-H systems' technical aspects. In summary, DHMM provides a

Algorithm 1
DHMM Model.

Input: $V(e^I)$ *and* $V(e^E)$
Output: *Events of x and y*
Begin
Step 1: *Get the events* $V(e^I)$ *and* $V(e^E)$ *at VMs*
Step 2: *Initialize DHMM* (V^R. $V(e^I)$ *and* $V(e^E)$)
Step 3: *Initialize DHMM for all R honeypot physical machines*
Step 4: *Create internal and external cooperative point function,*
$C^P(DHMM) = R\sum V^R.\ (V(e^I)\ .\ V(e^E))\#(7)$
Step 5: *Execute* $P(H^{PA})$ *to extract attacker events as hidden terms*
Step 6: *Form* $DHMM(Q^{eI})$ *and* $DHMM(Q^{eE})$
Step 7: *Determine* $P(A)$ *and* $P(L)$
End

robust mechanism for distinguishing between legitimate and malicious traffic events within the honeypot system. Its ability to process and predict traffic sequences contributes to the distributed and queued event management approach of the ADHDN framework. This ensures a dynamic and adaptive response to emerging cyber threats, strengthening the honeypot system's defense mechanisms. The DHMM's integration with other components like ARED and DGAN further amplifies its effectiveness, creating a comprehensive solution for traffic event analysis and attack prediction.

3.3. DGAN-H construction model

DGAN is a network generates random samples which contain both legitimate and attacker events (DoS and DDoS). This generation of random sample events is completed at the generator phase, G^{DGAN}. The next level of DGAN receives real-time active honeypot traffic events based on the probability models proposed in section 3.1(AR^{Ei} *and* VH^P). The received honeypot traffics are queued at VMs, $V(e^I)$ *and* $V(e^E)$. Once the DHMM computes both observable and attacker (hidden) event variations, the discriminator phase (D^{DGAN}) activate anomaly detection procedures to isolate DoS and DDoS attacks from legitimate traffic evenet [19,20]. Fig. 4 and 5 illustrate DGAN-H agent modules running inside each VM of R physical honeypot machines. Let the total VMS in a physical machine is V^R, then the total honeypot machines in the network, R^V is V^RXR.

Fig. 4 depicts the basic structure of DGAN for evaluating real-time honeypot traffic events. Fig. 5 shows the integration of both DHMM and DGAN approaches to build DGAN-H system. DHMM resolves the hidden sequences by observing actual events from the input traffic sequence. These observations are produced into DGAN for generating effective random samples of traffic event. The generator of DGAN, G^{DGAN} produces DHMM based random samples to discriminator phase, D^{DGAN}. Algorithm 2 illustrates the activities executed by DGAN-H system. The proposed DGAN-H system is implemented with the help of DHMM sequences and random event distribution models.

This DGAN-H system acts as a recurrent DGAN network with embedded DHMM procedures. Due to the continuous and discrete event management procedures, the internal and external attacks are effectively monitored. In addition, DGAN-H uses multi-probability event management systems and prediction systems for handling the attacks in

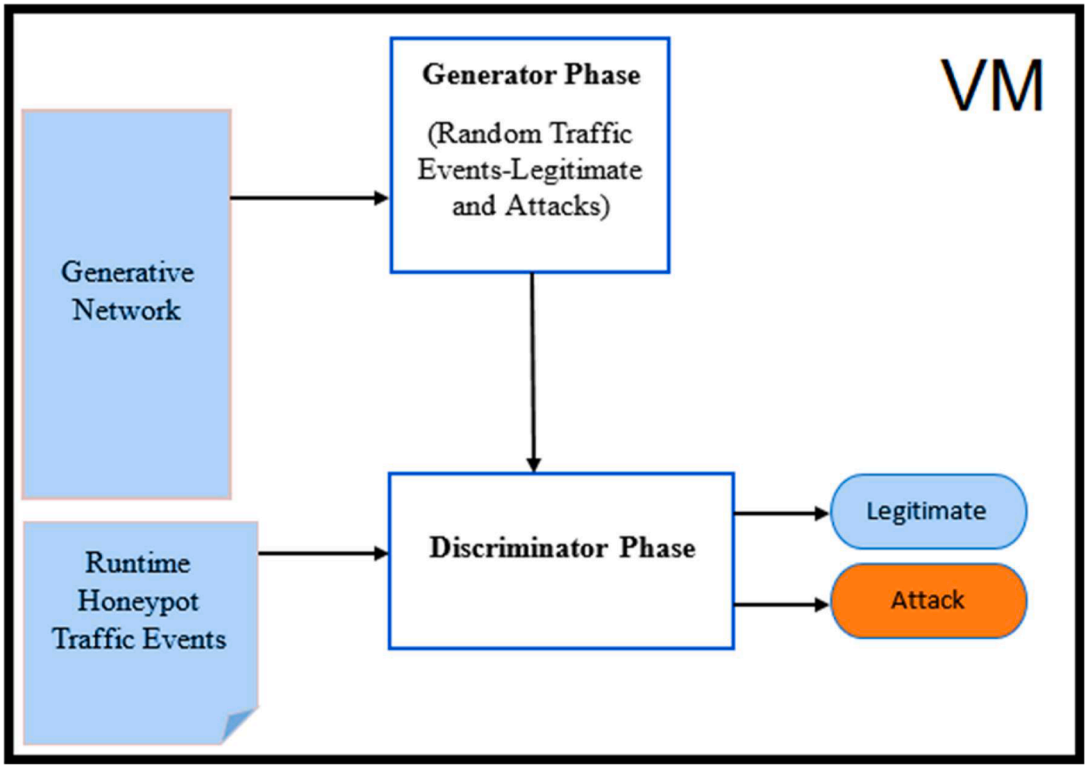

Fig. 4. GAN functions in VM.

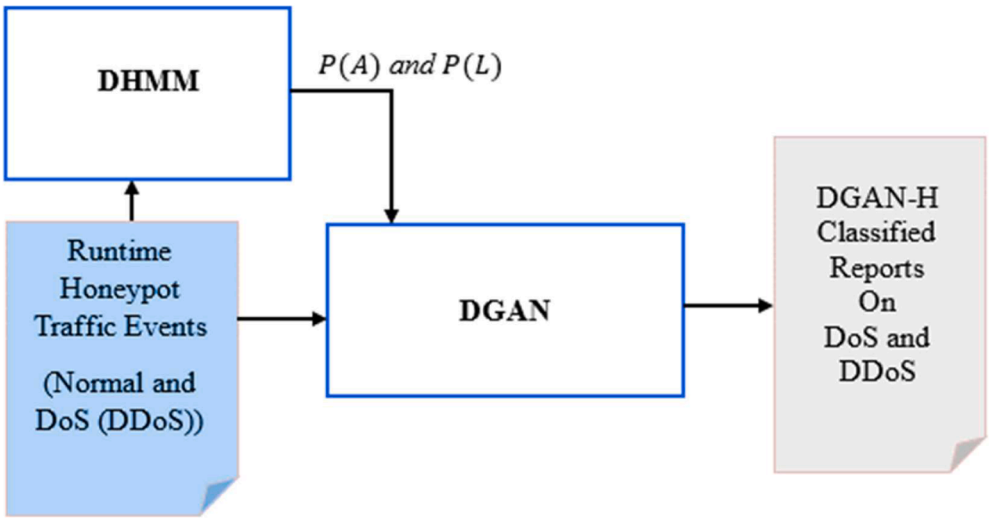

Fig. 5. DGAN-H structure inside honeypot VM.

Algorithm 2
DGAN-H construction model.

Input: *Events from* $V(e^I)$ *and* $V(e^E)$
Output: *DGAN alerts on DoS Attacks*
Begin
Step 1: *Find the events from* $DHMM(Q^{eI})$ *and* $DHMM(Q^{eE})$
Step 2: *Initiate* $P(A)$ *and* $P(L)$ *into the generator,* G^{DGAN}
Step 3: *Activate the generator,* G^{DGAN} *to create random traffic samples using,* E^i, $P(A)$ *and* $P(L)$.
Step 4: *Call the generator procedure,*
$G^{DGAN}(x) = R^V \sum \log(1 - D^{DGAN}(G^{DGAN}(E^i))) \pm DHMM(A|L) \#(8)$
Step 5: *Collect the random sample traffics*
Step 5: *Call the discriminator procedure,*
$D^{DGAN}(x) = R^V \sum \log D^{DGAN}((E^i)) + \log(1 - D^{DGAN}(G^{DGAN}(E^i))) \pm DHMM(A|L) \#(9)$
Step 6: *Initiate DoS detection procedures and KDD' 99 dataset features.*
Step 7: *Execute* $D^{DGAN}(x)$ *for detecting DoS and DDoS at* R^V*machines of the network*
Step 8: *Raise alert messages on each DoS detection*
Step 9: *Update* $P(H^{PA})$ *and the observations on DHMM*
Step 10: *Initiate DHMM in* R^V*machines to update all DGAN reports*
Step 11: *Predict the future samples*
Step 12: *Update the run-time events and alerts in* S^R *honeypot servers*
End

highly interactive honeypot system. In this highly interactive honeypot system, the proposed DGAN-H system manages a greater number of physical and virtual honeypot systems including multiple server units. Algorithm 3 illustrates the details of DoS detection procedures using DGAN.

3.4. DGAN-H based DoS detection model

The DGAN-H based DoS Detection Model is an innovative approach for identifying and predicting various types of DoS attacks, including DDoS, in real-time. This model leverages the distributed nature of honeypot systems and integrates analytical capabilities of DHMM and DGAN to enhance detection accuracy. By combining network credentials, traffic parameters, and node-specific signatures, the model ensures

Algorithm 3
DGAN-H based DoS detection model.

Input: *Events from* $V(e^I)$ *and* $V(e^E)$
Output: *Attack detection (DoS and DDoS)*
Begin
Step 1*: Call event processing procedures, DHMM* (E^i) *and DGAN* (E^i)
Step 2: *Extract the traffic features,*N^C, T^C and n^C
Step 3: *Do matching (*E^i==$KDD(E^i)$)
Step 4: *Set type field and alert flag*
Step 5: *If matched alert and send report to* R^V*honeypot VMs*
Step 6: *Share alert report with servers*
Step 7: *Recall DHMM* (E^i) *and DGAN* (E^i)
End

a robust mechanism for monitoring and mitigating malicious activities. The distributed architecture equips each VM with the ability to act as an independent attack detection unit, processing incoming traffic and sharing critical alerts across the network. In this model, traffic events are regularly queued within VMs based on a Poisson distribution approach. This systematic queuing ensures balanced event processing and efficient resource utilization. Equipped with DHMM and DGAN, each VM analyzes traffic sequences to differentiate between legitimate and attacker events as shown in Fig. 6. The dual capability of DHMM's predictive analysis and DGAN's adversarial learning allows for comprehensive detection of hidden and observable attack patterns. The workflow of the DGAN-H based DoS detection model is structured to systematically process traffic events and issue alerts for any identified threats. The sequence of steps involved is as follows:

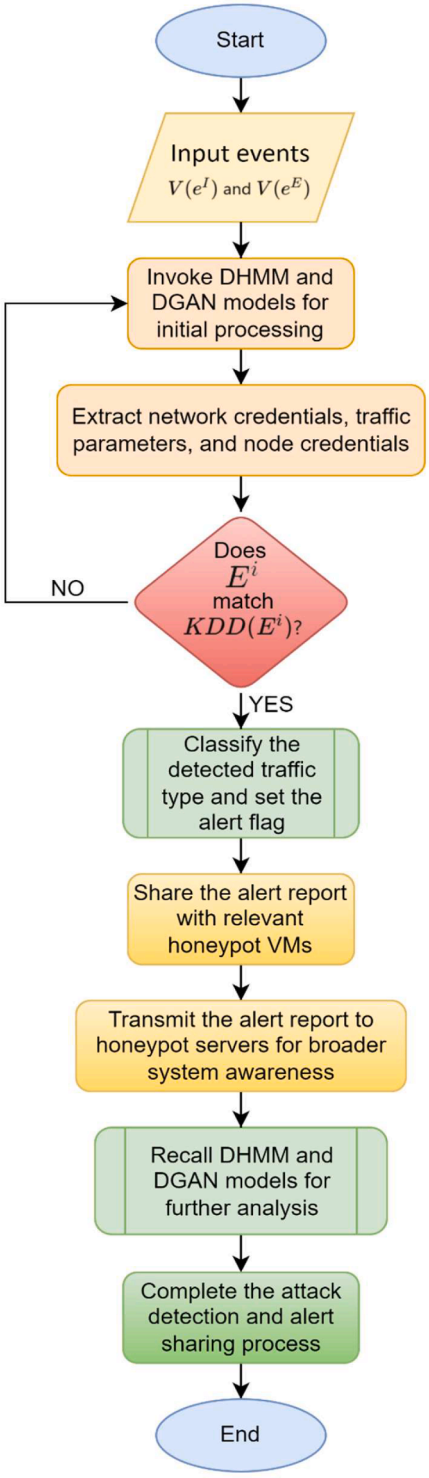

Fig. 6. Process flow of DGAN-H based DoS detection model.

a. **Event Initialization and Processing:** Incoming events, whether internal or external, are captured and processed by the DHMM and DGAN analytical agents within the VM. These procedures initiate the core detection mechanism, ensuring all traffic events are accounted for.
b. **Feature Extraction:** Essential traffic characteristics, such as network credentials (Nc), traffic parameters (Tc), and node-specific credentials (nc), are extracted. These features form the basis for distinguishing legitimate activities from attack patterns.
c. **Pattern Matching:** The extracted features are compared against known datasets, such as the IoTID20 dataset, to identify any deviations or potential threats. This step is pivotal in recognizing patterns indicative of DoS attacks.
d. **Alert Generation:** When a match is found, the system sets an alert flag and defines the type of attack detected. This information is immediately sent to the honeypot VMs within the network for distributed awareness.
e. **Collaborative Alert Sharing:** The alert reports are shared not only with the local honeypot system but also with centralized servers. This ensures a unified response mechanism, enhancing the overall security framework.
f. **Reiteration of Detection Procedures:** The DHMM and DGAN modules are reactivated to continually monitor traffic events, allowing the system to adapt and respond to dynamic attack patterns.

This iterative process ensures that all traffic events, regardless of their nature, are meticulously analyzed and categorized. The DGAN-H system's ability to integrate distributed monitoring and real-time alert sharing makes it a highly effective solution for managing the complex threat landscape posed by DoS and DDoS attacks. By utilizing the synergistic strengths of DHMM and DGAN, the DGAN-H based DoS Detection Model establishes a proactive and resilient defense mechanism in a highly interactive honeypot environment. The seamless flow of traffic analysis, feature extraction, pattern matching, and alert dissemination ensures the integrity and security of the network while maintaining high efficiency in threat detection.

4. Result and discussions

The adaptive distributed honeypot detection network system was meticulously designed and implemented within a highly active and practical experimental environment, demonstrating its capability to manage real-world complexities. The experimental setup emulates an operational honeypot environment comprising 25 equivalent server units, each optimized to achieve parallel computation efficiency. These servers are further expanded with 10 physical machines each, creating a robust and distributed infrastructure. To enhance scalability, every physical machine host four VMs. This layered architecture ensures an effective distribution of computational loads and resources, facilitating seamless DoS attack detection and prevention. To ensure comprehensive functionality, advanced models such as ARED and poison distribution were incorporated into the servers and physical machines, respectively. Additionally, DHMM and DGAN agents were deployed on individual VM units, each configured with distinct sets of principles and computational cores. This setup reflects the flexibility and adaptability required to counteract the ever-evolving nature of DoS and DDoS attacks.

4.1. Experimental setup and dataset

The core of DoS detection lies in intrusion detection mechanisms. For

this study, the IoTID20 dataset was utilized, which is a widely recognized benchmark for identifying anomalous activities across IoT networks [31]. This dataset was attached to each server to simulate patterns of attacks within the experimental honeypot environment. Its features were meticulously pre-processed and classified to isolate DoS events effectively. The IoTID20 dataset is renowned for its relevance in intrusion detection research and contains diverse and realistic IoT botnet attack scenarios, making it well-suited for evaluating modern cyber-attack detection systems. These distributions make it an ideal choice for validating the system's detection capabilities. The DoS attacks in the dataset are categorized into three levels: application-level attacks (e.g., web server and zero-day attacks), protocol-level attacks (e.g., smurf, SYN flood, ping, and fragmentation attacks), and data capacity-level attacks (e.g., UDP and ICMP flooding). The experimental environment relied on Weka 3.0 for data preprocessing tasks, ensuring accurate and efficient handling of raw features within the IoTID20 dataset as shown in Tab. 2. Python 3.7 was employed for the development of the ADHDN system, offering flexibility and compatibility with advanced machine learning and deep learning libraries. The hardware configuration consisted of a distributed architecture with 25 server units, each equipped with high-performance processors to manage substantial computational loads. Each physical machine hosting four VMs was optimized for concurrent processing, allowing efficient resource allocation for the deployed detection agents. The adaptive distributed honeypot detection network system's performance was evaluated against five existing methods to establish its effectiveness:

1. **Restricted Boltzmann Machine for DoS Detection (RBMD):** This method utilizes a Restricted Boltzmann Machine-based framework for identifying DoS attacks.
2. **Botnet Detection Using Honeypot Traffic Analysis (BNDH):** BNDH emphasizes botnet detection strategies through honeypot-based network traffic analysis.
3. **Anomaly Detection in Ad-hoc Networks Based on Deep Learning (AHDL):** AHDL uses a Deep Neural Network (DNN) model to detect DoS attacks and combines DNN, CNN, and LSTM models to identify XSS and SQL injection attacks.
4. **Correlation-based Feature Selection and Genetic Algorithm (CFS-GA):** CFS-GA enhances IoT network security against DoS attacks by combining anomaly detection with supervised ML algorithms like Decision Tree (DT), Random Forest (RF), K-Nearest Neighbor (kNN), and Support Vector Machine (SVM). Feature selection via Correlation-based Feature Selection (CFS) algorithm and the Genetic Algorithm (GA) optimizes the IDS for higher accuracy.
5. **Venus Fly-trap Optimization Algorithm with IDS (VFOA-IDS):** VFOA-IDS employs the Venus flytrap-inspired optimization algorithm to create an intelligent honeypot system integrated with IDS.

Table 2
Experimental settings.

Parameter	Value
Number of Physical Machines	10
Number of Servers	25
Number of Virtual Machines (VMs) per Machine	4
Total VM Units	100
CPU Cores per VM	4
Memory per VM	8 GB
Disk Space per VM	100 GB
Operating System	Ubuntu 20.04
Dataset	IoTID20 (IoT Network Intrusion Dataset)
Training Dataset Distribution	80%
Testing Dataset Distribution	74%
Traffic Distribution Model	Poisson Distribution
Attack Detection Models	DHMM and ADHDN Agents
Development Tools	Python 3.7, Weka 3.0
Hyperparameter Optimization	Grid Search
Evaluation Metrics	Precision, TPR, FPR
Application-level Attacks Tested	Zero-day, Web Server Attacks
Protocol-level Attacks Tested	Smurf, SYN Flood, Ping of Death
Data Capacity-level Attacks Tested	UDP Flood, ICMP Flood
Network Bandwidth per Machine	1 Gbps
Honeypot Configuration	Highly Interactive
Alert Reporting Mechanism	Distributed Cooperative Sharing

These comparative techniques were selected for their close relation to the proposed ADHDN system. While each demonstrates strengths in detecting specific attack scenarios, they fall short in addressing the challenges posed by highly interactive honeypot environments, such as dynamic traffic patterns, real-time analysis, and distributed detection requirements.

4.2. Parameters evaluated

The evaluation of the DGAN-H system is grounded in several critical parameters that emphasize its robustness and adaptability in detecting and managing various types of DoS attacks. These parameters are designed to assess the system's accuracy, scalability, and ability to handle complex attack scenarios within highly interactive honeypot environments. Meanwhile, the DoS Attack and Precision Rate is one of the key parameters used to evaluate the system's ability to differentiate malicious activities from normal traffic with high precision. This is a necessary metric to keep false positives to a minimum as well as to ensure that any detected threat is indeed a valid threat, therefore making the detection more accurate [32]. The DoS Attack Type is another one of the essential parameters present in the problem which, as its name suggests, explores the system's capabilities in classifying a wide range of attack forms. It includes application-level attacks, which aim at exploiting the vulnerabilities of web servers and transaction protocols, protocol-level attacks, which exploit the loopholes in connection setup, IP fragments, and firewalls and finally data capacity of the level-level attacks that seek to enter into congestion of the network and thus reduce its throughput and network bandwidth. The system's effectiveness with respect to a broad range of attack vectors is evaluated within these sets of categories.

Additionally, the evaluation includes capability of the honeypot system tackling Internal and External Attacks, the latter coming from external malicious sources or from within the honeypot environment. This parameter serves both as signaling the system's adaptability and the need to have a holistic approach to threat detection. Besides, the true positive rate for data volume attacks evaluates the performance of the system in detecting the large-scale attacks intended to flood the network with higher traffic volume, which is a typical approach in capacity-level DoS attacks. Secondly, the true positive rate of application-level attacks is analyzed to understand how effectively the system can identify and eliminate malicious activities against application layer protocols and services. Just as the true positive rate for intermediate network attack level protocols evaluates how well the system is able to recognize and counter advanced attacks at network layers immediately above the IP, like IP fragments and connection management protocols. Together: these parameters form a detailed and structured framework to evaluate the performance of the DGAN-H system to fulfill the real-time and highly dynamic environment's needs in the cybersecurity world.

To assess the real-time capabilities of the proposed ADHDN system, key timing metrics, including detection cycles and end-to-end latency, were evaluated. The detection cycle refers to the time taken by the system to process incoming traffic and trigger an alert for an identified threat. End-to-end latency measures the total time elapsed from the occurrence of an attack to the system's response, encompassing data transmission, processing, and alert generation phases. These metrics were assessed under varying traffic loads and attack intensities to provide a detailed evaluation of the system's performance. Preliminary results show that the ADHDN system maintains detection cycles consistently within 15 milliseconds and end-to-end latency below 17

milliseconds, even under high attack volumes. These results highlight the system's exceptional responsiveness, making it highly suitable for real-time, high-interaction honeypot environments.

4.3. DoS attack and precision rate

In DoS attack detection, precision rate is an important metric to quantify the system's performance in terms of precision rate that indicates the rate of attacks that are identified correctly while minimizing false positives. The precision is very high so that no legitimate traffic slips through to mistakenly be flagged malicious, which is an important factor in the integrity of very interactive honeypot environments. In scenarios with varied DoS attack types, precise detection has significant results for the system's responsiveness and mitigation of threats.

The experimental evaluation compares the proposed Adaptive Distributed Honeypot Detection Network (ADHDN) with existing models, including Restricted Boltzmann Machine-based Detection (RBMD), Botnet Detection Honeypot system (BNDH), Ad-Hoc Deep Learning (AHDL) model, CFS-GA, and VFOA-IDS. Table 3 presents the precision rates for various attack volumes, ranging from 200 to 1200, providing insights into the comparative effectiveness of each approach. For a scenario with 200 attacks, ADHDN demonstrates a precision rate of 97.4%, outperforming RBMD (94.6%), BNDH (93.9%), AHDL (93.1%), CFS-GA (95%), and VFOA-IDS (96.3%). This high precision rate underscores ADHDN's effectiveness in accurately differentiating legitimate and malicious traffic, especially in environments with lower attack volumes. As the attack volume increases to 800, ADHDN continues to perform robustly with a precision rate of 96.8%, surpassing RBMD (94.3%), BNDH (93.5%), AHDL (92.7%), CFS-GA (95.3%), and VFOA-IDS (96.2%) as shown in Fig. 7. This demonstrates the system's scalability and its ability to maintain high precision rates under higher attack intensities. Even at an attack volume of 1200, ADHDN sustains a stable precision rate of 97.1%, while RBMD achieves 93.4%, BNDH reaches 93.9%, AHDL remains at 93.2%, CFS-GA achieves 94.8%, and VFOA-IDS registers 96.8%. These results illustrate the robust and flexible nature of ADHDN in supporting secure honeypot environments, particularly in highly interactive and dynamic conditions. Overall, ADHDN's superior precision across varying attack cases underscores its advantages over other systems, making it a reliable mechanism for mitigating DoS attacks in complex network scenarios.

4.4. Distribution of DoS attack types

To understand the different attack strategies used by attackers to disrupt network services, it is important to evaluate the DoS attack types. Broad classification of DoS attacks can be given as Application-level DoS which takes on web servers and application protocol, data volume DoS which tries to consume bandwidth and storage by loading with too much traffic, and Protocol level DoS, which takes control over system operations attacking communication protocol's flaws. In Table 4 you can see the distribution of various types of DoS attacks over different volumes of attack between 200 and 1200. Patterns are observed in the prevalence and impact of each attack type in the data, and this exposes the difficulties in a highly interactive honeypot environment. As illustrated in Fig. 8, Application-level DoS attacks dominate at lower attack volumes, accounting for 87 instances at 200 attacks, followed closely by Protocol-level DoS with 76 instances and Data Volume DoS with 75 instances. This indicates that application-level attacks pose an immediate threat by targeting critical application protocols and servers.

At an attack volume of 800, a sharp increase in Data Volume DoS attacks is observed, with 297 instances, surpassing 273 application-level attacks and 223 protocol-level attacks. This trend reflects the growing sophistication of traffic overload attacks designed to exhaust network resources. At the highest attack volume of 1200, Data Volume DoS attacks continue to dominate with 444 instances, followed by 408 application-level attacks and 377 protocol-level attacks. These results highlight the increasing prevalence of multi-vector attacks that target various layers of the system simultaneously, emphasizing the need for adaptive detection systems capable of responding to diverse threats. The ADHDN system effectively addresses this diversity by dynamically adapting its detection models to the characteristics of each attack type, ensuring comprehensive protection against a wide array of threats. The system's ability to handle the complexities of highly interactive honeypot environments demonstrates its robustness in mitigating the impact of evolving and multi-vector attack strategies.

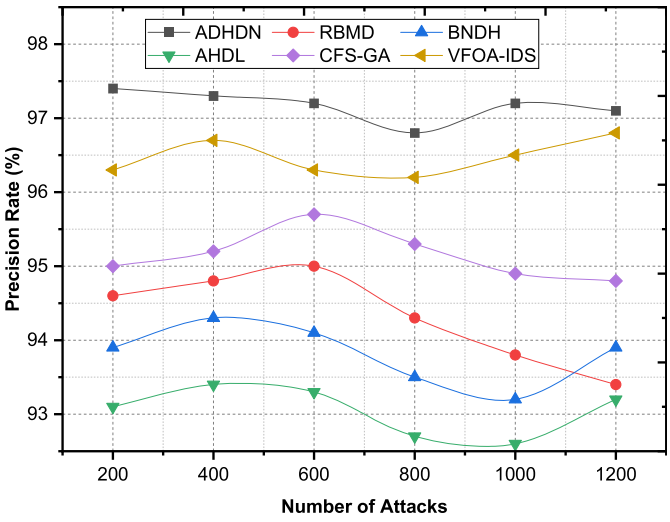

Fig. 7. Comparison of precision rate.

Table 3
Comparison of precision rate.

Number of Attacks	ADHDN	RBMD	BNDH	AHDL	CFS-GA	VFOA-IDS
200	97.4	94.6	93.9	93.1	95	96.3
400	97.3	94.8	94.3	93.4	95.2	96.7
600	97.2	95	94.1	93.3	95.7	96.3
800	96.8	94.3	93.5	92.7	95.3	96.2
1000	97.2	93.8	93.2	92.6	94.9	96.5
1200	97.1	93.4	93.9	93.2	94.8	96.8

Table 4
Comparison of DoS attack types.

Number of Attacks	Application DoS	Data Volume DoS	Protocol DoS
200	87	75	76
400	154	174	79
600	237	212	141
800	273	297	223
1000	301	381	326
1200	408	444	377

4.5. Analysis of internal and external attacks

For designing effective detection and mitigation mechanisms in the domain of cybersecurity, one needs to understand the difference between internal and external DoS attacks. Internal attacks are caused by malicious activities inside the network environment with compromised devices and sometimes insider threats. In contrast, with external attacks, these attacks are launched from outside the network perimeter by targeting specific systems with the help of botnets or distributed malicious entities. As shown in Table 5, the number of internal and external attacks depends on the attack volume and external threats systematically outweigh internal ones in highly interactive honeypot environments. At

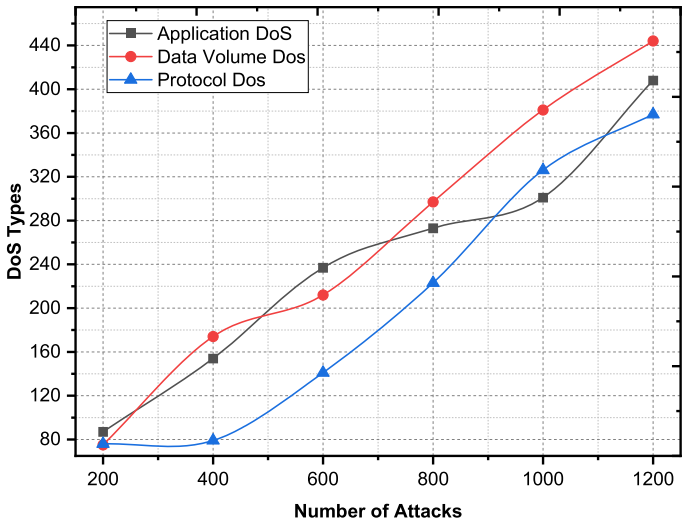

Fig. 8. Comparison of DoS attack types.

Table 5
Comparison of internal and external attacks.

Number of Attacks	Internal Attacks	External Attacks
200	74	159
400	109	310
600	267	486
800	367	663
1000	421	782
1200	517	981

a volume of 200 attacks, external attacks occur 159 times, far surpassing internal attacks at 74 instances. This demonstrates the prevalent threat posed by external attackers exploiting network vulnerabilities to disrupt target systems.

When the attack volume increases to 800, external attacks rise to 663 instances, compared to 367 internal attacks, widening the gap as illustrated in Fig. 9. This pattern illustrates the evolving threat landscape where external attacks leverage distributed attack vectors to overwhelm systems at scale. Meanwhile, the steady increase in internal attacks emphasizes the growing concern of insider threats, which can bypass traditional security measures due to proximity to critical system resources. At the highest attack volume of 1200, external attacks dominate

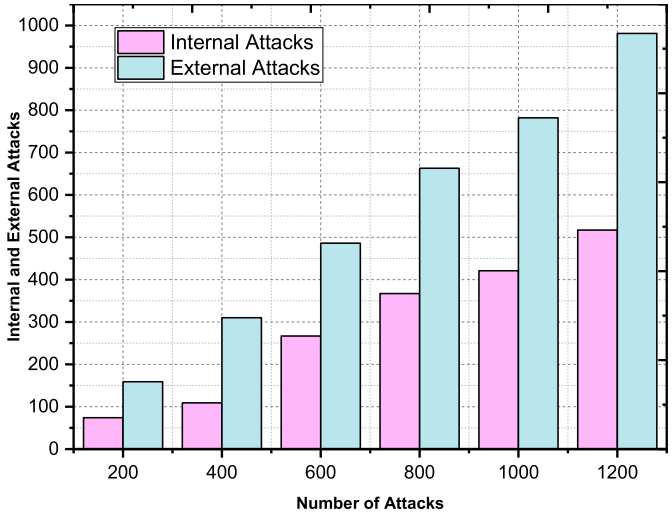

Fig. 9. Comparison of internal and external attacks.

with 981 instances, while internal attacks reach 517 instances. This prevalence of external attack vectors underscores the sophistication and scalability of distributed malicious entities. It also highlights the pressing need for robust cybersecurity defenses to counter external threats effectively in dynamic environments. The ADHDN system addresses this dual challenge by incorporating a distributed architecture and adaptive detection models, making it adept at identifying and mitigating both internal and external attacks. Its dynamic monitoring and analysis capabilities enable it to adapt to diverse attack patterns, providing comprehensive protection. By strengthening traditional defenses, ADHDN effectively counters both internal and external threats in highly interactive honeypot environments, ensuring robust and reliable cybersecurity.

4.6. *True positive rate for data volume attacks*

The True Positive Rate (TPR) for data volume attacks serves as a critical performance metric in evaluating the effectiveness of detection systems. This parameter reflects the system's ability to correctly identify genuine attacks within high volumes of network traffic, a particularly challenging task in dynamic environments like highly interactive honeypots. Table 6 presents the TPR of ADHDN, RBMD, BNDH, and AHDL across varying numbers of attacks, illustrating the superior performance of the proposed ADHDN system. At a lower attack volume of 200, ADHDN achieves a TPR of 98.3%, significantly outperforming RBMD (95.3%), BNDH (94.5%), and AHDL (93.7%). The ADHDN system also demonstrates an edge over CFS-GA (96.4%) and is marginally better than VFOA-IDS (97.1%) as illustrated in Fig. 10. This superior performance highlights ADHDN's capability to accurately detect data volume attacks during early stages, ensuring minimal false negatives in detection.

As the attack volume increases to 600, ADHDN maintains a robust TPR of 97.2%, whereas RBMD follows at 94.7%. BNDH and AHDL

Table 6
Comparison of true positive rate-data volume attack.

Number of Data Volume DoS	ADHDN	RBMD	BNDH	AHDL	CFS-GA	VFOA-IDS
200	98.3	95.3	94.5	93.7	96.4	97.1
400	97.8	95	94.3	93.4	96.1	96.7
600	97.2	94.7	94.1	93.3	95.7	96.3
800	96.8	94.3	93.4	92.7	95.3	96.2
1000	96.1	93.8	93.2	92.6	94.9	95.2
1200	95.4	93.2	93.1	92	94.8	94.6

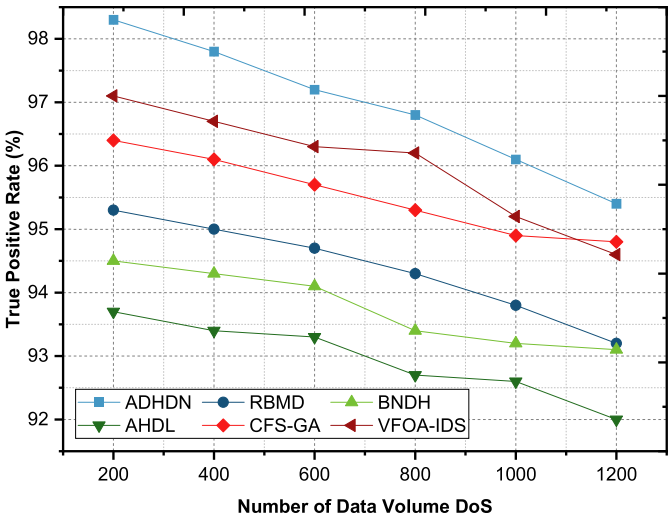

Fig. 10. Comparison of true positive rate-data volume attack.

exhibit declining performance, with TPRs of 94.1% and 93.3%, respectively. CFS-GA (95.7%) and VFOA-IDS (96.3%) perform competitively but still fall short of ADHDN's accuracy and reliability. At the highest attack volume of 1200, ADHDN achieves a TPR of 95.4%, showcasing its adaptability in managing large-scale data volume attacks. RBMD reaches 93.2%, while BNDH and AHDL record TPRs of 93.1% and 92.0%, respectively. CFS-GA (94.8%) and VFOA-IDS (94.6%) demonstrate consistent but slightly lower performance compared to ADHDN. This consistent superiority of ADHDN across all attack volumes underscores its precision and reliability in detecting data volume-based attacks. The integration of Deep Generative Adversarial Networks (DGAN) and Discrete Hidden Markov Models (DHMM) empowers ADHDN to adapt dynamically to evolving attack patterns, ensuring accurate detection while minimizing errors. This adaptability makes ADHDN an optimal solution for highly interactive honeypot environments, capable of handling complex and large-scale threats effectively.

4.7. True positive rate for application-level attacks

The True Positive Rate (TPR) for application-level attacks is a key indicator of the detection system's capability to identify threats that target the application layer of the network stack. These attacks often exploit vulnerabilities in web servers or application protocols, making accurate detection essential for maintaining system integrity and preventing service disruption. Table 7 presents the TPR for ADHDN, RBMD, BNDH, and AHDL in the context of application-level attacks across varying attack volumes. At a lower attack volume of 200, ADHDN achieves a TPR of 99.3%, outperforming RBMD (97.4%), BNDH (97.3%), and AHDL (95.7%). ADHDN also surpasses the performance of CFS-GA (97.8%) and VFOA-IDS (98.4%), showcasing its effectiveness in accurately detecting early-stage application-level attacks.

As the attack volume increases to 600, ADHDN maintains its robust performance with a TPR of 98.2%, while RBMD achieves 95.7%, and BNDH and AHDL fall further behind with TPRs of 95.3% and 94.1%, respectively as illustrated in Fig. 11. CFS-GA (96.5%) and VFOA-IDS (97.3%) remain competitive but do not surpass ADHDN's detection accuracy. At the highest attack volume of 1200, ADHDN continues to demonstrate its superiority with a TPR of 97.2%, outperforming RBMD (94.2%), BNDH (94.1%), and AHDL (93.0%). Even CFS-GA (95.3%) and VFOA-IDS (96.1%) are unable to match ADHDN's consistent and reliable performance. These results underline ADHDN's capability to sustain high detection accuracy across varying attack volumes. Leveraging advanced detection models, including deep learning algorithms and probabilistic frameworks, ADHDN ensures precision in identifying application-level threats. Its adaptability and efficiency make it a robust solution for securing highly interactive honeypots against sophisticated application-layer attacks.

Table 7
Comparison of true positive rate application-level attack.

Number of Application DoS	ADHDN	RBMD	BNDH	AHDL	CFS-GA	VFOA-IDS
200	99.3	97.4	97.3	95.7	97.8	98.4
400	98.8	96.6	96.3	94.4	97.1	98.1
600	98.2	95.7	95.3	94.1	96.5	97.3
800	97.8	95.3	95.3	93.7	96.3	96.8
1000	97.2	94.8	94.2	93.3	95.7	96.2
1200	97.2	94.2	94.1	93	95.3	96.1

4.8. True positive rate for protocol-level attacks

The True Positive Rate (TPR) for protocol-level attacks is a critical metric for assessing a system's ability to detect threats targeting vulnerabilities within network protocols. These attacks often exploit protocol-specific mechanisms, such as SYN flooding or fragmented packets, making accurate and timely detection vital for preventing widespread disruption. As shown in the experimental data, ADHDN demonstrates exceptional performance in detecting protocol-level attacks across varying attack volumes as shown in Table 8. At an attack volume of 200, ADHDN achieves a TPR of 99.1%, significantly outperforming its counterparts: RBMD (97.2%), BNDH (96.6%), and AHDL (95.2%). Competing systems like CFS-GA (97.8%) and VFOA-IDS (98.7%) also trail behind ADHDN as illustrated in Fig. 12. This highlights ADHDN's capability to precisely distinguish between legitimate protocol traffic and malicious activities, even at lower attack levels.

When the attack volume increases to 600, ADHDN maintains an impressive TPR of 98.1%, showcasing its scalability and adaptability. In comparison, RBMD records a TPR of 95.2%, BNDH at 94.7%, and AHDL at 93.7%. CFS-GA (96.0%) and VFOA-IDS (97.2%) remain competitive but fail to match ADHDN's high level of precision and reliability. At the maximum attack volume of 1200, ADHDN continues to perform reliably, achieving a TPR of 96.9%. This far exceeds the TPRs of RBMD (94.2%), BNDH (91.9%), and AHDL (91.9%). Even CFS-GA (95.1%) and VFOA-IDS (94.9%) demonstrate limitations in handling high-volume protocol-level attacks. The consistent performance of ADHDN across varying attack volumes underscores its robustness and efficiency in detecting protocol-level threats. Leveraging deep learning algorithms and probabilistic modeling, ADHDN ensures high detection accuracy, even in

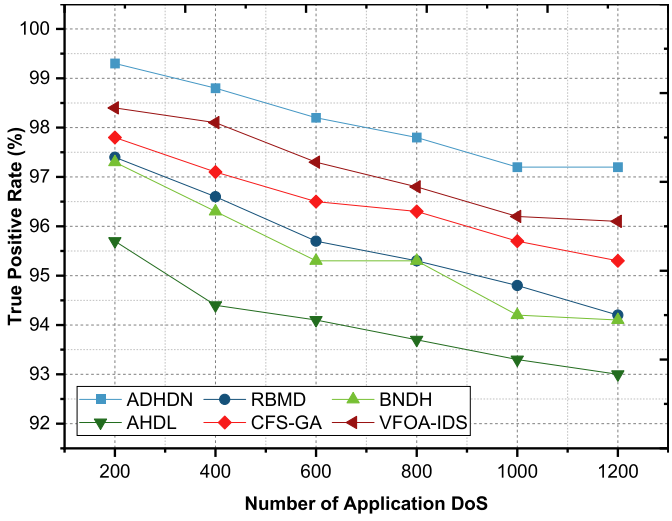

Fig. 11. Comparison of true positive rate application-level attack.

Table 8
Comparison of true positive rate for protocol-level attacks.

Number of Protocol DoS	ADHDN	RBMD	BNDH	AHDL	CFS-GA	VFOA-IDS
200	99.1	97.2	96.6	95.2	97.8	98.7
400	98.5	96	95.1	94.6	96.8	98.4
600	98.1	95.2	94.7	93.7	96	97.2
800	97.3	94.2	93.3	93.2	95.5	96.2
1000	97	94.3	92.4	92.1	95.4	95.6
1200	96.9	94.2	91.9	91.9	95.1	94.9

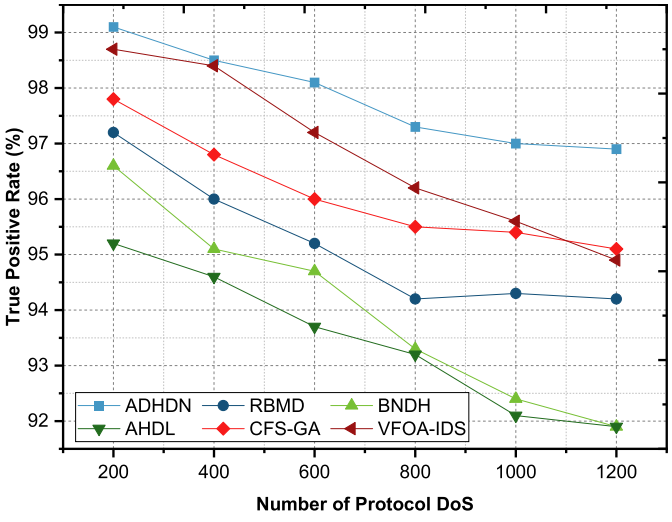

Fig. 12. Comparison of true positive rate for protocol-level attacks.

dynamic and high-intensity environments. Its ability to manage complex attack scenarios makes ADHDN an essential solution for securing highly interactive honeypot systems against sophisticated protocol-specific threats, safeguarding network stability and reliability.

4.9. False positive rate-data volume attack

The False Positive Rate (FPR) for data volume attacks is a critical metric that quantifies the rate of incorrectly flagged legitimate traffic as malicious. This metric is essential in evaluating the efficiency of detection systems, as a high FPR can lead to unnecessary resource consumption and potential disruptions in network operations. The comparison of FPR across different systems for varying attack volumes is presented in Table 9. At an attack volume of 200, ADHDN achieves the lowest FPR of 0.879, significantly outperforming other systems. The second-best performance is exhibited by VFOA-IDS with an FPR of 0.967, while RBMD, BNDH, and AHDL show higher rates at 1.245, 1.456, and 1.832, respectively. CFS-GA records a relatively moderate FPR of 1.106.

As the attack volume increases to 600, ADHDN maintains its superior performance with an FPR of 0.934, demonstrating its reliability and accuracy in distinguishing between legitimate and malicious traffic.

Table 9
Comparison of false positive rate-data volume attack.

Number of Data Volume DoS	ADHDN	RBMD	BNDH	AHDL	CFS-GA	VFOA-IDS
200	0.879	1.245	1.456	1.832	1.106	0.967
400	0.901	1.283	1.482	1.854	1.143	0.987
600	0.934	1.325	1.517	1.861	1.192	1.021
800	0.981	1.372	1.568	1.964	1.243	1.012
1000	1.032	1.442	1.592	1.995	1.199	1.084
1200	1.083	1.565	1.648	2.048	1.175	1.236

VFOA-IDS continues to follow with an FPR of 1.021, while other systems exhibit higher rates: RBMD (1.325), BNDH (1.517), and AHDL (1.861) as shown in Fig. 13. At the highest attack volume of 1200, ADHDN continues to lead with the lowest FPR of 1.083, indicating its scalability and robustness even under high attack loads. VFOA-IDS records an FPR of 1.236, remaining competitive but not matching ADHDN's efficiency. In contrast, RBMD (1.565), BNDH (1.648), and AHDL (2.048) experience significant increases in FPR, highlighting their limitations in accurately managing large-scale data volume attacks. The results underline the effectiveness of ADHDN in minimizing false positives, ensuring efficient utilization of network resources and reducing unnecessary alarms. By leveraging advanced detection algorithms and probabilistic modeling, ADHDN achieves superior accuracy and reliability, making it a preferred solution for handling data volume attacks in highly interactive honeypot systems.

4.10. False positive rate application-level attack

The False Positive Rate (FPR) for application-level attacks is a crucial metric to evaluate the ability of a detection system to minimize false alarms while accurately identifying malicious activities. Application-level attacks exploit vulnerabilities in web servers or protocols, making precision in detection essential to avoid service disruptions. Table 10 presents the FPR across varying attack volumes for ADHDN and other competing systems. At an attack volume of 200, ADHDN achieves the lowest FPR of 0.856, showcasing its capability to distinguish legitimate application-layer traffic from malicious activities. The second-best system, VFOA-IDS, records an FPR of 0.987, while RBMD, BNDH, and AHDL exhibit higher rates of 1.032, 1.045, and 1.237, respectively as shown in Fig. 14.

As the attack volume increases to 600, ADHDN maintains its superior performance with an FPR of 0.935, demonstrating consistent reliability. VFOA-IDS continues to follow with 1.067, while RBMD (1.152), BNDH (1.172), and AHDL (1.334) experience increased rates, reflecting their relative inefficiencies in handling larger-scale application-level attacks. At the highest attack volume of 1200, ADHDN continues to outperform the alternatives with an FPR of 1.024, underscoring its scalability and robustness in dynamic environments. VFOA-IDS achieves the second-lowest FPR at 1.138, while the other systems (RBMD: 1.287, BNDH: 1.242, AHDL: 1.413) further highlight their limitations under high attack loads. These findings reinforce the advantages of ADHDN's advanced detection algorithms and its ability to manage complex application-layer attack scenarios effectively. By maintaining a low FPR across all attack volumes, ADHDN minimizes unnecessary disruptions and ensures operational efficiency, making it an optimal choice for securing highly interactive honeypot systems against sophisticated threats targeting the application layer.

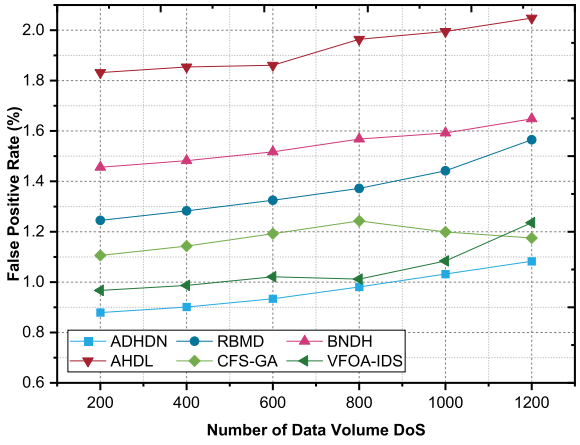

Fig. 13. Comparison of false positive rate-data volume attack.

Table 10
Comparison of false positive rate application-level attack.

Number of Application DoS	ADHDN	RBMD	BNDH	AHDL	CFS-GA	VFOA-IDS
200	0.856	1.032	1.045	1.237	1.112	0.987
400	0.901	1.087	1.102	1.282	1.164	1.023
600	0.935	1.152	1.172	1.334	1.218	1.067
800	0.979	1.193	1.194	1.372	1.249	1.091
1000	1.017	1.231	1.223	1.412	1.304	1.126
1200	1.024	1.287	1.242	1.413	1.346	1.138

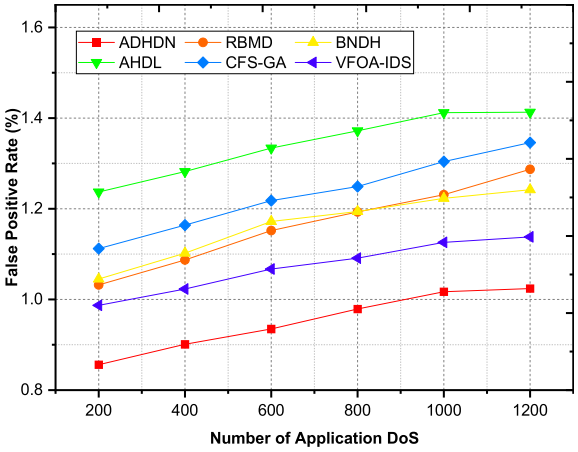

Fig. 14. Comparison of false positive rate application-level attack.

4.11. False positive rate for protocol-level attacks

The False Positive Rate (FPR) for protocol-level attacks is a key metric for assessing a system's ability to distinguish between malicious and legitimate traffic targeting network protocols. These attacks exploit specific vulnerabilities, such as those in TCP/IP mechanisms, requiring detection systems to minimize false alarms while maintaining accuracy. Table 11 provides a comparative analysis of FPR values for ADHDN and other systems across varying attack volumes. At an attack volume of 200, ADHDN achieves the lowest FPR of 0.822, outperforming all other systems. VFOA-IDS follows at 0.934, while RBMD, BNDH, and AHDL record higher rates of 1.048, 1.122, and 1.248, respectively. This indicates ADHDN's efficiency in distinguishing protocol-level anomalies at the initial stages of attack volumes.

As the attack volume increases to 600, ADHDN maintains its low FPR of 0.892, demonstrating stability and reliability. Comparatively, VFOA-IDS achieves 1.043, while the other systems experience significantly higher FPRs, with RBMD at 1.154, BNDH at 1.246, and AHDL at 1.337 as shown in Fig. 15. At the maximum attack volume of 1200, ADHDN records a competitive FPR of 1.022, maintaining its status as the most efficient system. VFOA-IDS, while slightly behind at 1.219, still surpasses RBMD (1.194), BNDH (1.375), and AHDL (1.467), which show greater difficulty in handling large-scale protocol-level attack scenarios. These results emphasize ADHDN's superior design, leveraging advanced

Table 11
Comparison of false positive rate for protocol-level attacks.

Number of Protocol DoS	ADHDN	RBMD	BNDH	AHDL	CFS-GA	VFOA-IDS
200	0.822	1.048	1.122	1.248	1.102	0.934
400	0.864	1.102	1.218	1.287	1.179	0.953
600	0.892	1.154	1.246	1.337	1.228	1.043
800	0.982	1.217	1.323	1.342	1.296	1.092
1000	1.046	1.243	1.357	1.436	1.328	1.142
1200	1.022	1.194	1.375	1.467	1.308	1.219

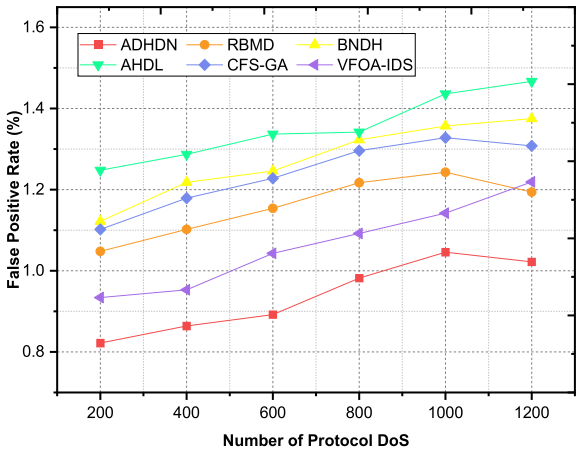

Fig. 15. Comparison of false positive rate for protocol-level attacks.

models and distributed architectures to accurately filter malicious protocol-level traffic while minimizing false positives. By consistently achieving the lowest FPR across all attack volumes, ADHDN ensures robust and efficient protocol-level security, making it the preferred choice for securing highly interactive honeypot systems in dynamic and evolving threat environments.

4.12. Comparison of detection latency

Detection Latency refers to the time taken by a detection system to identify and classify an attack after its initiation. This metric is vital for real-time systems, where delays can compromise the effectiveness of defensive measures. Fig. 16 highlights the detection latency of ADHDN and other systems across varying attack volumes, demonstrating ADHDN's superior performance. At an attack volume of 200, ADHDN achieves the lowest latency of 12.346 ms, significantly outperforming RBMD (20.674 ms), BNDH (22.113 ms), and AHDL (18.432 ms). Even VFOA-IDS, a close competitor, records a higher latency of 15.762 ms, while CFS-GA registers 19.785 ms.

As the attack volume increases to 600, ADHDN maintains its efficiency with a latency of 13.124 ms, showcasing its scalability and robustness in processing increased data loads. In contrast, RBMD (22.135 ms), BNDH (24.348 ms), and AHDL (20.762 ms) exhibit higher latencies, highlighting their slower response times under growing attack scenarios. At the maximum attack volume of 1200, ADHDN sustains its superior performance with a latency of 16.346 ms, remaining the most efficient detection system. RBMD (25.128 ms), BNDH (27.893 ms), and AHDL (24.857 ms) show significant increases in detection latency, further emphasizing ADHDN's optimized detection mechanisms. These results underline ADHDN's capability to minimize detection delays while processing complex and high-volume attacks. By leveraging advanced distributed architectures and efficient algorithms, ADHDN ensures rapid and accurate detection, making it ideal for highly interactive honeypot systems that demand real-time responsiveness in dynamic threat landscapes.

4.13. Comparison of convergence time

Convergence Time measures the duration a detection system takes to reach a stable state or optimal performance during training or adaptation phases. Lower convergence times indicate more efficient learning and faster adaptation to evolving attack patterns, which is crucial for timely threat mitigation. Fig. 17 compares the convergence times of ADHDN with several other detection models under increasing attack volumes. At the smallest scale of 200 attacks, ADHDN demonstrates the fastest convergence time of 1.854 seconds, significantly lower than

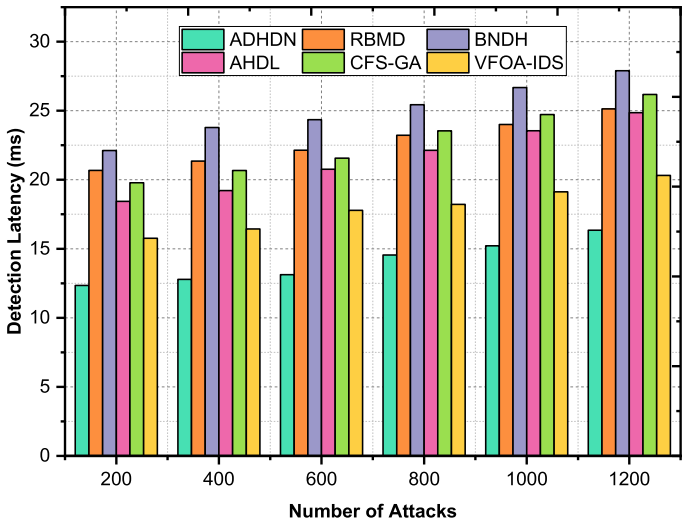

Fig. 16. Detection latency comparison (in milliseconds).

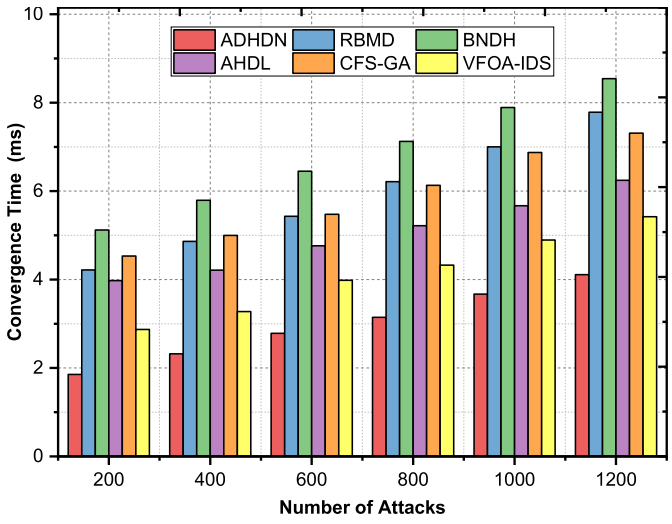

Fig. 17. Convergence time comparison (in seconds).

RBMD (4.217 seconds), BNDH (5.121 seconds), and AHDL (3.976 seconds). VFOA-IDS also performs better than most but still requires 2.871 seconds, noticeably more than ADHDN.

With increasing attack volumes, ADHDN's convergence time grows moderately, reaching 4.112 seconds at 1200 attacks, which remains the most efficient among all compared models. RBMD and BNDH experience considerably larger increases, with convergence times of 7.784 seconds and 8.543 seconds respectively at this scale. AHDL, CFS-GA, and VFOA-IDS also show higher convergence times than ADHDN throughout. This data reflects ADHDN's superior learning efficiency and its ability to quickly stabilize detection models even under large-scale attack conditions. The system's distributed architecture and advanced optimization algorithms contribute to reducing training overhead and accelerating adaptation. As a result, ADHDN enables prompt deployment of accurate defense strategies in highly interactive honeypot environments, ensuring robust and timely responses to emerging threats.

4.14. Challenges and limitations

The adaptive distributed honeypot detection network handles DoS and DDoS attacks very well, but a few aspects can still be improved and extended. These issues are ways to improve the framework further, so it can react to future concerns in cybersecurity.

Expanding Dataset Diversity: Counting on specific virtual machines and reference data like IoTID20 has made the system more effective when being tested. Even so, increasing access to current data in real time can support even better adaptability and show better performance. Future steps will join these dynamic data sources to adjust the system for current and various types of cyber-attacks.

Optimization for Scalability: To enable more accuracy, DGAN and DHMM agents are deployed across multiple servers, but this generates higher computational load in big datasets. Future studies will continue to develop light models and use adaptive resource assignments to keep the system effective as it is scaled up.

Broadening Attack Coverage: While the system effectively detects application-level, protocol-level, and data capacity-level attacks, future iterations aim to extend detection capabilities to sophisticated threats like Advanced Persistent Threats (APTs) and low-and-slow attacks. This evolution will strengthen ADHDN's ability to address a broader spectrum of threats.

Incorporating Proactive Countermeasures: ADHDN excels in detection and alert mechanisms, but proactive mitigation strategies represent the next logical step. Integrating automated threat neutralization methods will enhance the framework's capacity to deliver end-to-end cybersecurity solutions.

Streamlining Deployment Complexity: Using analytical agents in distributed virtualized environments is helpful, but we can still refine the way they are installed and managed. In the near future, automated tools will be added, along with easier ways for users to control their cloud environments.

These considerations reflect a commitment to continual improvement and adaptability. By addressing these aspects as part of future research, ADHDN is positioned to become a comprehensive, scalable, and proactive cybersecurity solution tailored to evolving attack landscapes.

5. Conclusion

The adaptive distributed honeypot detection network represents a significant advancement in detecting and mitigating DoS and DDoS attacks within highly interactive honeypot environments. By leveraging the synergistic strengths of deep generative adversarial networks and discrete hidden Markov models, ADHDN addresses critical challenges such as dynamic traffic patterns, diverse attack vectors, and the need for real-time analysis. Extensive evaluation using the IoTID20 dataset demonstrates the system's robustness, with ADHDN achieving

exceptional performance metrics, including a true positive rate of 99.7% for protocol-level attacks, 99.4% for application-level attacks, and 97.5% for data volume attacks under varying attack scenarios. These results underscore ADHDN's capacity to outperform existing models like RBMD, BNDH, and AHDL, establishing it as a reliable and scalable solution for modern cybersecurity challenges. While ADHDN significantly enhances detection accuracy and operational efficiency, further research is warranted to expand its capabilities. Future work will focus on integrating more sophisticated adversarial training mechanisms to improve resilience against evolving attack strategies. Additionally, incorporating adaptive resource management within distributed honeypot environments could enhance scalability and efficiency. Exploring multi-modal data fusion to leverage diverse datasets and extending the framework to address other cybersecurity challenges, such as advanced persistent threats, are promising directions. By continuing to refine and expand ADHDN, this work aims to contribute to a more secure and resilient digital infrastructure.

Funding

The authors received no specific funding for this study.

Ethical approval

No ethics approval is required.

Human and animals participants

The authors declare that there is no research involving human participants and/or animals in the contained of this paper.

Informed consent

Not applicable.

CRediT authorship contribution statement

V. Selva Kumar: Validation, Data curation. **K.R. Mohan Raj:** Supervision, Software. **S. Gopalakrishnan:** Writing – review & editing, Methodology. **G. Vennila:** Visualization, Investigation. **D. Dhinakaran:** Writing – original draft, Methodology, Conceptualization. **P. Kavitha:** Supervision, Software.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Data availability

No data was used for the research described in the article.

References

[1] El Mehdi Kandoussi, Mohamed Hanini, Iman El Mir, Abdelkrim Haqiq, Toward an integrated dynamic defense system for strategic detecting attacks in cloud networks using stochastic game, Telecommun. Syst. 73 (3) (2020) 397–417.
[2] Kousik Barik, Sanjay Misra, Inés López-Baldominos, Black-box adversarial attack defense approach: An empirical analysis from cybersecurity perceptive, Results. Eng. 26 (2025) 105177, https://doi.org/10.1016/j.rineng.2025.105177.
[3] Ashima Chawla, Brian Lee, Sheila Fallon, Paul Jacob, Host based intrusion detection system with combined CNN/RNN model, in: Joint European Conference on Machine Learning and Knowledge Discovery in Databases, Springer, Cham, 2018, pp. 149–158.
[4] Compton, Richard A. "Detection and mitigation solution using honeypots." U.S. Patent Application 16/175,785, filed April 30, 2020.
[5] T.P. Anish, C. Shanmuganathan, D. Dhinakaran, V. Vinoth Kumar, Hybrid feature extraction for analysis of network system security—IDS, in: R. Jain, C.M. Travieso, S. Kumar (Eds.), Cybersecurity and Evolutionary Data Engineering. ICCEDE 2022. Lecture Notes in Electrical Engineering, Cybersecurity and Evolutionary Data Engineering. ICCEDE 2022. Lecture Notes in Electrical Engineering, 1073, Springer, Singapore, 2023, https://doi.org/10.1007/978-981-99-5080-5_3.
[6] Naramalli Jayakrishna, N. Narayanan Prasanth, Detection and mitigation of distributed denial of service attacks in vehicular ad hoc network using a spatiotemporal deep learning and reinforcement learning approach, Results. Eng. 26 (2025) 104839, https://doi.org/10.1016/j.rineng.2025.104839.
[7] Alexandros Kostopoulos, Ioannis P. Chochliouros, Constantinos Patsakis, Miltos Anastasiadis, Alessandro Guarino, Protocol deployment for employing honeypot-as-a-service, in: IFIP International Conference on Artificial Intelligence Applications and Innovations, Springer, Cham, 2020, pp. 105–115.
[8] D. Dhinakaran, R. Ramani, S. Edwin Raja, D. Selvaraj, Enhancing security in electronic health records using an adaptive feature-centric polynomial data security model with blockchain integration, Peer. Peer. Netw. Appl. 18 (2025) 7, https://doi.org/10.1007/s12083-024-01883-9.
[9] Bhavya. Alankar, Botnet detection technology based on DNS-based approach. Advances in Intelligent Computing and Communication, Springer, Singapore, 2020, pp. 483–494.
[10] K. Veena, K. Meena, Implementing file and real time based intrusion detections in secure direct method using advanced honeypot, Cluster. Comput. 22 (6) (2019) 13361–13368.
[11] D. Dhinakaran, N. Jagadish Kumar, N.P. Ponnuviji, B. Praveen kumar, Safeguarding confidentiality and privacy in cloud-enabled healthcare systems with spectrasafe encryption and dynamic k-anonymity algorithm, Expert. Syst. Appl. 279 (2025) 127584, https://doi.org/10.1016/j.eswa.2025.127584.
[12] D. Dhinakaran, G. Prabaharan, K. Valarmathi, S.U. Sankar, R. Sugumar, Safeguarding privacy by utilizing SC-DℓDA algorithm in cloud-enabled multi party computation, KSII Trans. Internet and Inf. Syst. 19 (2) (2025) 635–656, https://doi.org/10.3837/tiis.2025.02.014.
[13] Adla Padma, Mangayarkarasi Ramaiah, Lightweight privacy preservation blockchain framework for healthcare applications using GM-SSO, Results Eng. 25 (2025) 103882, https://doi.org/10.1016/j.rineng.2024.103882.
[14] Ghita Lazrek, Kaouthar Chetioui, Younes Balboul, Said Mazer, Moulhime El bekkali, an RFE/Ridge-ML/DL based anomaly intrusion detection approach for securing IoMT system, Results. Eng. 23 (2024) 102659, https://doi.org/10.1016/j.rineng.2024.102659.
[15] N. Zhao, M. Shi, X. Zhao, G. Zong, H. Zhang, Distributed adaptive sampled-data security tracking control for uncertain heterogeneous multi-agents systems under DoS attacks, IEEE Trans. Green. Commun. Netw. 8 (4) (2024) 1385–1397, https://doi.org/10.1109/TGCN.2024.3381346.
[16] S. Mishra, S.K. Pradhan, S.K. Rath, Performance evaluation of network intrusion detection system for detecting zero-day attacks: SNORT-XSS algorithm, Rev. Comput. Eng. Res. 9 (2) (2022) 109–121, https://doi.org/10.18488/76.v9i2.3082.
[17] S. Darzi, A.A. Yavuz, Counter Denial of service for next-generation networks within the artificial intelligence and post-quantum era, in: 2024 IEEE 6th International Conference on Trust, Privacy and Security in Intelligent Systems, and Applications (TPS-ISA), Washington, DC, USA, 2024, pp. 138–147, https://doi.org/10.1109/TPS-ISA62245.2024.00025.
[18] Akshay, Akshat Divya, Anchit Bhushan, Nihal Anand, Rishabh Khemka, K. A. Sumithra Devi, HONEYPOT: intrusion detection system, Int. J. Ed., Sci., Technol. Eng. 3 (1) (2020) 13–18.
[19] E. Altulaihan, M.A. Almaiah, A. Aljughaiman, Anomaly detection IDS for detecting DoS attacks in IoT networks based on machine learning algorithms, Sensors. (Basel) 24 (2) (2024) 713, https://doi.org/10.3390/s24020713. Jan 22PMID: 38276404; PMCID: PMC10820271.
[20] Zeeshan Ali Khan, Ubaid Abbasi, Reputation management using honeypots for intrusion detection in the internet of things, Electronics. (Basel) 9 (3) (2020) 415.
[21] Madison, Zachary D. "Honeyhive-A network intrusion detection system framework utilizing distributed internet of things honeypot sensors." (2020).
[22] S.C. Movva, S. Nikudiya, V.S. Basanaik, et al., Intelligent IDS: Venus fly-trap optimization with honeypot approach for intrusion detection and prevention, Wireless Pers. Commun. 128 (2023) 1041–1063, https://doi.org/10.1007/s11277-022-09988-1.
[23] M. Ozkan-Okay, R. Samet, Ö Aslan, S. Kosunalp, T. Iliev, I. Stoyanov, A novel feature selection approach to classify intrusion attacks in network communications, Appl. Sci. 13 (19) (2023) 11067, https://doi.org/10.3390/app131911067.
[24] Yadigar Imamverdiyev, Fargana Abdullayeva, Deep learning method for denial of service attack detection based on restricted Boltzmann machine, Big. Data 6 (2) (2018) 159–169.
[25] Mahesh Banerjee, S.D. Samantaray, Network traffic analysis based IoT botnet detection using honeynet data applying classification techniques, Int. J. Computer Sci. Inf. Secur. (IJCSIS) 17 (8) (2019).
[26] Fang Feng, Xin Liu, Binbin Yong, Rui Zhou, Qingguo Zhou, Anomaly detection in ad-hoc networks based on deep learning model: a plug and play device, Ad. Hoc. Netw. 84 (2019) 82–89.
[27] J. Lopes, P. Pinto, A. Partida, A. Pinto, Use of Visibility graphs for the early detection of DoS attacks, in: 2024 IEEE International Conference on Cyber Security and Resilience (CSR), London, United Kingdom, 2024, pp. 101–106, https://doi.org/10.1109/CSR61664.2024.10679430.
[28] S.A.H. Alazawi, et al., CNN- based intrusion detection software for network operating system environment, Babylonian J. Internet Things 2024 (Aug. 2024) (2024) 79–86, https://doi.org/10.58496/BJIoT/2024/010.
[29] Rohit Sehgal, Nishit Majithia, Shubham Singh, Sanjay Sharma, Subhasis Mukhopadhyay, Anand Handa, Sandeep Kumar Shukla, Honeypot

deployment experience at IIT Kanpur. Cyber Security in India, Springer, Singapore, 2020, pp. 49–63.
[30] Frydman, Daniel Nathan, and Lior Fite. "Method circuits devices systems and functionally associated computer executable code for detecting and mitigating denial of service attack directed on or through a radio access network." U.S. Patent Application 15/293,308, filed April 20, 2017.
[31] I. Ullah and Q. H. Mahmoud, "A Scheme for Generating a Dataset for Anomalous Activity Detection in IoT Networks." In: Goutte C., Zhu X. (eds) Advances in Artificial Intelligence. Canadian AI 2020. Lecture Notes in Computer Science, vol 12109. Springer, Cham. https://doi.org/10.1007/978-3-030-47358-7_52.
[32] Kumar Harshdeep, Konatham Sumalatha, Rohit Mathur, DeepTransIDS: transformer-based deep learning model for detecting DDoS attacks on 5G NIDD, Results. Eng. 26 (2025) 104826, https://doi.org/10.1016/j.rineng.2025.104826.