International Journal of Computer Networks and Applications (IJCNA)
DOI: 10.22247/ijcna/2023/223316 Volume 10, Issue 4, July – August (2023)

RESEARCH ARTICLE

An Automated Intrusion Detection and Prevention Model for Enhanced Network Security and Threat Assessment

K Prabu
School of Computing Science and Engineering, Galgotias University, Uttar Pradesh, India.
k.prabu@galgotiasuniversity.edu.in

P Sudhakar
School of Computing Science and Engineering, Galgotias University, Uttar Pradesh, India.
p.sudhakar@galgotiasuniversity.edu.in

Received: 07 June 2023 / Revised: 26 July 2023 / Accepted: 04 August 2023 / Published: 31 August 2023

Abstract – Amid the soaring cyber threats and security breaches, we introduce an automated intrusion detection and prevention model to bolster threat assessment and security data solutions. Our model, utilizing the state-of-the-art Automatic Intrusion Detection System (AIDS) and real-time data analysis, promptly identifies and responds to potential security breaches. It gathers security data from multiple sources, such as network traffic, system logs, user behaviour, and external threat intelligence feeds, enhancing overall cybersecurity defenses. The increasing volume of data sharing and network traffic has raised concerns about cybersecurity. To address this issue, we propose the Automatic Intrusion Detection System (AiDS) is defined as monitoring the network for suspicious activity for managing network traffic. The activities detected are monitored based on the alerts, and the operation centres are analyzed using the appropriate actions to remediate the threat. The Automatic intrusion Detection System and the Intrusion Prevention System (IPS) have been used to prevent and secure network data. By using the technique of Automatic intrusion Detection System (AiDS), the identification of the endpoint protection, which is related to the hunting engine, risk management, incident response mobile security, and access management and by using the technique of Intrusion Prevention System (AiPS) the vulnerability of threat management and the analysis of the data in the network is proposed. The result describes the 97.2% of data in the KDD 99 data set, the accuracy and sensitivity of the data from the network is 92.8%, and the system's formation. The approximate data in the database is 75%. The security services' intrusion and the system's data formation in the digital threat data have been accessed successfully.

Index Terms – Automated Intrusion Detection, Network Security, Risk Management, Endpoint Protection, Incident Response, Intrusion Prevention System, SOC-As-A Services, Vulnerability Threat Management, Mobile Security.

1. INTRODUCTION

In today's ever-evolving digital landscape, cyber security threats have become more sophisticated and prevalent, posing significant risks to organizations critical assets and data. Due to data sharing, the traffic in the network has increased, and the monitoring of the activity for network sharing has been proposed. The process of managing the communication in the network and the detection of the intrusion of the communication system [1] of long distance encourages the experimental research economically for maintaining the data in the network. The issues and the alerts for the suspicious activity discover the harmful activity, and this network manages the policy breaching for the data traffic [2]. The event management and the filtering technique have been done, and the suspicious and the issues which activate the filtering technique have also been done. The intrusion detection for monitoring the network traffic is monitored [3] [4] [5] [6]. The secure way of event management is done for various malicious activities [7]. The process of maintaining the network monitoring is proposed.

The information security theory permits the security policies of the information to be done [8]. This data security manages the limitation of storage, confidentiality, and accuracy has been proposed. This risk theory gives data security, enabling the breach consequence of the basic security proposed [1]. This security of the data, hardware, software and the organization for maintaining the procedure of the policies and the organization manages the policies and procedure for maintaining the procedures, and the organization has proceeded. The autoimmune process for progressing the weak and moderate sensory changes for respiratory failure is proposed. The security and the prevention of the system have been proposed using the intrusion and the prevention of the data. This identifies the threats and attacks in the network [8]. This reports the security operations center and the cyber security to analyze the network for trending analysis. This can be detected using the software, and the application of the

RESEARCH ARTICLE

policy violations has been proposed. The event management system has been instructed between the networks and the system. The traffic, threat data in the intrusion system, and buffer are suggested to ensure that the threat personnel data that assaults the networks are not there. It is done to find breaches. Electronic, physical, and skimming breaches are a few examples.

The threat management for responding to security incidents and the cybersecurity factor has proceeded [9]. In managing the prevention and security of the data in the network traffic, the data's loss and redundancy can be managed [10]. For detecting a threat, the configuration, modeling, indicator, behavioral analysis, and control system have been enabled for the environment data sharing. The organization of detecting and preventing cyber threats and data security is done using the Security Operation Center (SOC). Some components for managing the auditing standards and reporting this work in the performance actions. The harmful process for the compromised data for the recovery and the system for sharing and deleting files is proposed. The attacker reduction accuracy manages the surface, including the network and the devices for leaving the attackers and the attack based on the organization devices.

The primary objective of this research is to present a novel scheme for automated intrusion detection and prevention, ensuring data security and minimizing cyber threats in modern network environments. By integrating advanced techniques in the AiDS and AiPS model, we aim to provide a robust defense against malicious activities and enhance overall network security. The proposed AiDP model holds immense potential for various application areas, such as financial institutions, healthcare organizations, telecommunications networks, and critical infrastructure sectors. Implementing this model in these industries will bolster their cybersecurity measures, safeguard sensitive data, and protect against potential cyber-attacks. The main contribution of the study proposes as follows:

In Section 1, the introduction discusses the impact of increasing data sharing and network traffic on cybersecurity and presents the main objective of proposing the Automated Intrusion Detection and Prevention (AiDP) model. Section 2 provides a thorough literature review on automated intrusion detection and prevention. In Section 3, delves into the proposed Automatic Intrusion Detection System (AiDS) methodology is presented and discussed. Section 4 explains the Automatic Intrusion Prevention System (AiPS) and its components in detail. Section 5 serves as the results and analysis obtained from the discussion on theory-based security data. Finally, in Section 6, the paper concludes by summarizing the findings and discussing future work to be explored based on this study.

2. LITERATURE REVIEW

Singh et al. (2022) study describes the AutoML-ID for detecting the intrusion for the machine learning model that has been proposed using the wireless sensor network for the dramatic increase of synthetic data. The wireless sensor network manages the machine learning model to predict skillful automated machine learning for managing the data processing automation in the network. Also, the data's prevention and detection are done using the Bayesian optimization process. The machine learning model for performing similar fractions for detecting the intrusion is proposed by implementing this in the currently proposed system. Also, machine learning for maintaining the Gaussian process has been proposed. AutoML models are often more complex than manually crafted models. This complexity can make it difficult to interpret how the mode arrives at its decisions, leading to reduced explaining ability and transparency [3].

Echeberria et al. (2021) research enable the automated intrusion detection system for smart contracts for the decentralized scenarios for the blockchain facilities. The detection of the smart contract and automation of the potential threats for monitoring the blockchain has been proposed. The security based on the threats based on the smart contracts for the centralized and decentralized data is proposed. The automated approach and the potential threats to the development of the IDS are proposed. By implementing this in the currently proposed system, the automated IDS can be used in data management, and security can be proposed. Also, the blockchain-related factor for improving the transaction-based technology is done [4].

Saliu et al. (2022) manuscript manage the O-AIDS for managing the intelligent house surveillance security system for storing the data from the smart home appliances for the smart display. This is designed for the internet protocol camera, SMS notification, smart display, etc. The interface is related to the wide viewing angles for maintaining intelligent home applications. Here are angles that share the integrated factor data to show the system's maintenance for the microcontroller and the document's unit. By implementing this in the proposed system, intelligent home application data security can be analyzed and implemented. The systems performance become impractical as the volume of network traffic to handle large-scale environments. [11].

Hammar et al. (2021) study proposed the prevention of intrusion through optimal stopping can be proposed. Here for the prediction, reinforcement learning is proposed for problem stopping. This defender manages the dynamic program for feasible and practical cases for the dynamic programming and optimal defender policy measurements. By implementing this in the currently proposed system, the environment simulation for the simulation of the data is collected. Managing the data

RESEARCH ARTICLE

from the dynamic programming for the automatic system, automatic data analysis is predicted based on data sharing. [12].

Tripathi et al. (2022) manuscript study describes intrusion prevention based on the system availability and the proposed NPP of the factorization. The power generation of the cyber-attacks and the integration of the security of the data are done in this study. Also, the critical system of functionalities of the physical process of the Petri Net based on the cyber-attack is done. The understanding of the controlling parameter of the security of the data in the electric power manages the primary sources and the system's electric power is proposed. The availability of the system data is analyzed, and then the prediction of the data is made. By involving this method in the currently proposed system, the prediction of the data in the network based on availability can be found. [13].

Khan et al. (2022) study describe the security and the intrusion-based deep learning for the current analysis and the possible solutions proposed for the data. Deep learning is used for the analysis of the data and the security of the data using infrastructure is done. By involving this in the proposed the IoT. The balancing of the data is done based on precision, accuracy, and recall. This can be analyzed using smart homes, grids, and cities to develop data from smart homes and cities. The data classification is done using the automatic prediction of the data in the network. By involving this deep learning method in the currently proposed system, the data security from the smart cities is managed securely. [1].

Pani et al. (2021) study enables the feature selection of the data for intrusion deductions. The efficient algorithm for feature selection based on the internet of things is done. The flower pollination algorithm for intrusion detection has been proposed for the logistic regression and random forest for the smart cities and the high performance of the experimental factor for the FPA method. This method performs the logistics, and the classification of the literature survey and classification of the system is proposed. By implementing this in the currently proposed system, the data from the smart homes and smart cities are proposed by the IoT devices [14]. The overall summary of the literature review is shown in table 1.

Table 1 Summarization of Related Works

Author and Year	Proposed system	Method	Future Enhancement
Singh et al. (2022) [3]	In this study, AutoML-ID for intrusion detection using wireless sensor network	Bayesian optimization process	In the future, Enhancing data processing automation and handling synthetic data
Echeberria et al. (2021) [4]	Automated Intrusion Detection System	Automation of potential threat monitoring	Here the Improving transaction-based technology and centralized monitoring.
Saliu et al. (2022) [11]	In this manuscript, the OFFICE-AUTOMATED Intrusion Detection System (O-AIDS) are proposed.	Intelligent house surveillance security	Analyzing and implementing intelligent home application data security.
Hammar et al. (2021) [12]	In this study, Learning intrusion prevention policies through optimal stopping is done	Dynamic programming for defender policy	Simulation of data collection and prediction based on data sharing.
Tripathi et al. (2022) [13]	The intrusion prevention and response on cyber-physical system availability.	MCPs method and the game theory model.	Here the profitable management of the integration for the market buyers is done.
Khan et al. (2022) [1]	Deep Learning for Intrusion Detection and Security of Internet of Things (IoT)	Data classification using deep learning.	Secure data management from smart cities using deep learning.
Pani et al. (2021) [14]	IoT-based intrusion detection system	Flower pollination algorithm	Classification of data from smart homes and smart cities

International Journal of Computer Networks and Applications (IJCNA)
DOI: 10.22247/ijcna/2023/223316 Volume 10, Issue 4, July – August (2023)

RESEARCH ARTICLE

3. AUTOMATIC INTRUSION DETECTION SYSTEM (AiDS)

Intrusion in an unauthorized activity on the network thus can be managed by continuous automated monitoring and prevention. Thus, detecting the intrusion is monitoring an event that takes place in the network for the process of communication systems. The two or more systems are connected through a server for sharing resources or communication; thus, the systems in the network might be connected through a wired or wireless method [15]. To prevent network communication from a cyber-threat, a detection process is essential in finding the threat for protecting or preventing the system. An Automatic intrusion Detection System (AiDS) as shown in Figure 1 is used to find vulnerabilities or uncertain activity during an exchange of data or communication. These processes are automated by using software for detecting intrusions or threats. From Figure 1, the Automatic intrusion Detection System (AiDS) describes the network and other systems that are protected from cyber threats using IDS by placing an intrusion detector in a network and all the individual end-user devices.

To make intrusion effective, Unified Vulnerability Identity Management consists of five levels: Hunting Engine, Risk Management, Incident Response, Mobile and Cloud Security, and SOC-As-A-Service [16].

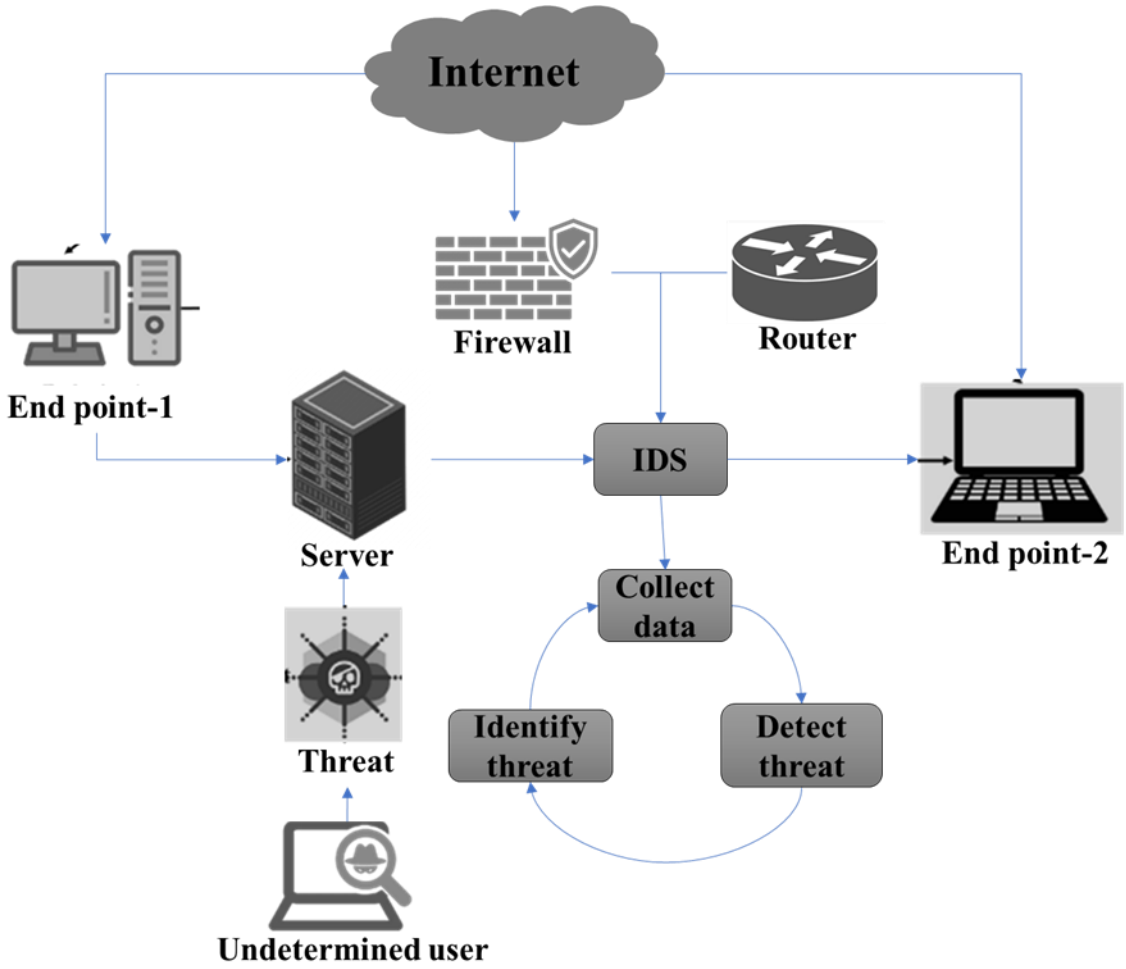

Figure 1 Process of Automatic Intrusion Detection System (AiDS) for Thread Detection

3.1. Hunting Engine

A hunting engine is an approach used to identify an unknown event or harmful threat to protect the network's endpoints. It might be WAN, LAN, or MAN. Each device connected to the network is known as an endpoint; the various endpoints are sensors, mobiles, servers, databases, and so on. The critical security threat in a network is that every endpoint in the network can share its resources, access the data, and also communicate with each other thus hunting engine is used to

RESEARCH ARTICLE

protect each end user from cyber or unknown attacks in the network by detecting malicious activities in the network [17]. The hunting engine detects the threat by continuously monitoring the cyber-attacks on the network and identifying the presence of the threat by comparing the pre-designed conditions with the current events. The condition is designed to detect whether the end user conducts normal network activities, like transmitting, receiving, and searching, or undetermined access to data transmitted by the endpoints by duplicating the data, altering data, and finding the IP from where the data are transmitted and so on. If any threat in the network is detected, they are identified using a hunting engine to rectify the threat.

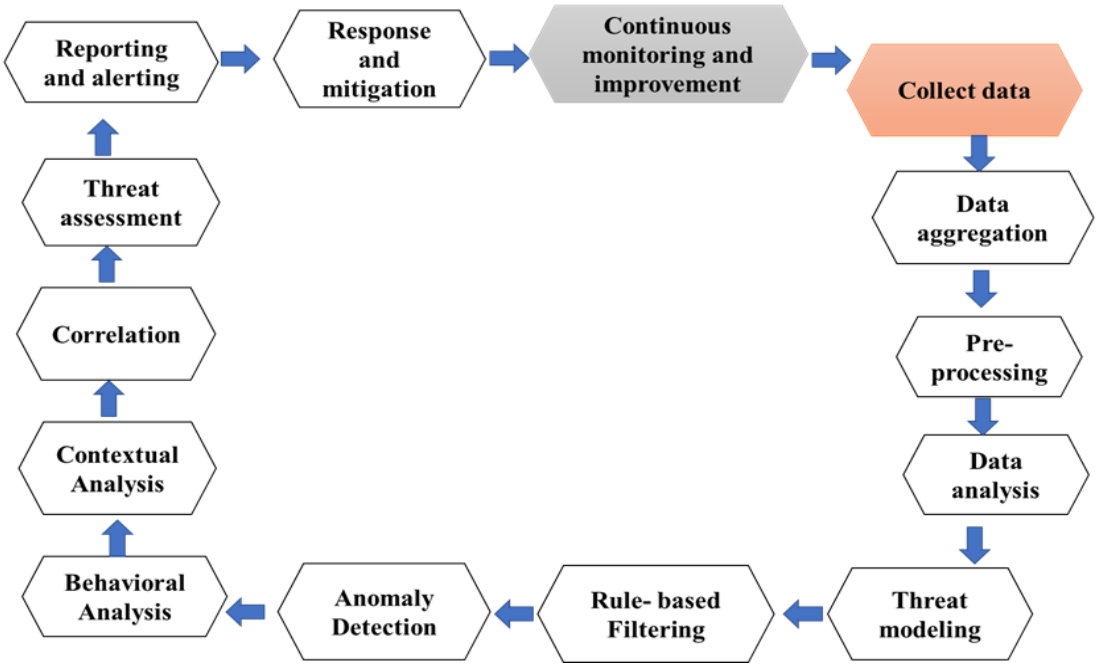

Figure 2 Process Cycle of Identifying Threat

This process of threat identification is a forward approach in which the hunting engine searches for risk in the network. The destination of the hunting engine is every activity and traffic for each second. It compares it with the conditions to find the threat in the network [18]. A threat or attack is a systematic approach to getting uncertain access to the system or network; thus, this threat can be identified using the hunting engine by extracting all the communication details from the network. It is analyzed with the conditions [19]. Thus, after analyzing the data, a continuous monitoring process is applied to identify an actual threat in the network as shown in Figure 2.

3.2. Risk Management

Risk management is finding security risks in the network caused by a cyber-threat. The risk is identified by determining the threats which cause vulnerability to the endpoints. A comprehensive strategy is applied for risk management using the basic 5 levels. The risk determines potential loss or damage in the network risk because of the threat [20]. Thus the risk generated by the threat is managed using a risk management method that contains different steps like risk identification, analysis, prioritization, treatment, and monitoring of risk as shown in Figure 3.

3.2.1. Risk Identification

The initial stage of the risk management process involves identifying and comprehending potential risks stemming from various threats. It involves identifying and classifying the roots of risk to know how and which risk should be managed to avoid risk in the network. One of the standard ways for risk identification is by reviewing previous network histories like a type of cyber threat and its effects using the method of the information collection process [21].

3.2.2. Risk Analysis

It is the process of evaluating the risk that negatively impacts the network during the communication process. The process of analysis occurs after the identification of the risk. Thus evaluation of risk helps avoid those risks from the network by understanding how the outcome of communication and objective gets affected due to the impact of risk on the network events [22].

RESEARCH ARTICLE

3.2.3. Prioritization of Risk

It is the process of identifying all potential threats within the network and evaluating which threat is the most severe so that they can be solved at the beginning. The way of prioritizing the risk is based on the likelihood of the risk and its potential impact on the process. Hence, the ranking order is from most critical to least critical threat [7]. The objective of ranking is to form a basis for resource allocation.

3.2.4. Treating an Identified Risk

It is based on the ranking order for reducing or removing the risk from the network. It is an essential process for the network to prevent communication events from risk. In this stage, the strategy of risk mitigation, prevention, and contingency plans was generated based on evaluated values of risk [23].

3.2.5. Risk Monitoring

It is the process of identifying whether the evaluated risk has been reduced effectively and finding whether the treatment used to reduce the risk is effective; otherwise, alternative treatments should be chosen to reduce the risk further. Thus, monitoring risk also helps track and evaluate risk management systems' effectiveness.

The unified Vulnerability Identity Management includes different levels for making an Automatic intrusion Detection System (AiDS), such as hunting engine, risk management, incident response, and mobile and cloud security. Algorithm 1 shows the process of hunting engine. It is used to detect the harm threat or any unauthorized activity in the network. Various types of devices are connected through a network called endpoints. Hunting engines protect each endpoint from cyber-attacks by detecting malicious activities in the network. Each endpoint can share its data and resources, access the data, and communicate with each other in the network, so security is essential for making the above-stated process. The hunting engine detects the threat by continuously monitoring the cyber-attacks on the network. It can identify the presence of a threat when comparing the pre-designed conditions with the current events when the undetermined access to data transmitted by the endpoints by duplicating the data, altering data, finding IP from the data transmitted, and so on are identified as malicious activities.

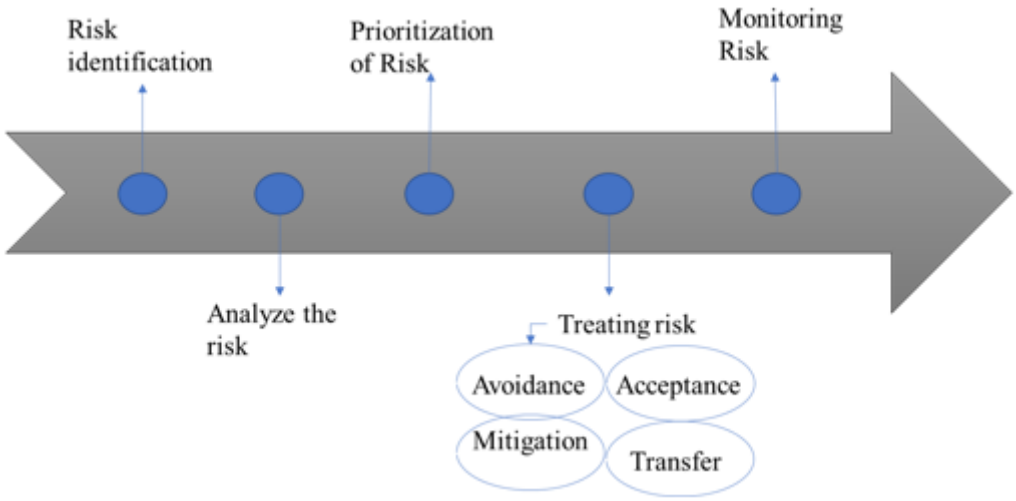

Figure 3 Steps for Risk Management

Input data; endpoint node set E, E_k -normal endpoint with relation set RS= {data storing, data sharing, data access}, unknown activities= {data duplication, altering data, finding IP}

while communicating ()

repeat

perform hunting engine Ht

do monitoring

for each endpoint E

if (E performs unknown activities) then

E performs malicious activities

else

for each endpoint Ek

evaluate SIM (E, Ek)

if (SIM (E, Ek) =1)

RESEARCH ARTICLE

E performs normal activities

end if

until

end if

end for

end repeat

end

Algorithm 1 LEVEL1: The Process of Hunting Engine

When the endpoints or end user conducts normal activities like transmitting, receiving, and searching, the endpoints are identified as regular activities.

Risk management is finding security risks in the network caused by a cyber-threat. The risk is identified by determining the threats which cause vulnerability to the endpoints [24]. Each endpoint has a unique device ID authorized for accessing the data. Initially, each endpoint is needed to check whether it is authorized. The system provides access when the user id, unique endpoint id, is genuine.

Initialize: endpoint device id- EID

value = authorization (var EID)

if (value = authorized)

log(value)= log in (var EID, var IP address, var login id)

if log (value) true

allow access to E

else if (value = un-authorized)

block (Value)= prevent system

end if

end if

if (block (Value)) true

send(alert)= alerting (log(value))

if (send(alert) AND log(value)) false

append alert in a local file

else

var((log(value))) = alert (var EID, var IP address, var login id)

end if

end if

Algorithm 2 LEVEL 2: Endpoint Protection & Risk Management

When the above details are false, as shown in the algorithm 2, the system restrictor blocks the access. The alert is sent to an endpoint id whenever the system blocks the access. Otherwise, the alert is appended to a local file.

3.3. Incident Response

Incident response is the collection of information security policies and procedures used for identifying, evaluating, and responding to incidents of potential risk caused by reduced threats and help in faster recovery [25]. It is also one of the essential components. When risk management neglects to reduce the risk, incident response is activated to handle the risk. The objective of incident response is mentioned in Figure.4.

Figure 4 illustrates the Incident Response process, which involves a series of well-defined steps. These steps include preparation, detection, analysis, contamination containment, eradication of threats, recovery, and post-incident assessment. Each phase plays a crucial role in efficiently and effectively responding to security incidents, minimizing potential damages, and restoring normal operations following an incident. An incident represents a process that occurs in a network because of a malicious attack or threat [26]. The incident response is used to manage the risk caused by the threat. The incident response process comprises several distinct phases, as highlighted in Figure 4. These phases include preparation, detection and analysis, containment, eradication, recovery, and post-incident activities.

Each stage is essential in effectively addressing security incidents, ensuring the containment of threats, and facilitating a comprehensive recovery process. By following this structured approach, organizations can enhance their ability to respond to incidents promptly and mitigate potential damages. The Preparation phase involves the proactive efforts made by a network to get ready for incident response. This includes setting up the necessary tools and resources and providing appropriate training to the response team. Additionally, this phase encompasses activities aimed at preventing incidents from occurring in the first place. By taking these preparatory measures, organizations can enhance their readiness to handle security incidents effectively and minimize potential risks.

An effective incident response begins before an actual detection of any incident. The time a network spends preparing and planning before an incident can minimize the impact and exposure during an incident. The goal of the preparation stage is to ensure that the network can comprehensively respond to an incident when detected [8].

Detection involves collecting data from the network's history, then identifying precursors for finding the signs that an incident may happen in the future, and indicators are used for whether the data shows the presence of a threat determines whether an attack has happened or is happening at present.

RESEARCH ARTICLE

The primary purposes of this detection and analysis phase are to determine whether the incident is indeed occurring and to analyze its nature. The analysis involves identifying a baseline or ordinary activity for the affected systems, correlating related events, and finding when and how they deviate from normal behavior [27].

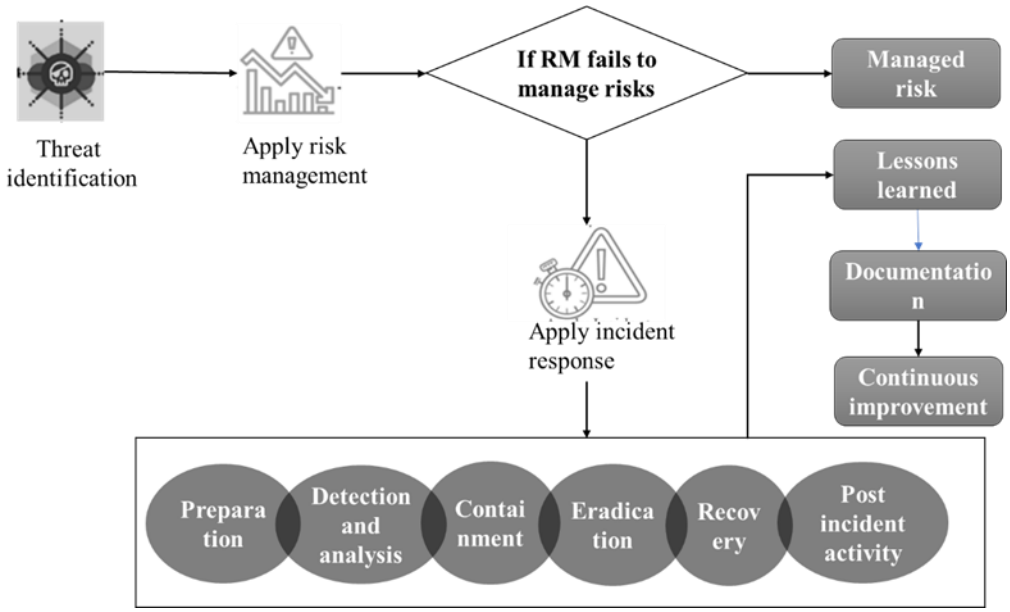

Figure 4 Process Flow of Incident Response

Contamination is an action that is required to prevent the incident or event from spreading across the network.

The eradication is an action that is required to wipe the threat from the network or system entirely.

Recovery is an action that is required to bring back the network or system to its former functionality and use.

In the post-incident phase, the incident information is thoroughly reviewed from the time of occurrence to its closure. This process involves a comprehensive examination of the incident, aiming to identify potential findings and areas where the incident response could have been improved.

The outcome of this review is a detailed report that highlights lessons learned and suggests better approaches for handling similar incidents in the future. The post-incident analysis plays a crucial role in enhancing the incident response capabilities of an organization and fostering continuous improvement in its security practices.

The incident response is performed only the device security experiences some attacks. Each device has an incident response preparedness for dealing with the data breach. Initially, we need to prepare for the incident response planning, then identify or detect whether the everyday operations and activities have breached the device [10]. When we identify and know the breaches, we want to fix them immediately. The forensic investigation method plays a vital role in identifying critical details about a breach. It involves a meticulous examination to determine the specifics of the breach, including how and when it occurred, the nature of the breach, and the origin of the security compromise.

Input: C_d - collected data

Initially, $C_d = \phi$

while stopping criteria is not met, do

for each system

perform risk assessment

recon-fig(data)= remove. data vulnerability

Check for threat

if (identify== breach)

if (detect== network attacks)

determine attacks type

determine attacks source

set up = system (Incident Response)

if (incident==containing)

eliminate = remove(threat)

if (found==malware traces)

remains = alert (system)

RESEARCH ARTICLE

end if

end if

end if

end if

recover= restore (data in device)

store events

end for

end while

Algorithm 3 LEVEL 3: Incident Response

Recovering from a data breach is restoring and returning affected devices. After the incident, find and eliminate data that led to the breach. This process removes all device malware, which should be patched and updated. In the device, if any trace of malware or security issues is present, the system reminds you of your devices [28] as shown in the algorithm 3. After the forensic investigation, all incident response is stored for preparing for the subsequent attacks.

4. AUTOMATIC INTRUSION PREVENTION SYSTEM (AiPS)

An intrusion prevention system (IPS) is a fundamental tool in network security that plays a vital role in thwarting malicious activities. It actively responds to potential threats by promptly identifying and taking necessary actions, such as reporting the detected activities or implementing blocks to prevent their progress.

In addition to its real-time actions, IPS maintains detailed records of observed events, ensuring a comprehensive understanding of network security incidents. It also provides notifications to security administrators about significant events and generates comprehensive reports to aid in analysing and responding to security incidents effectively. IPS is an essential asset in safeguarding networks and enhancing the organization's overall security posture.

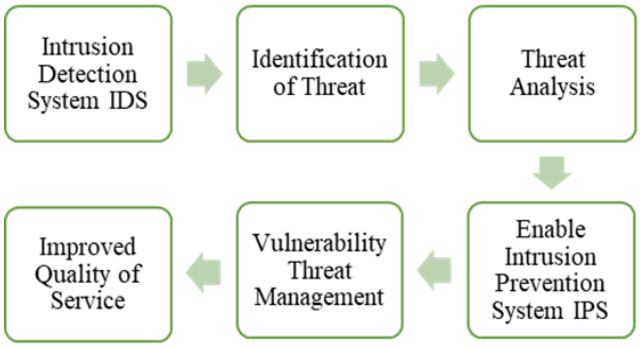

Figure 5 Process of Automatic Intrusion Prevention System (AiPS) for Data Prevention

Numerous intrusion prevention systems (IPS) have the capability to respond to identified threats by proactively preventing their successful execution [29]. These IPS employ diverse response techniques, such as directly halting the attack, modifying the security environment, or altering the content of the attack. In the context of the proposed system, the Vulnerability Threat Management process incorporates the utilization of Security-as-a-Service and SOC-as-a-Service, as illustrated in Figure 5. This integrated approach enhances the network's resilience against threats, enabling a robust security management solution that leverages external security services and a Security Operations Center (SOC).

4.1. Security-as-a-Service

Security as a service (SECaaS) is an outsourced service that helps handle and manage a network's security. The system's security is provided by continuous monitoring for finding the security issues caused by the cyber threat using the intrusion detection method (IDS). When the security issues in the network are detected using IDS, an IPS system enabled with Security-as-a-Service is triggered to protect the network by providing control over the access. Access control is a critical data security process that empowers the system to regulate and manage authorized access to corporate data and resources [30]. Implementing secure access control involves the establishment of robust policies that validate the identity of users, ensuring that they are indeed who they claim to be. Security-as-a-Service plays a pivotal role in enabling and enforcing secure access control mechanisms, providing organizations with an efficient and scalable approach to safeguarding their valuable data and resources as shown in algorithm 4. This system plays a crucial role in providing authentication to the authorized servers within the network, ensuring secure access to the communication process. Access control mechanisms are implemented to regulate data access by end users, ensuring data security during communication. Administrators can control access by authorizing users with specific access levels to doors connected to the required reader and controller [31]. This authorization can be easily managed through a secure database containing user credentials stored in the cloud. Authentication is a critical process used to verify the identity of users seeking access to the system. Access control is typically based on the authenticated user's identity, making authentication vital for ensuring adequate security [32]. Effective access control management is essential for controlling threats and preventing unauthorized access by limiting access only where necessary. This improves data security, enhances service availability, and enables efficient communication with reduced latency, leading to improved quality-of-service (QoS). An intrusion prevention system (IPS) is a component of Automatic Intrusion Prevention System (AiPS) network security designed to proactively prevent identified threats. IPS continuously monitors the network, detecting potential malicious incidents (MI) and gathering valuable information

RESEARCH ARTICLE

about them [32] [33]. By promptly responding to detected threats, IPS plays a critical role in maintaining network security and safeguarding against potential intrusions.

During the data transmission, the endpoints are in intrusion prevention mode either by blocking the network traffic or neglecting the data in case of intrusion, thus preventing the malicious data from reaching the destination [34]. The endpoint can be configured for reset connection, firewall reconfiguration, or traffic block as a countermeasure, such as blocking the traffic as soon as they detect any intrusions by mediating the traffic flow [13].

Begin

while data transmission

do continuous monitoring

if (detect= P(MI))

extracts info (MI)

block malicious activities

else

continuous monitoring

end if

end while

end

Algorithm 4 Result with Intrusion Prevention System for Process 1: Security-as-a-Service

4.2. SOC-as-a-Service

A Security Operations Center (SOC) is an essential security model dedicated to managing and safeguarding networks against cyber-attacks. It operates by continuously monitoring various components, including networks, servers, computers, endpoint devices, operating systems, applications, and databases, to detect any indications of potential cyber threats. The SOC plays a proactive role in identifying and responding to security incidents, ensuring a robust defense against cyber adversaries and enhancing the overall security posture of the organization. A Security Operation Center (SOC) is a centralized unit that contains processes and technologies to provide network security. In this operation center, the extracted threats are analyzed after identifying the threat using IDS to find the exact solution for solving the threat to increase the network performance [35].

5. THE RESULT FROM THE DISCUSSION WITH THEORY-BASED SECURITY DATA ANALYSIS

We proposed a system named Automated Intrusion Detection and Prevention (AiDP) model for analyzing the Theory-based Security Data and Analytics Solution. In an intrusion detection phase, various individual endpoint-related data are collected over the network. However, the various endpoints are sensors, mobiles, servers, databases, etc.

The IDS for intelligent contracts (IDS-SC) Echeberria et al. (2021) [4] and the CRÈME (Configuration, REproduction, Multi-dataset, and Evaluation) Bui et al. (2021) [6] are compared with the proposed Automated intrusion detection and prevention (AiDP) model for displaying the various quality factors against Automated intrusion detection and prevention (AiDP) model. The performance of our proposed method is measured using the above characteristics [9].

- True Positive (TP) represents the number of endpoints correctly classified as malicious.
- True Negative (TN) indicates the number of endpoints accurately identified as usual (non-malicious).
- False Positive (FP) shows the number of endpoints wrongly classified as malicious when they are standard endpoints.
- False Negative (FN) represents the number of endpoints mistakenly labelled as standard (non-malicious) when they are actually malicious.

The system evaluation using standard metrics is shown in table 2.

Table 2 Confusion Matrix for Actual Threat Data

Actual Class	Normal endpoint As output	Intrusion Endpoint As Output
Normal Endpoint As Input	TRUE NEGATIVE (TN)	FALSE POSITIVE (FP)
Intrusion Endpoint As Input	FALSE NEGATIVE (FN)	TRUE POSITIVE (TP)

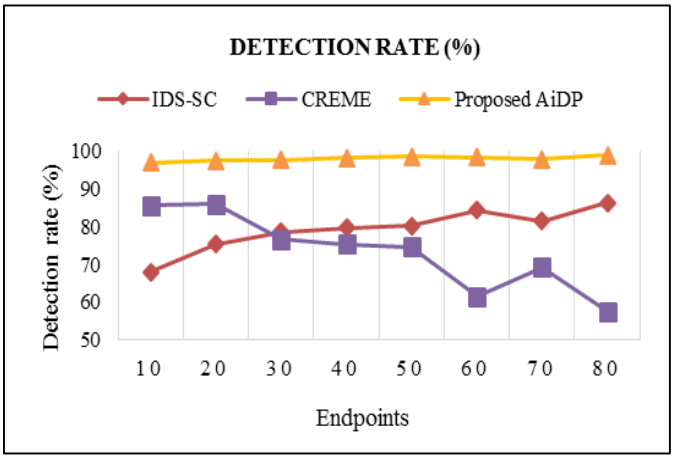

Figure 6 Detection Rate with Endpoints Analysis

RESEARCH ARTICLE

In evaluating our system, we measure three key metrics: network accuracy, intrusion detection rate (DR), and false positive rate (FPR). The intrusion detection rate (DR) specifically measures the system's ability to correctly detect intrusions out of all the actual intrusions present in the dataset. , and it is mathematically expressed in equation (1) as

$$\text{Detection Rate} = \frac{True\ Positive}{False\ Negative + True\ Positive} \quad (1)$$

Figure 6 represents the intrusion detection rate of the proposed AiDP system with an increasing count of endpoints. The line in figure 6 clearly shows that the proposed system has higher detection accuracy in detecting cyber threats. From the result, the proposed system has a better detection rate in terms of percentage.

The false positive rate (FPR) is the proportion of non-intrusive events that are incorrectly classified as intrusions by the system.

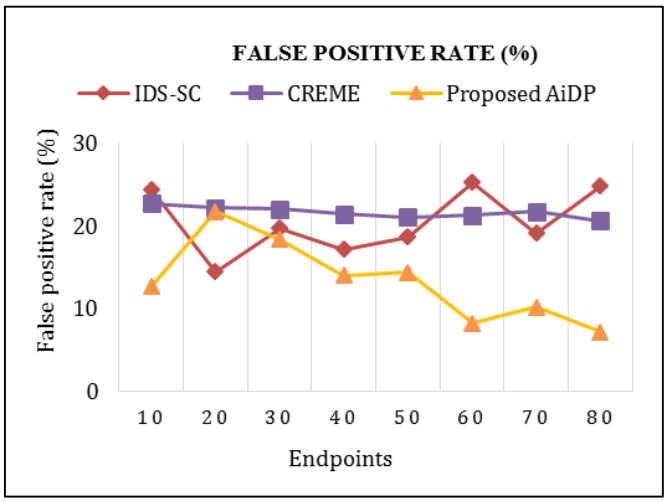

Figure 7 False Positive Rate with Endpoints

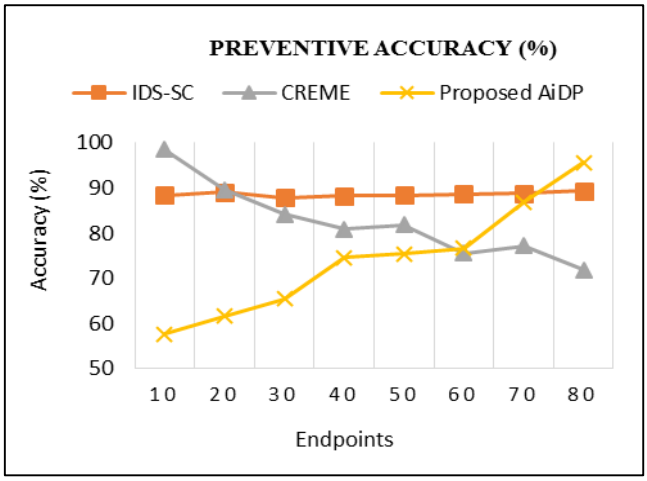

Figure 8 Accuracy Analysis Based on Increasing Count of Endpoints

Figure 7 depicts the false positive rate at different count of endpoints. The X-axis denotes the increasing count of endpoints, while the Y-axis refers the false positive rate in percentage. Figure 7 shows that the false positive rate is reduced with the increasing count of endpoints. The curves measure the False Positive Rate (FPR) as expressed mathematically as follows in equation (2).

$$FPR = \frac{False\ Positive}{True\ Negative + False\ Positive} \quad (2)$$

Figure 8 shows the increasing number of endpoints, and the accuracy of the proposed AiDP system increases. So, for a count of endpoints of 80, it provides the maximum accuracy of 95.67%. The standard metrics for the system performance is shown table 3.

Standard metrics have been extensively employed to evaluate the effectiveness and performance of network intrusion detection systems. The standard metrics are packet delivery ratio, average delay, average detection ratio, and average false alarm rate.

The average delay is a crucial metric used to measure the time taken on average, for the transmission of the first data packet from the sender node to the reception of the last data packet at the receiver node within the network. In this study, we have conducted evaluations for various network sizes, ranging from 10 to 80 nodes. The calculated average delay values for both the existing method and the proposed method are presented in table 4.

The network attack or cyber threat may be in the form of data snooping, modification, masquerading ad, denial of service, data loss, data duplication, etc. Average Detection Rate and Average False Alarm Rate are the two most famous metrics that have already been used.

The detection rate is a fundamental metric that measures the effectiveness of our cyber-threat detection system. It is calculated as the ratio of accurately detected cyber-threats to the total count of cyber threats in the dataset. The corresponding detection rate values for both tables 3 and 4 are provided.

Figure 9 illustrates the Packet Delivery Ratio (PDR) for different types of attacks. PDR represents the ratio of data packets successfully delivered to recipient nodes within secure zones to the total packets transmitted from the source node. The proposed AiDP method demonstrates significantly higher PDR, highlighting its effectiveness in Intrusion Detection and Prevention. SVM shows a lower PDR than the other two methods, while ZBIDS has a higher PDR than SVM but lower than AiDP. These findings provide valuable insights into each method's performance under various attack scenarios, aiding in network optimization and security decision-making.

RESEARCH ARTICLE

Table 3 Performance Metrics Analysis of Detection Rate, False Positive Rate, and Accuracy Comparison

Endpoints Node count	Detection Rate (%)			False Positive Rate (%)			Accuracy (%)		
	IDS-SC	CREME	Proposed AiDP	IDS-SC	CREME	Proposed AiDP	IDS-SC	CREME	Proposed AiDP
10	67.98	85.6	96.82	24.47	22.74	12.67	88.46	98.53	57.68
20	75.36	85.97	97.35	14.5	22.21	21.74	89.12	89.59	61.59
30	78.65	76.58	97.51	19.74	22.05	18.37	87.84	84.16	65.36
40	79.642	75.434	98.12	17.144	21.44	14.02	88.26	80.838	74.64
50	80.256	74.642	98.47	18.662	21.09	14.4	88.47	81.774	75.43
60	84.3665	61.5905	98.23	25.263	21.33	8.19	88.7	75.5535	76.58
70	81.356	69.302	97.79	19.132	21.77	10.21	88.81	77.244	86.91
80	86.35	57.68	98.91	24.87	20.65	7.2	89.34	71.89	94.03

Table 4 Performance Metrics Analysis of Packet Delivery Ratio, Average Delay, Average Detection Rate, and Average False Alarm Rate with Various Cyber Attack

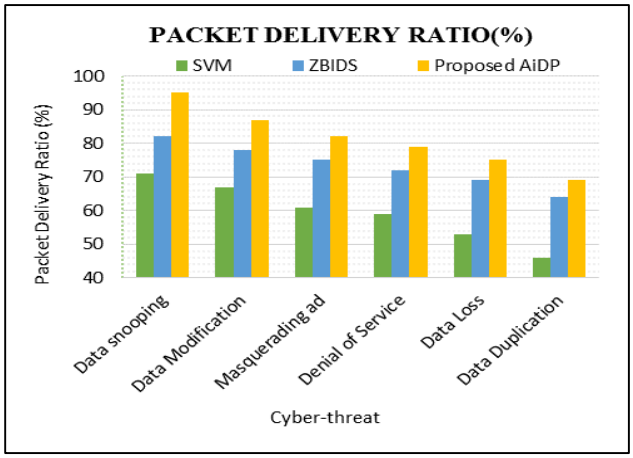

Figure 9 Packet Delivery Ratio Analysis with Various Types of Cyber Attack

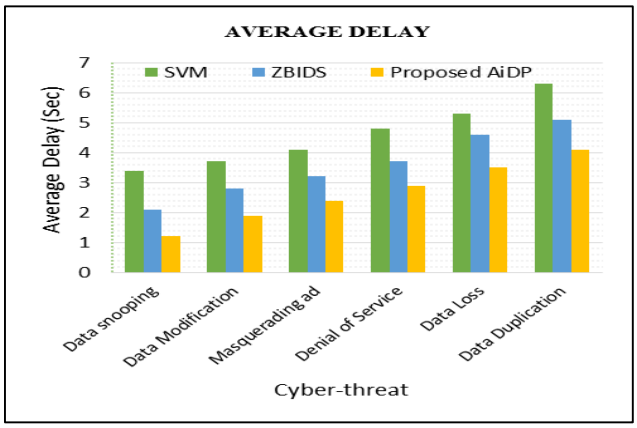

Figure 10 Average Delay Analysis with Various Types of Cyber Attacks

Figure 10 shows the average delay of various cyber-attacks such as data snooping, data modification, masquerading ad, denial of service, data loss, and data duplication. From the graph, it is evident that the average delay of the proposed method is significantly lower compared to the SVM and ZBIDS methods. Due to the proposed method's higher successful packet delivery ratio, the proposed method's average delay is lesser than the existing methods.

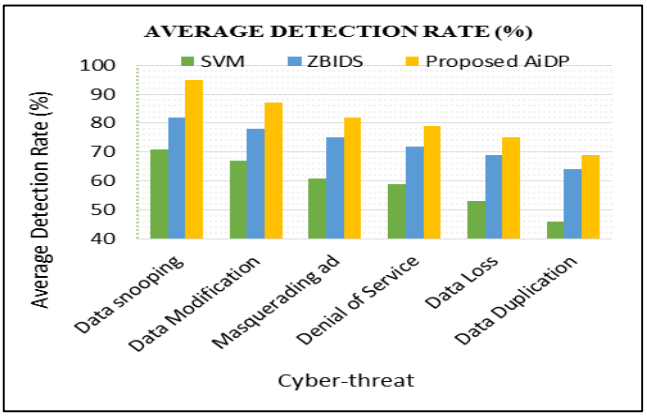

Figure 11 The Analysis of the Average Detection Rate Across Various Types of Cyber Attacks

Figure 11 depicts that the average detection rate of the proposed AiDP method and existing methods for all cyber-attack possibilities. Due to the cyber-attacks and traffics in the network, the proposed method has a lesser detection rate for single cyber-attacks and the highest detection rate for multiple cyber-attacks. The average detection rate is expressed in equation (3) as follows,

$$\text{Detection Rate} = \frac{correctly\ detected\ threat\ count}{total\ no.of\ threat} \quad (3)$$

RESEARCH ARTICLE

Table 4 Performance Metrics Analysis of Packet Delivery Ratio, Average Delay, Average Detection Rate, and Average False Alarm Rate with Various Cyber Attack

Cyber-threat	Packet Delivery Ratio			Average Delay			Average Detection Rate (%)			Average False Alarm Rate (%)		
	SVM	ZBIDS	Proposed AiDP	SVM	ZBIDS	Proposed AiDP	SVM	ZBIDS	Proposed AiDP	SVM	ZBIDS	Proposed AiDP
Data snooping	71	82	95	3.4	2.1	1.2	62	40	76	11.85	22.87	8.97
Data Modification	67	78	87	3.7	2.8	1.9	70	22	93	12.65	21.07	10.67
Masquerading ad	61	75	82	4.1	3.2	2.4	71	53	87	12.75	24.17	7.07
Denial of Service	59	72	79	4.8	3.7	2.9	92	90	94	16.05	28.87	9.77
Data Loss	53	69	75	5.3	4.6	3.5	88	89	93	14.45	27.77	7.67
Data Duplication	46	64	69	6.3	5.1	4.1	84	88	92	14.05	29.97	8.57

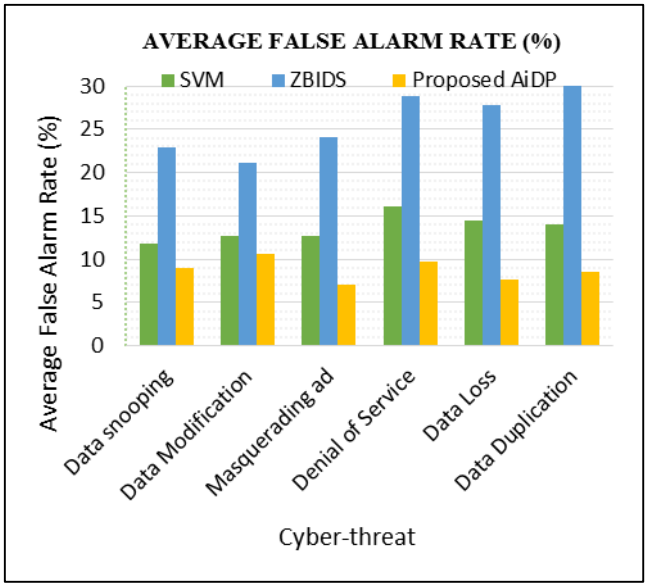

Figure 12 Average False Alarm Rate Analysis with Various Types of Cyber Attacks

The average False Alarm Rate (FAR) is calculated as the ratio of endpoints incorrectly classified as malicious to the total number of actual non-malicious instances. The corresponding Figure 12 presents the assessment of the false alarm rate, comparing our proposed AiDP method to other existing methods. According to the results depicted in Figure 12, our proposed AiDP method demonstrates superior performance compared to the other existing methods in terms of reducing false alarms. According to figure 12, our proposed AiDP method outperforms the other existing method. The false alarm rate eqn (4) is computed as,

$$FAR = \frac{false\ negative}{false\ negative + true\ positive} \quad (4)$$

The Average false alarm rate metric is calculated that shown in eqn 5, it defines the ratio among the count of standard connections that are wrongly misclassified as a cyber-threat and the total count of standard connections that is,

$$\text{Average False alarm rate} = \frac{false\ positive}{total\ no.of\ standard\ connections} \quad (5)$$

Table 5 Attacker Reduction Accuracy Analysis with Various Methods

Methods	Attacker Reduction Accuracy (%)	
	Intrusion Detection	Intrusion Prevention
SVM	75.31	76.42
ZBIDS	78.62	77.53
Proposed AiDP	92.45	95.61

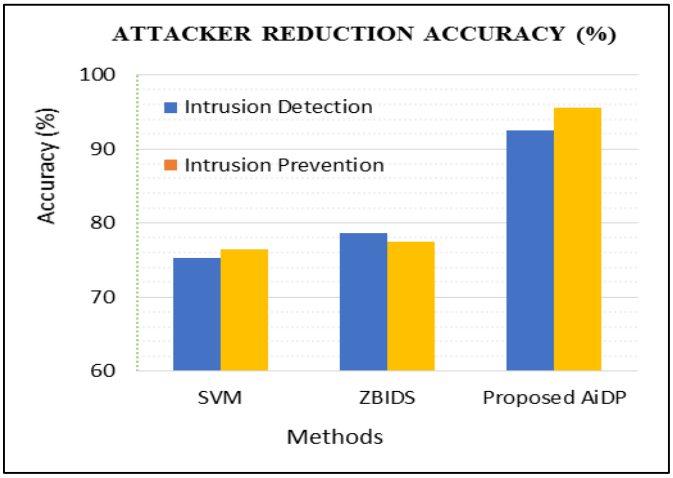

Figure 13 Attacker's Reduction Accuracy Analysis with Existing Methods

RESEARCH ARTICLE

From Figure 13, presents, as for cyber-attacks, all of the success packet delivery rate, average delay, and average false alarm rate of the proposed method.

The unified vulnerability identity management includes five levels: hunting engine, risk management, incidence response, and data security process for identifying the cyber threat [36]. The hunting engine is used to encounter a harmful event or threat over the network.

The risk management system determines the risks caused by the threats. Incident response is used for performing the identification of threats and evaluating their threat. Mobile and cloud data security is used to protect the data stored on the devices, as shown in Table 5.

Figure 13 demonstrates the attacker's reduction accuracy of various methods like SVM, ZBIDS, and the proposed AiDP method. From the above graph, the SVM method has attackers' reduced accuracy of 75.31% and 76.42% for the intrusion detection and prevention process, respectively. The ZBIDS method has attackers' reduction accuracy of 78.62% and 77.53% for the intrusion detection and intrusion prevention process, respectively. The proposed AiDP method has attackers' reduction accuracy of 92.45% and 95.61% for the intrusion detection and intrusion prevention process, respectively.

From the above result, the proposed AiDP method has higher attacker reduction accuracy in intrusion detection and intrusion prevention methods than the other methods. Analysis of the performance of our system with two conditions: In the network, authorized users have the capability to request data anonymously while ensuring their authenticity through valid signatures.

This approach enables them to securely access the data they are entitled to, maintaining data integrity and confidentiality. On the contrary, malicious users attempt to gain unauthorized access to data by submitting requests with invalid signatures. These illegitimate requests aim to exploit vulnerabilities and potentially disrupt the network's operations through a Denial-of-Service (DoS) attack on the data.

The proposed Automated Intrusion Detection and Prevention (AiDP) model demonstrates outstanding performance in enhancing cybersecurity, as supported by the following numerical values. AiDP achieves detection rates ranging from 67.98% to 98.91%, this highlights AiDP's superior ability to accurately detect cyber threats. AiDP exhibits a low false positive rate of 7.2% to 25.263%, outperforming that indicates fewer instances of misclassifying normal connections as threats.

AiDP's accuracy reaches up to 95.67%, and it achieves an average detection rate of 76.589%. AiDP maintains a low average false alarm rate of 8.057%, demonstrating its ability to minimize false alarms and reduce unnecessary alerts and it exhibits a high packet delivery ratio and it achieves attacker reduction accuracy of detection and prevention of 92.45% and 95.61%, respectively, it shows ability to effectively reduce malicious attacks.

Overall, the proposed AiDP model offers superior performance in detecting and preventing cyber threats, ensuring robust network security and safeguarding against unauthorized intrusions. These numerical values validate the effectiveness and efficiency of AiDP, making it a promising solution for enhancing cybersecurity in various network environments.

6. CONCLUSION

This research centered on the Automated Intrusion Detection and Prevention (AiDP) model, analyzing Theory-based Security Data and Analytics solutions through Intrusion Detection Systems and Intrusion Prevention System. The study also incorporated Security-as-a-Service and SOC-as-a-Service Techniques to enhance Cybersecurity with the proposed Theory-based intrusion detection and prevention approach. The Intrusion Detection System employs Unified Vulnerability Identity Management, encompassing Endpoint Protection & Hunting Engine, Risk Management, Endpoint Security, Incident Response, and Cloud & Mobile Security. This comprehensive approach fortifies network security, detects and prevents intrusions, and improves overall cybersecurity defences. However, the Vulnerability Scanning and Threat Assessment are made using Data Breach Verification. On the other hand, the Intrusion Prevention systems are employed for Vulnerability Threat Management using Security-as-a-Service and SOC-as-a-Service. This helps prevent the Application of Data Security and Analytics by using the Global Risk Management Security Solutions. The final analysis of intrusion detection and prevention (AiDP), Data, and Analytics is made by accessing the Unified Vulnerability Identity Management and Security-as-a-Service Algorithms.

As the simulated Results of Security-as-a-Service Attacker Reduction Percentile return 97.56%, at the Level of Intrusion Detection System, it's become 97.84% and in Level of Intrusion Prevention System return the 96.34%. Although the Moving signals data becomes 54% and Attacker Reduction Accuracy is 95.43% on Phase 1 Step 1. Moreover, the Attacker Reduction Accuracy is 97.33% in Phase 1 Step 2. Finally, the Attacker Reduction Accuracy is 98.84% in Phase 2, Step 3. The result closed with Intrusion Prevention System for Security-as-a-Service and SOC-as-a-Service against the Vulnerability Scanning and Threat Assessment for reducing the attacks on the average vulnerability data and digital threat data. Future work for this paper involves enhancing detection accuracy using advanced techniques, developing real-time intrusion prevention mechanisms, and addressing zero-day attacks while maintaining privacy and ethical considerations.

RESEARCH ARTICLE

REFERENCES

[1] Khan, A. R., Kashif, M., Jhaveri, R. H., Raut, R., Saba, T., & Bahaj, S. A. (2022). Deep Learning for Intrusion Detection and Security of Internet of Things (IoT): Current Analysis, Challenges, and Possible Solutions. Security and Communication Networks, 2022.

[2] Hyde, P., Ulianov, C., Liu, J., Banic, M., Simonovic, M., & Ristic-Durrant, D. (2022). Use cases for obstacle detection and track intrusion detection systems in the context of new generation of railway traffic management systems. Proceedings of the Institution of Mechanical Engineers, Part F: Journal of Rail and Rapid Transit, 236(2), 149-158.

[3] Singh, A., Amutha, J., Nagar, J., Sharma, S., & Lee, C. C. (2022). AutoML-ID: automated machine learning model for intrusion detection using wireless sensor network. *Scientific Reports*, *12*(1), 1-14.

[4] Echeberria-Barrio, X., Zola, F., Segurola-Gil, L., & Orduna-Urrutia, R. (2021, September). SmartWarden: Automated Intrusion Detection System for Smart Contracts. In 2021 3rd Conference on Blockchain Research & Applications for Innovative Networks and Services (BRAINS) (pp. 51-52). IEEE.

[5] Pasikhani, A. M., Clark, J. A., Gope, P., & Alshahrani, A. (2021). Intrusion detection systems in RPL-based 6LoWPAN: a systematic literature review. IEEE Sensors Journal, 21(11), 12940-12968.

[6] Bui, H. K., Lin, Y. D., Hwang, R. H., Lin, P. C., Nguyen, V. L., & Lai, Y. C. (2021). CREME: A toolchain of automatic dataset collection for machine learning in intrusion detection. 193, 103212.

[7] M. Aljabri et al., "Detecting Malicious URLs Using Machine Learning Techniques: Review and Research Directions," in IEEE Access, vol. 10, pp. 121395-121417, 2022,doi:10.1109/ACCESS.2022. 3222307.

[8] Hughes, K., McLaughlin, K., & Sezer, S. (2021, July). Towards Intrusion Response Intel. In 2021 IEEE International Conference on Cyber Security and Resilience (CSR) (pp. 337-342). IEEE.

[9] J. Lee, J. Kim, I. Kim and K. Han, "Cyber Threat Detection Based on Artificial Neural Networks Using Event Profiles," in IEEE Access, vol. 7, pp. 165607-165626, 2019. doi: 10.1109/ACCESS.2019.2953095

[10] P. A. Legg, O. Buckley, M. Goldsmith and S. Creese, "Automated Insider Threat Detection System Using User and Role-Based Profile Assessment," in IEEE Systems Journal, vol. 11, no. 2, pp. 503-512, June 2017. doi: 10.1109/JSYST.2015.2438442

[11] Otapo, A. T., Saliu, L. A., Sodiq, K. A., Tokunbo-Cole, M. O., & Okia, F. U. OFFICE-AUTOMATED intrusion DETECTION SYSTEM (O-AIDS).

[12] Hammar, K., & Stadler, R. (2021, October). Learning intrusion prevention policies through optimal stopping. In 2021 17th International Conference on Network and Service Management (CNSM) (pp. 509-517). IEEE.

[13] Tripathi, D., Tripathi, A. K., Singh, L. K., & Chaturvedi, A. (2022). Towards analyzing the impact of intrusion prevention and response on cyber-physical system availability: A case study of NPP. Annals of Nuclear Energy, 168, 108863.

[14] Pani, A. K., Manohar, M., & Kumar, R. (2021). An efficient algorithmic technique for feature selection in IoT-based intrusion detection system. Indian J. Sci. Technol, 14, 76-85.

[15] Alavizadeh, H., Alavizadeh, H., & Jang-Jaccard, J. (2022). Deep Q-Learning based Reinforcement Learning Approach for Network Intrusion Detection. Computers, 11(3), 41.

[16] Chou, D., & Jiang, M. (2021). A survey on data-driven network intrusion detection. ACM Computing Surveys (CSUR), 54(9), 1-36.

[17] E. Anthi, L. Williams, M. Słowińska, G. Theodorakopoulos and P. Burnap, "A Supervised Intrusion Detection System for Smart Home IoT Devices," in IEEE Internet of Things Journal, vol. 6, no. 5, pp. 9042-9053, Oct. 2019. doi: 10.1109/JIOT.2019.2926365

[18] W. -C. Hong, D. -R. Huang, C. -L. Chen and J. -S. Lee, "Towards Accurate and Efficient Classification of Power System Contingencies and Cyber-Attacks Using Recurrent Neural Networks," in IEEE Access, vol. 8, pp. 123297-123309, 2020. doi: 10.1109/ACCESS.2020.3007609

[19] Mohamed, T. S., & Aydin, S. (2021). IoT-Based Intrusion Detection Systems: A Review. Smart Science, 1-18.

[20] R. Ishibashi, K. Miyamoto, C. Han, T. Ban, T. Takahashi and J. Takeuchi, "Generating Labeled Training Datasets Towards Unified Network Intrusion Detection Systems," in IEEE Access, vol. 10, pp. 53972-53986, 2022. doi: 10.1109/ACCESS.2022.3176098

[21] Ge, M., Fu, X., Syed, N., Baig, Z., Teo, G., & Robles-Kelly, A. (2019, December). Deep learning-based intrusion detection for IoT networks. In 2019 IEEE 24th pacific rim international symposium on dependable computing (PRDC) (pp. 256-25609). IEEE.

[22] S. Pan, T. Morris and U. Adhikari, "Developing a Hybrid Intrusion Detection System Using Data Mining for Power Systems," in IEEE Transactions on Smart Grid, vol. 6, no. 6, pp. 3104-3113, Nov. 2015. doi: 10.1109/TSG.2015.2409775

[23] Saranya, T., Sridevi, S., Deisy, C., Chung, T. D., & Khan, M. A. (2020). Performance analysis of machine learning algorithms in intrusion detection system: a review. Procedia Computer Science, 171, 1251-1260.

[24] Gassais, R., Ezzati-Jivan, N., Fernandez, J. M., Aloise, D., & Dagenais, M. R. (2020). Multi-level host-based intrusion detection system for Internet of things. *Journal of Cloud Computing*, *9*, 1-16.

[25] Nagaraja, U. Boregowda, K. Khatatneh, R. Vangipuram, R. Nuvvusetty and V. Sravan Kiran, "Similarity-Based Feature Transformation for Network Anomaly Detection," in IEEE Access, vol. 8, pp. 39184-39196, 2020. doi: 10.1109/ACCESS.2020.2975716

[26] M. Zeeshan et al., "Protocol-Based Deep Intrusion Detection for DoS and DDoS Attacks Using UNSW-NB15 and Bot-IoT Data-Sets," in IEEE Access, vol. 10, pp. 2269-2283, 2022. doi: 10.1109/ACCESS.2021.3137201

[27] Krishna, A. M., & Tyagi, A. K. (2020, February). Intrusion detection in intelligent transportation system and its applications using blockchain technology. In 2020 International Conference on Emerging Trends in Information Technology and Engineering (ic-ETITE) (pp. 1-8). IEEE.

[28] P. Krishnamurthy, F. Khorrami, S. Schmidt and K. Wright, "Machine Learning for NetFlow Anomaly Detection With Human-Readable Annotations," in IEEE Transactions on Network and Service Management, vol. 18, no. 2, pp. 1885-1898, June 2021.

[29] Rajagopal, S., Kundapur, P. P., & Hareesha, K. S. (2021). Towards effective network intrusion detection: from concept to creation on Azure cloud. IEEE Access, 9, 19723-19742.

[30] Y. Li et al., "Automated Anomaly Detection via Curiosity-Guided Search and Self-Imitation Learning," in IEEE Transactions on Neural Networks and Learning Systems, vol. 33, no. 6, pp. 2365-2377, June (2022). doi: 10.1109/TNNLS.2021.3105636

[31] W. Xu, J. Jang-Jaccard, A. Singh, Y. Wei and F. Sabrina, "Improving Performance of Autoencoder-Based Network Anomaly Detection on NSL-KDD Dataset," in IEEE Access, vol. 9, pp. 140136-140146, 2021. doi: 10.1109/ACCESS.2021.3116612

[32] J. Pacheco, V. H. Benitez, L. C. Félix-Herrán and P. Satam, "Artificial Neural Networks-Based Intrusion Detection System for Internet of Things Fog Nodes," in IEEE Access, vol. 8, pp. 73907-73918, 2020. doi: 10.1109/ACCESS.2020.2988055

[33] M. Poongodi, V. Vijayakumar, F. Al-Turjman, M. Hamdi and M. Ma, "Intrusion Prevention System for DDoS Attack on VANET With reCAPTCHA Controller Using Information Based Metrics," in IEEE Access, vol. 7, pp. 158481-158491, 2019. doi: 10.1109/ACCESS.2019.2945682

[34] D. Vallejo-Huanga, M. Ambuludi and P. Morillo, "Empirical Exploration of Machine Learning Techniques for Detection of Anomalies Based on NIDS," in IEEE Latin America Transactions, vol. 19, no. 5, pp. 772-779, May 2021. doi: 10.1109/TLA.2021.9448311

[35] F. van Wyk, Y. Wang, A. Khojandi and N. Masoud, "Real-Time Sensor Anomaly Detection and Identification in Automated Vehicles," in IEEE Transactions on Intelligent Transportation Systems, vol. 21, no. 3, pp. 1264-1276, March 2020. doi: 10.1109/TITS.2019.2906038

[36] R. K. Sharma, B. Issac and H. K. Kalita, "Intrusion Detection and Response System Inspired by the Defense Mechanism of Plants," in IEEE Access, vol. 7, pp. 52427-52439, 2019. doi: 10.1109/ACCESS.2019.2912114

RESEARCH ARTICLE

Authors

Mr K Prabu is working as an Assistant Professor in School of Computing Science and Engineering, Galgotias University. He has 15 years of experience in teaching. He is Pursuing PhD (CSE) in Galgotias University & done M.Tech CSE (with Distinction) in SRM University. In addition, he has completed MBA in Anna University., He has published 4 patents and 9 research papers in various conferences. His area of interest includes Cyber Security, Networks, Cloud Computing, Software Engineering and Machine Learning.

Dr. P. Sudhakar is working as a Professor and Program Chair in School of Computing Science and Engineering, Galgotias University. He has 20 years of experience in teaching. He has done PhD (CSE) & ME CSE (with Distinction) at Anna University. He has published 14 patents and 22 research papers in reputed International Journals and Conferences. His area of interest includes Cyber Security, Networks, Cloud Computing, and Machine Learning.

How to cite this article:

K Prabu, P Sudhakar, "An Automated Intrusion Detection and Prevention Model for Enhanced Network Security and Threat Assessment", International Journal of Computer Networks and Applications (IJCNA), 10(4), PP: 621-636, 2023, DOI: 10.22247/ijcna/2023/223316.