JOURNAL OF MACHINE LEARNING AND APPLICATIONS
Jul-Dec 2025, VOL. 1, ISSUE 2, pp. 32-46
https://doi.org/10.61577/jmla.2025.100010

RESEAPRO JOURNALS

ORIGINAL ARTICLE

OPEN ACCESS

Integrating cybersecurity controls into network administration practices for securing computer information systems

Bishal Chowdhury Nihal and Joy E Jilqued

Department of Computer and Information Technology, Phoenix College, Arizona, United States

ABSTRACT

The rising sophistication of computer networks and cyber threats has made cybersecurity a vital part of modern network management. Traditionally, network management and security have been treated as separate domains, leading to delayed threat detection and increased system vulnerabilities. This study focuses on integrating cybersecurity controls into everyday network administration to improve the security of computer information systems. It highlights the importance of incorporating mechanisms such as traffic monitoring, access control, intrusion detection, and anomaly detection into routine network operations. The NF-UNSW-NB15-V2 dataset, which contains extensive network traffic records including normal and malicious activities, is used to support the analysis. The dataset includes features such as IP addresses, ports, protocol types, packet counts, byte volumes, and flow characteristics, enabling detailed evaluation of network behavior. Data analysis and feature exploration are conducted to identify traffic patterns associated with potential security risks and to assess how these metrics support the implementation of cybersecurity controls. The results indicate that integrating cybersecurity controls with network administration improves visibility into network activities and enables timely detection of abnormal and malicious behavior. Flow-level metrics, including packet rates, byte distribution, and protocol usage, are effective for intrusion detection attack surfaces, and protecting critical information assets for administrators and security professionals.

KEY WORDS

Network security; Cybersecurity controls; Network administration; Intrusion detection systems; Computer information systems; Network traffic analysis

ARTICLE HISTORY

Received 07 October 2025;
Revised 27 October 2025;
Accepted 04 November 2025

Introduction

Background

Computer networks are essential in aiding contemporary computer information systems by facilitating communication, the exchange of data, and access to digital services within organizations. Networks have gradually become an important infrastructure that supports applications, databases, cloud platforms, and remote services as companies continue to rely on interconnected systems to perform daily business activities. The fast development of technologies like cloud computing, mobile devices, Internet of Things (IoT), and remote workplace has greatly complicated the networks [1]. Although such developments make it more efficient and scalable, security risks and vulnerabilities arise. Network security is referred to as policies, practices, and technologies employed to safeguard network infrastructure and data transferred over the network against attacks by unauthorized individuals, mishandling, or interference. Intranet Traditional network environments were somewhat stable and were easier to protect using perimeter-based controls like firewalls and access control lists. Nevertheless, current networks are very dynamic, distributed, and heterogeneous, thus becoming more vulnerable to cyber threats [2]. Attackers currently take advantage of vulnerabilities on several levels of the network, such as protocols, applications, and user behavior. Network attack surfaces have increased the number of cyber-attacks, including malware infection, data breaches, denial-of-service attacks, and unauthorized access. Such threats may jeopardize the confidentiality, integrity, and availability of computer information systems, leading to lost revenues, business interruptions, and reputation [3-5] Network security has therefore become essential for organizations seeking to ensure that sensitive information is not compromised and system operations remain stable. Good network security must be regularly monitored, threats should be detected in time, and vulnerabilities should be handled proactively [6]. Organizations should also consider adopting an integrated security approach rather than relying on specific tools that are not tailored to the network's evolving environment. This increasing demand to have strong network protection highlights the significance of having cybersecurity considerations in the design, operation, and administration of networks to achieve robust and secure information systems [7].

Cybersecurity issues on network administration

The main issue of network administration is to provide network performance, availability, reliability, and efficient exploitation of resources. The duties of network administrators include finding solutions to these problems: setting up gadgets, traffic control, connection security, and fixing malfunctions. Nevertheless, in most organizations, the duties of cybersecurity are divided among special security teams, and thus, a disjointed effort is made to protect the network [8]. This segregation poses a major challenge to effective and timely security management. One significant drawback is the inability to have a real-time view of network activities. In the absence of the complete involvement of security monitoring in network administration procedures, the unusual patterns of traffic, as well as abnormal behaviors, may remain unnoticed until an incident has already taken place. Also, administrators usually focus on optimizing performance and uptime, which may lead to delayed patches, inadequate access controls, or incorrect

***Correspondence:** Mr. Bishal Chowdhury Nihal, Department of Computer and Information Technology, Phoenix College, Arizona, United States, e-mail: bishalchowdhurynihal@gmail.com

settings that can be used by attackers. These loopholes enhance the security risks of successful cyber-attacks [9]. The conventional security strategies that emphasize borderline security measures are also inadequate in the contemporary network setup. Advanced threats often impact firewalls by using internal weaknesses, hacked credentials, or encrypted traffic. Detecting insider threats, horizontal network movement, and advanced attack methods further complicate the issues of detecting threats. The tools or information-based insights to spot these threats may not be available to the network administrators in the normal operation workflow. The other problem is the management of massive traffic in networks created by contemporary systems. The administrators find it difficult to distinguish between normal and malicious traffic without automated analysis and built-in security measures. The fact that network and security teams do not have a coherent coordination of workflows and policies makes the incident response capabilities even weaker [10]. These issues demonstrate that a unified strategy is needed, which integrates cybersecurity measures into the routine of network management. Through security as an operational issue and not a distinct operation, organizations are able to enhance threat recognition, mitigate their vulnerabilities, and improve the overall resilience of the network.

Value of introducing cybersecurity controls

Incorporating cybersecurity measures in the network administration practices is imperative in dealing with the changing threat environment of contemporary computer information systems. With security mechanisms being built into day-to-day network processes, the administrators are able to proactively detect, block, and react to cyber threats without affecting network performance. Such a combination makes security not a process of reaction but an active and dynamic network management process [11]. Access management, traffic monitoring controls, intrusion detection systems, and configuration management are also cyberspace security controls that are essential in the security of networks. Access controls are used to guarantee that only authorized devices and users can access the network resources so that the chances of unauthorized access are minimized [12]. Traffic monitoring and flow analysis allow administrators to view network behavior, find anomalies, and detect possible attacks in real time. Intrusion detection systems also help in improving security by detecting the traffic patterns in order to detect known and unknown threats. An integrated approach enables network administrators to use the security data in the normal functions like monitoring the performance, updating the configuration, and troubleshooting [13]. This orientation enhances awareness of the situation and responds to the incident more quickly. Also, implementing cybersecurity controls helps minimize the risk of misconfigurations and policy mismatches that frequently arise when security and administration functions are isolated [14]. Organizationally, integration enhances better working efficiency through reducing unnecessary redundancy and simplifying work processes. It also facilitates adherence to security policies and regulatory requirements by ensuring uniform enforcement across the network [3]. More to the point, coordinated cybersecurity controls enhance the overall security posture of computer information systems by minimizing attack surfaces and improving the resilience of computer systems. In the new age where cyber-attacks are becoming more intricate and demanding, it is no longer a choice to incorporate cybersecurity measures in network management [15]. It is an effective and sensible approach to securing key information resources, preserving the continuity of services, and having confidence in online systems.

Problem statements

Although cybersecurity technologies have improved over the years, breaches of security continue to be witnessed in various organizations because of the failure to integrate cybersecurity controls and normal network management practices. The performance, availability, and connectivity are often given attention by the network administrators, whereas the security monitoring is inactive and piecemeal. The consequences of this disconnect are reduced visibility of network threats and a slow response to an incident. Lack of data-based security analysis in day-to-day network management limits early identification of abnormal behavior. To fill this gap, there should be a systematic formulation for resolving this gap, whereby cybersecurity controls are integrated into the network administration processes to drive the safety and soundness of computer information systems.

Research objectives

The key aim of the study is to analyze the adoption of cybersecurity controls in network administration practices to secure computer information systems. The particular research aims of the study are to:

- Determine the major flow-based features that help in supporting cybersecurity control measures like intrusion detection and traffic monitoring.
- Test the capability of integrated cybersecurity controls to monitor the abnormal activities of the network.
- Show how the analysis of the data can strengthen network administration and security practices.

Research questions

To fulfill the objectives mentioned, the proposed study is aimed at addressing the following research questions:

- What cybersecurity controls can be part of the normal network administration practices to safeguard computer information systems?
- What are the most effective network traffic characteristics that can be used to support intrusion detection and monitoring controls?
- What is the enhancement or benefit of cybersecurity control integration to detect abnormal and malicious network behavior?
- What is the best way to use data-driven network traffic analysis to augment proactive security management in operational networks?

Literature Review

Modern computer network security approaches

Network security has thus been changing massively in line with the development of computer networks and the ensuing advancements in cyber threats. The models of early network security were heavily dependent on perimeter-based defenses, such as firewalls, access control lists, and static filtering mechanisms. Although such solutions worked well in the closed and predictable network settings, they have not been found to be effective in the current distributed networks that accommodate cloud computing, mobile access, and dynamically changing traffic patterns [13]. Modern network

https://doi.org/10.61577/jmla.2025.100010

security focuses on the use of layered defense mechanisms that secure systems at various points along the network. The current methods aim at the protection of the confidentiality, integrity, and availability of information through the integration of preventive, detective, and remediation controls. Such preventive features as an authentication mechanism, encryption, and network segmentation are designed to prevent unauthorized access [14]. Detective measures like intrusion detection systems and traffic monitoring applications analyze network traffic and data in real time to detect any suspicious activity. The incident response, recovery, and system restoration after the security incidents are supported by corrective controls. Recent research emphasizes the need to have real-time monitoring and dynamic security systems that can handle changing threats [3]. Sophisticated network security systems are now moving towards behavioral analysis and anomaly detection systems as a way to detect attacks that are not detected by standard protection mechanisms. These methods take advantage of traffic flow traits, protocols used, and communication patterns to determine normal and malicious activities [15]. Flow-based analysis has received a lot of attention because it is scalable and can be used in high-speed networks. Difficulties exist in implementing multilayered security systems on the networks of operation. Most security tools are independent and hence lack integration of visibility and coordination. It is a fragmentation that diminishes the efficacy of the network security strategies [16]. As a result, wonderment is increasing about the necessity of coordinated methods that will ensure security mechanisms are synchronized with the management of the network operations. This kind of integration enhances the resilience of computer information systems against emerging cyber threats, improves situational awareness, and supports ongoing protection.

Cybersecurity controls and network administration practices

Cybersecurity controls are critical mechanisms designed to prevent attacks, abuse, and disruption of network resources. The controls are usually grouped into technical, administrative, and operational controls. Firewalls, intrusion detection systems, access control mechanisms, and encryption technologies are some of the technical controls. Examples of administrative controls include administrative security policies, procedures, and compliance requirements, whereas examples of operational controls are monitoring, maintenance, and incident response activities [17]. These controls, when coordinated in network environments, are needed to provide effective cybersecurity. Network administration practices refer to the establishment, management, and maintenance of network infrastructure to achieve maximum functioning and dependability. Even in traditional networks, availability and efficiency have been given precedence over security; therefore, security is usually put as a second consideration by network administrators [18]. This division has seen scanty cooperation between network operations and security functions. As a result, security controls are often implemented without sufficient attention to network workflows, leading to misconfigurations and decreased effectiveness [19]. Recent studies have highlighted the need to make cybersecurity controls part of mainstream network management activities. Introduction of security measures in the day-to-day operations enables administrators to detect threats in the routine activities of monitoring and maintenance [20]. As an illustration, centralized network management systems can be used to enforce access control policies, whereas performance analysis and intrusion detection can be supported by traffic monitoring tools. This integration makes it possible to have a coherent picture of the behavior and events of the network in relation to security. Operational integration is also beneficial in faster incident response and enforcing of the rules in a more consistent manner. When administrative workflows are in line with the security controls, the network administrators can easily detect abnormal behavior and act accordingly. But to ensure successful integration, processes should be clear, tools to be used adequately, and decisions should be made based on data. Research shows that those organizations that embrace built-in security and management systems have better detection of threats and minimize exposure to vulnerabilities [21]. This literature underscores the importance of models that ensure cybersecurity controls are aligned with the network administrative practices to increase the security of the computer information systems.

Intrusion detection data-driven network traffic analysis

Intrusion detection and network security management have become based on network traffic analysis driven by data analysis. As network traffic volume and variability increase, it is no longer possible to efficiently discover sophisticated cyber threats using manual inspection and rule-based methods. Data-driven approaches use the data on traffic flows to identify patterns, abnormalities, and signs of bad behavior [22]. These methods can provide valuable insights into network behavior and support active security surveillance. Flow-based analysis concentrates on overall traffic qualities, e.g., the quantity of packets, the quantity of bytes exchanged, the type of protocols, and the connection time duration. All these features record the statistical properties of network communications and allow monitoring of large network scales [23]. Using data-driven solutions to analyze differences from regular traffic patterns, anomalies can be identified to detect possible intrusions, abuse, or policy violations. This would be especially useful in the detection of stealth attacks that are not detected by signature-based detection systems. In the recent literature, it is noted that traffic analysis is effective when implemented together with intrusion detection systems to increase the detection accuracy. An intrusion detection model based on data may be able to adjust to changing threats by learning from historical traffic patterns and detecting hitherto-unseen attack patterns. This flexibility enhances detection rates and minimizes the false positives [24]. The data-informed analysis enables constant vigilance, which enables network administrators to maintain situational awareness and act upon threats on the spot. Although it has such advantages, data-driven approaches have issues associated with data quality, feature selection, and scalability [25]. Larger datasets demand effective methods of preprocessing and analysis to detect them in time. Also, there is a challenge to combine analytical insights into the management of the operational networks. Numerous surveys highlight the need to align security analysis based on data with the network administration processes to achieve the highest effectiveness [26]. This agreement results in analytical findings that are translated into practical security controls, supporting the imperative to incorporate cybersecurity in contemporary network settings.

Empirical study

Cybersecurity is a pressing issue in contemporary information

https://doi.org/10.61577/jmla.2025.100010

systems, and organizations are turning to the internet to handle sensitive information more than ever before. In the article Cybersecurity in Management Information Systems (MIS): Challenges and Best Practices to Protect Data by Nicole Kidman [1], the issue of cybersecurity in the context of MIS is considered through a qualitative research methodology. The research recognizes data breaches, phishing, ransomware, and insider threats as major threats that can highly affect the confidentiality, integrity, and availability of organizational data. It highlights that the old method of providing perimeter-based security is not adequate to deal with the dynamic cyber threat, and it is important to embrace the best practices such as multi-layered security architecture, encryption systems, and two-factor authentication. The article further emphasizes the importance of employee awareness and training programs in minimizing the vulnerabilities that human beings pose and that attackers often exploit. Moreover, regulatory compliance frameworks such as GDPR and HIPAA are considered necessary instruments for implementing security standards and safeguarding user privacy. Constant checking and monitoring, the conduction of regular security audits, and the implementation of policies are identified as the needed measures to secure MIS environments. This research focuses on worthwhile conceptual knowledge, presenting cybersecurity as a managerial and technical task and advocating the necessity of integrated security controls. These insights are consistent with the current study's interest in integrating data-driven cybersecurity controls into operational network administration practices to improve the protection of computer information systems.

Cybersecurity is of growing importance as a criterion affecting the organizational decision-making process in digitally dependent settings. The role of cybersecurity is presented in the article by Adebola Folorunso, in the article titled Cybersecurity and Its Global Applicability to Decision Making: A Comprehensive Approach in the University System, both strategically and institutionally, with specific reference to academic settings [4]. The paper points out that, given the vast digital infrastructure and data assets, universities are highly susceptible to cybercrime, and cybersecurity is a primary part of institutional controls and decision-making. The article highlights that cybersecurity frameworks play a major role in strategic planning, resource allocation, and policy development, as they provide risk management and continuity-of-operations frameworks. It also addresses the role of proactive cybersecurity in defending against sensitive student, administrative, and research information as well as facilitating efficient institutional operations [4]. Constant monitoring, incident response, planning, and stakeholder engagement are recognized as key aspects of effective decisions to be made in cybersecurity. The research recommends a holistic approach in which cybersecurity is incorporated into daily operations and strategic operations and is not a separate technical issue. The insights support the opinion that cybersecurity needs to be integrated into organizational systems and management practices. The views expressed in this publication are consistent with the aim of the current study, which entails developing cybersecurity controls in the network management practices to improve proactive threat detection, well-informed decision-making, and overall security of computer information systems.

The issue of cybersecurity has become especially urgent with regard to enterprise systems that sustain a country's critical infrastructure, due to which security breaches may have a devastating economic and social impact. In the article A Multi-Layered Cybersecurity Model to ERP Systems Supporting National Critical Infrastructure: Threats, Challenges, and Solutions by Chandrasekhar Atakari, an elaborate model of cybersecurity is developed in order to deal with the increased complexity of threats against Enterprise Resource Planning (ERP) systems [6]. The paper highlights that the combination of ERP systems and cloud services, IoT, and artificial intelligence has dramatically increased the attack space, and a multifaceted security strategy is required. The given model involves preventative, detective, and corrective controls on both physical, network, application, and data layers to protect it holistically. The important security mechanisms to be discussed are zero-trust architecture, role-based access control, intrusion detection systems, anomaly detection systems based on AI, and blockchain-based integrity systems [7]. The article emphasizes the need to constantly observe and adopt dynamic security controls to deal with emerging cyber threats. Through experimental assessment in simulated attack conditions, better threat mitigation and system resiliency is realized. The paper highlights the importance of cybersecurity being entrenched at all levels of operation as opposed to being applied as single-point controls. The results of these findings are highly indicative of the theme of the current study, which is the incorporation of cybersecurity controls into network management activity to obtain proactive threat identification, operational resistance, and the most efficient level of computer information system security.

In a digitized environment, cybersecurity has emerged as a basic need of safeguarding critical infrastructure and enterprise networks. In the article, Implementing Robust Cybersecurity Strategies to Protect Critical Infrastructure and Enterprise Networks, by Aryendra Dalal, the author discusses the inability of single-level security systems and highlights the necessity of developing multi-layered, multi-tiered cybersecurity systems [8]. As the study points out, the current cyber threats affect both physical and digital resources, and conventional perimeter-based security is no longer effective. It talks of the combination of proactive and reactive security measures, which are backed by the risk management models and ongoing monitoring habits. The article focuses on the significance of implementing Zero Trust architecture, automation, and innovative technologies like artificial intelligence and machine learning to improve the ability to detect and prevent threats [8]. The AI- and ML-based systems are listed as the enabling factors to detect sophisticated attack patterns and react to the threats in real-time. Also, the paper discusses how incident response planning, secure network architecture, and multilayered defense models can be used to ensure operational resilience. The results emphasize that cybersecurity is to be constantly adapted to match the changing methods of attack, but not executed as fixed controls. These findings corroborate the theme statement of the current study, which is the incorporation of information-based cybersecurity measures into the network management processes to enhance proactive security, enhance threat awareness, and maintain the confidentiality and integrity of computer information systems.

Methodology

This study employs a guided research approach to analyze how cybersecurity controls can be incorporated into network administration practice to ensure the security of computer

https://doi.org/10.61577/jmla.2025.100010

information systems. The methodology involves quantitative analysis of data and machine learning-based intrusion detection methods in order to study the actual network traffic behavior in practice [7]. The methodology starts with the choice of a benchmark network security dataset, preprocessing of the data, and feature selection to guarantee the reliability of the analysis. The model of supervised learning is then applied to categorize traffic over the network into normal and malicious traffic. Last but not least, several evaluation measures are used to determine the performance of detection and security effectiveness [27]. This methodological approach allows the overall analysis of how a data-driven cybersecurity control can be used to improve proactive network security and assist in sound administrative decision-making.

Research design and approach

The research design is a quantitative, experimental research design that will seek to assess the effectiveness of integrating cybersecurity controls into a regular network administration practice. The research is based on the data and aims at conducting the empirical analysis of network traffic behavior to identify normal and malicious activity. The methodology is an experimental one to apply and test a machine learning-based intrusion detection mechanism in a controlled analytical environment [28]. The scientific process is sequential and is divided into different phases that include the acquisition and comprehension of data, preprocessing, and identification of features [5]. The above steps would make sure that the data is appropriate to model and would be a good representation of network behavior. A supervised learning method is subsequently implemented, with the help of which the labeled network traffic data trains a classification model. The model learns the characteristics of legitimate and malicious traffic flows, enabling automatic identification of security threats. This can be used to experimentally control the performance of a model in realistic network conditions [29]. Using a set of evaluation measures, the study evaluates the model's classification accuracy and its ability to identify uncommon attacks [30]. The design allows objective comparison of detection performance and gives quantifiable evidence of the value of the integration of cybersecurity controls in network administration. All in all, the research design will guarantee systematic analysis, reliability, and applicability to network security activities in the real world.

Dataset description

This study relies on the NF-UNSW-NB15-V2 dataset as its primary source of data because this source is more relevant and applicable in the research on network security. The data set will consist of network flow records that represent extensive normal and malicious traffic patterns. It involves traffic created with the help of various network protocols, services, and attack scenarios, which makes it reflective of the actual network environment [31]. The dataset records have several flow-related attributes, including the number of packets, the number of bytes, protocol identifiers, and connection-related statistics. These characteristics provide detailed information on communication patterns, traffic direction, and session characteristics. This dataset is labeled such that it can be utilized in supervised learning methods in order to detect intrusions. The dataset's realism makes it particularly appropriate for assessing cybersecurity controls in a working network [32]. It is a mirror of universal problems, like the problem of class imbalance, when the normal traffic is much more than the malicious traffic. This feature reflects the actual network scenarios and allows a worthwhile comparison of detection. The NF-UNSW-NB15-V2 dataset can be considered a solid source for analyzing network behavior, intrusion detection models, and evaluating how cybersecurity controls can be integrated into the network administration practice.

Data preprocessing

Data preprocessing is a very important process in determining the accuracy and reliability of analytical results. The preprocessing step will start with eliminating the irrelevant or redundant features that do not add any significant meaning to intrusion detection [33]. This not only minimizes the dimensionality of data but also enhances the performance of calculation without the effect of affecting the value of the analysis. Encoding techniques are used to encode protocol identifiers, among other categorical features, into numerical forms, which can be used in machine learning algorithms [34]. Data types such as packets and bytes are normalized to make them fall within a range. The feature scaling can make sure that attributes that have bigger numeric values do not imbalance the process of learning. Controlled sampling techniques are used to ensure that the large dataset size is dealt with and the original class distribution is preserved to enhance training performance. This maintains the original nature of the data set, especially the imbalance between classes [35]. Checking for missing and inconsistent values is also part of preprocessing, as it checks the integrity of the data. These pre-processing processes increase the stability of the model, minimize the noise, and detect with greater accuracy [36]. Through data preparation in a systematic manner, the study ensures that the further feature selection training and model training processes will be performed on a high-quality and trustworthy dataset, which allows the study to present a strong intrusion detection analysis.

Selection and engineering of features

The feature selection aims at identifying the most useful network traffic characteristics that can be used in effective intrusion detection. Flow-based features get preference because they can capture communication behavior and do not require any inspection of the payload. The major attributes, like the number of packets inbound and outbound, the volume of data in the form of bytes, and protocols, are picked depending on their implication in the analysis of traffic behavior. These characteristics are vital attributes of network communication, such as intensity of traffic, directionality, and usage pattern of the protocols [37]. A small number of informative features chosen helps reduce the model's complexity without compromising detection performance. The use of feature engineering is used when required to enhance interpretability and to better represent network behavior. The approach is normalized by paying attention to flow-based features, which are compatible with the real-world constraints of network administration, where lightweight monitoring is desirable [38]. The chosen features empower cybersecurity regulations, including traffic surveillance, anomaly detection, and intrusion identification [39]. The feature selection and engineering process, on the whole, guarantees that the model of intrusion detection is effective and could be integrated into the real-life network administration environment.

Implementation of the machine learning models

The Support Vector Machine (SVM) classifier is utilized as the main intrusion detection model in the current research. SVM is

https://doi.org/10.61577/jmla.2025.100010

selected because it is a high-dimensional space and has a good performance in constructing optimal decision boundaries among classes [40]. The network traffic data is labeled with the labels normal or malicious and is used to train the model to label other network traffic as normal or malicious. Class weighting is used in model training to eliminate the problem of class imbalance. This method gives more weight to cases of minority classes that enhances the sensitivity of the model to malicious traffic. The feature-scaled data is applied to guarantee a smooth model convergence and constant performance. The trained SVM model is an automated control solution against cybersecurity and can identify abnormal traffic patterns. It can be integrated into network administration procedures to be able to monitor the network in real time and detect threats beforehand [41]. The structure of the model is focused on both the accuracy in detection and the feasibility of the operation; hence it can be implemented into practice in terms of network security.

Metrics of performance evaluation

To assess the performance of the intrusion detection model, several complementary measures will be used to make sure that it is considered holistically. A confusion matrix is employed to examine the results of classification, and it also gives an understanding of the number of true positives, false positives, true negatives, and false [42,43]. This measure emphasizes the accuracy of detection and errors. To consider the trade-off between true positive and false positive rates at different levels, receiver Operating Characteristic (ROC) curves are used [44]. Precision recall curves also evaluate the performance of detection in the case of imbalanced classes. Also, recall and F1-score measures measure how sensitive the model is to malicious traffic and precision and recall balance [45]. There are various evaluation metrics that must be used to guarantee the real workability of intrusion detection. With the help of this multi-metric method, it is possible to come to informed decisions about the effectiveness of implementing machine learning-based cybersecurity controls into network administration practices.

Limitations

This study is limited in a number of ways, although it has some contributions to make. The evaluation is based on one benchmark dataset, and this might not reflect all the fluctuations that exist in the actual network setups [46]. Although the dataset is realistic, network traffic patterns and attack behavior may change over time, potentially impacting the model's generalizability. Besides, the research is based on binary classification of normal and malicious traffic rather than multi-class attacks [47]. Offline analysis does not provide an opportunity to test in real-time performance and scalability. These limitations can be overcome in future studies through the addition of live network data, investigation of more machine learning models, and analysis of multi-class intrusion detection.

Conceptual Framework

This conceptual framework will aim to explain the connections among network administration practices, cybersecurity controls, data-driven analysis, and the security of computer information systems. The framework shows how the incorporation of cybersecurity into everyday administration of the network improves detection of threats, monitoring effectiveness, and protection of the whole system [48]. The network traffic data is at the center of the framework, as it reflects the working habits of computer networks. Network traffic consists of flow-level information, including the number of packets, volume of bytes, protocol usage, and patterns of communication. These attributes are measurable attributes of network behavior, and they are the input for the security analysis. In the normal situation, the network traffic is predictable in nature as a result of organizational policies and user actions. But ill intentions also create deviations which are observable with systematic analysis [49]. The second part of the framework is preprocessing and feature extraction of data, which converts raw traffic on the network to analytical inputs. This step guarantees data quality, consistency, and relevance through noise-filtering, coding of categorical variables, and normalization of the numeric ones. The feature selection is important in drawing attention to the most effective characteristics of traffic, which can be used in identifying abnormal behavior [50]. These characteristics facilitate the adoption of cybersecurity measures like traffic monitoring and the detection of an anomaly. The third element is concerned with cybersecurity controls that are incorporated in network administration. The controls are intrusion detection mechanisms, access monitoring, and traffic analysis tools. These controls will be integrated into the normal network administration process so that security becomes proactive instead of reactive [51]. Models based on machine learning, like SVMs, serve as analytical control that constantly assesses traffic behavior and identifies malicious and normal network flows. Security outcomes are the last element of the framework that involves the enhancement of threat detection accuracy, shorter response time, and better protection of computer information systems. The measures of performance evaluation include recall, precision, F1-score, and ROC analysis to give feedback on the efficiency of the integrated controls. This feedback process allows administrators to optimize policies, change detection thresholds, and enhance system resilience [52]. The conceptual model illustrates that successful network security is realized by the interaction of network data on an ongoing basis with analytical processing and integrated cybersecurity controls on one hand and administrative decision making on the other hand. In conjunction with data-driven intrusion detection, network administration practices can enhance the role of organizations to protect their cybersecurity status and maintain the confidentiality, integrity, and availability of computer information systems (Figure 1).

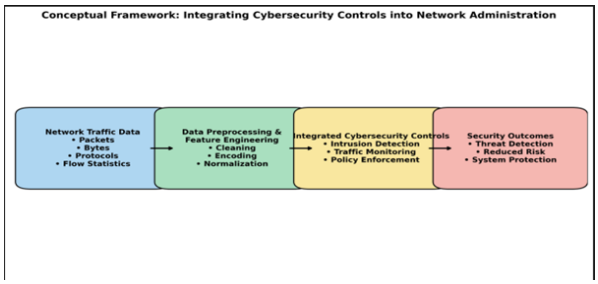

Figure 1. Conceptual framework for integrating cybersecurity controls into network administration.

The conceptual framework diagram depicts an effective, evidence-based strategy of incorporating cybersecurity controls into network administration activities. The first framework is the network traffic data, which are raw inputs representing the monitored networks of operation; hence, packets, amount of bytes transmitted, protocol usage, and flow

https://doi.org/10.61577/jmla.2025.100010

statistics. These data components represent the basic actions of the network communications and form the foundations of security analysis [53]. The second phase is data preprocessing and feature engineering, which converts raw traffic data into useful inputs to the security mechanisms. This phase entails cleaning up the data so that it eliminates noise, coding categorical characteristics into numbers, and normalizing them so that the measures of features are uniform in size. Such processes enhance the quality of data and data analysis reliability. The third level emphasizes combined cybersecurity controls, where intrusion detection systems, traffic monitoring, and policy enforcement systems are built into network management processes. The controls allow proactive threat identification and continuous monitoring [54]. The last stage reflects the security outcomes, which indicate the way integrated controls can result in effective detection of threats, lower security risks, and better defense of computer information systems. In general, the framework highlights the rational sequence of data collection to the process of security improvement.

IPV4_SRC_ADDR	L4_SRC_PORT	IPV4_DST_ADDR	L4_DST_PORT	PROTOCOL	L7_PROTO	IN_BYTES	IN_PKTS	OUT_BYTES	OUT_PKTS	TCP_FLAGS	CLIENT_TCP_FLAGS	SERVER_TCP_FLAGS	FLOW_DURATION_MILLIS	DURATION_IN	DURATION_OUT	MIN_TTL	MAX_TTL	LONGEST_FLOW_PKT	SHORTEST_FLOW_PKT	MIN_IP_PKT_LEN	MA... LEN
59.166.0.5	1305	149.171.126.8	21	6	1	9	5	159	7	24	24	24	0	0	0	31	32	96	52	52	
59.166.0.5	1305	149.171.126.8	21	6	1	281	5	469	7	24	24	24	0	0	0	31	32	96	52	52	
59.166.0.5	1305	149.171.126.8	21	6	1	481	9	750	11	24	24	24	0	0	0	31	32	96	52	52	
59.166.0.5	1305	149.171.126.8	21	6	6	781	11	7054	17	24	24	24	0	0	0	31	32	106	52	52	
59.166.0.5	1305	149.171.126.8	21	6	1	1031	19	1474	21	24	24	24	0	0	0	31	32	106	52	52	
59.166.0.5	1305	149.171.126.8	21	6	6	1231	23	1770	25	24	24	24	0	0	0	31	32	106	52	52	
59.166.0.5	1305	149.171.126.8	21	6	1	1491	27	2054	25	24	24	24	0	0	0	31	32	106	52	52	
175.45.176.1	42206	149.171.126.8	21	6	1	338	7	150	7	24	24	24	4294952	9	10	62	62	106	47	42	
59.166.0.5	1305	149.171.126.8	21	6	1	1817	13	2334	15	24	24	24	4294952	15	15	31	32	106	52	52	
59.166.0.5	1305	149.171.126.8	21	6	1	2059	37	2914	79	24	24	24	4294952	15	15	31	32	106	52	52	
59.166.0.5	1305	149.171.126.8	21	6	1	2319	43	3213	45	24	24	24	4294952	15	15	31	32	106	52	52	
59.166.0.0	42206	149.171.126.8	21	6	1	9	1	191	9	24	24	24	0	0	0	31	32	96	52	52	
59.166.0.0	44206	149.171.126.8	21	6	1	281	5	469	7	24	24	24	0	0	0	31	32	96	52	52	
59.166.0.0	44206	149.171.126.8	21	6	1	481	9	750	11	24	24	24	0	0	0	31	32	96	52	52	
59.166.0.0	44206	149.171.126.8	21	6	1	799	11	1474	15	24	24	24	0	0	0	31	32	106	52	52	
59.166.0.0	44206	149.171.126.8	21	6	1	1051	13	1474	21	24	24	24	0	0	0	31	32	106	52	52	
59.166.0.0	44206	149.171.126.8	21	6	1	1331	23	1751	24	24	24	24	0	0	0	31	32	106	52	52	
59.166.0.0	44206	149.171.126.8	21	6	1	1851	17	1474	29	24	24	24	0	0	0	31	32	106	52	52	
59.166.0.0	44206	149.171.126.8	21	6	1	1037	13	2474	23	24	24	24	0	0	0	31	32	106	52	52	
59.166.0.0	44206	149.171.126.8	21	6	1	2059	27	2318	79	24	24	24	0	0	0	31	32	106	52	52	
59.166.0.0	44206	149.171.126.8	21	6	1	2557	43	3232	45	24	24	24	0	0	0	31	32	106	52	52	
175.45.176.1	44206	149.171.126.1	21	6	1	557	11	619	9	24	24	24	4294952	15	15	31	32	106	40	40	
175.45.176.1	44206	149.171.126.1	21	6	1	757	13	829	11	24	24	24	4294952	15	15	31	32	106	40	40	
59.166.0.7	64716	149.171.126.3	21	6	1	9	1	119	1	24	24	24	0	0	0	31	32	98	52	52	
59.166.0.7	64716	149.171.126.3	21	6	1	331	9	469	7	24	24	24	0	0	0	31	32	98	52	52	
59.166.0.7	64716	149.171.126.3	21	6	1	481	9	793	11	24	24	24	0	0	0	31	32	98	52	52	
59.166.0.7	64716	149.171.126.3	21	6	1	791	11	1054	11	24	24	24	0	0	0	31	32	106	52	52	
59.166.0.7	64716	149.171.126.3	21	6	1	1251	23	1754	21	24	24	24	0	0	0	31	32	106	52	52	
59.166.0.7	59648	149.171.126.3	21	6	1	9	1	113	1	24	24	24	0	0	0	31	32	92	52	52	
59.166.0.7	64716	149.171.126.3	21	6	1	1251	23	1751	25	24	24	24	0	0	0	31	32	106	52	52	
59.166.0.7	59648	149.171.126.3	21	6	1	321	2	429	7	24	24	24	0	0	0	31	32	98	52	52	
59.166.0.7	59648	149.171.126.3	21	6	1	481	5	750	11	24	24	24	0	0	0	31	32	98	52	52	
59.166.0.7	64716	149.171.126.8	21	6	1	1493	27	2028	29	24	24	24	0	0	0	31	32	106	52	52	
59.166.0.7	59648	149.171.126.8	21	6	1	791	11	2214	21	24	24	24	0	0	0	31	32	106	52	52	
59.166.0.7	64716	149.171.126.8	21	6	1	1817	33	2210	33	24	24	24	0	0	0	31	32	106	52	52	
59.166.0.7	64648	149.171.126.8	21	6	1	1031	18	1674	21	24	24	24	0	0	0	31	32	106	52	52	

Source: https://www.kaggle.com/datasets/sankurisrinath/nf-unsw-nb15-v2csv

Dataset overview

The current study makes use of the NF-UNSW-NB15-V2 dataset as the main repository of the data on the network traffic behavior that could be used to analyze and measure the efficiency of cybersecurity controls incorporated into the network administration practices. The dataset is a variation of the popular UNSW-NB15 dataset that is specifically aimed at backups of network security and intrusion detection studies. It is realistic with regard to network conditions as it mimics the various legitimate and malicious activities of traffic under a controlled experimental setting. The dataset contains a large set of network flow records, each of which indicates a network communication session between network parties [55]. These records contain many attributes in the form of flows, which are the number of inbound and outbound packets, size in bytes, protocol identifiers, source and destination addresses, and session-level statistics. These characteristics can be used to analyze the patterns of traffic, communication intensity, and protocol behavior in a fine-grained manner without having to access the payload data, and therefore, the dataset is well-suited to a privacy-preserving security analysis. The main peculiarity of NF-UNSW-NB15-V2 data is the existence of both normal network activity and diverse types of malicious traffic. This variation enables intrusion detection models to acquire valuable differences between normal and abnormal behavior. There is also a high level of imbalance in classes in the dataset, where the normal traffic is more common compared to the attack traffic [56]. This feature is very similar to practice in network settings and poses a real challenge to the creation and testing of intrusion detection systems. The data is presented as an organized CSV, which allows easy data preprocessing, feature selection, and implementation of machine learning. Every flow record is tagged, and supervised learning methods can be used to categorize traffic as normal or malicious. This labeling is critical to training and assessing machine learning models to be used as cybersecurity controls. On the whole, the NF-UNSW-NB15-V2 data set offers strong and credible background studies in this study. Its extensive set of features, extensive scale, and realistic traffic distribution allow examining the behavior of the network in detail and experimentally testing intrusion detection schemes. Through this dataset, the analysis will guarantee that the results of the analysis are applicable in real-life network administration contexts and can be used to develop integrated, data-driven cybersecurity solutions.

Results

This is the section of the paper where the findings of the NF-UNSW-NB15-V2 data analysis will be discussed to assess the implementation of cybersecurity controls in network administration practices. The protocol distribution, traffic volume, and packet flow analyses were used to investigate the behavioral patterns in normal and malicious activities [57]. Besides, an intrusion detection model based on a SVM was deployed to evaluate the usefulness of data-driven security measures. Confusion matrix, ROC curve, precision-recall curve, F1-score, and recall measures were used to evaluate model performance. The findings offer information on the nature of a network, showcase the difficulties of intrusion detection under an unbalanced dataset, and illustrate the role of machine learning in complementing proactive security surveillance and safeguarding computer information systems.

Analysis of protocol distribution

https://doi.org/10.61577/jmla.2025.100010

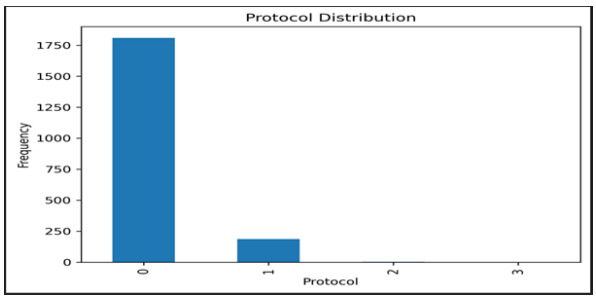

Figure 2. Distribution of protocols in network traffic flows.

The network protocols distribution of the NF-UNSW-NB15-V2 is shown in Figure 2. The figure demonstrates a much skewed distribution whereby one of the protocol categories carries most of the network traffic, with the other protocols having a much lower frequency. This asymmetry indicates the nature of the existing enterprise networks in the real world where only a small number of protocols usually do most of the communication [5]. The prevalence of the main protocol demonstrates that the normal network functions are dependent on the conventional transport mechanisms that are necessary to transmit data and to deliver the services. Conversely, the lower rates of the other types of protocols indicate that there was a narrow scope of their usage or the protocols were specifically utilized in the network [29]. This is in line with policy-controlled network administration systems that restrict the use of unusual or even dangerous protocols. Regarding the aspect of cybersecurity, this protocol concentration has significant implications for network monitoring and the implementation of security control [30]. High-frequency protocols have to be inspected constantly because they are usually attacked by attackers to perform malicious actions in the regular traffic streams. On the other hand, low-frequency protocols are not as prevalent but could manifest as an anomalous or suspicious action when it does not follow the expected pattern [31]. These deviations can be identified and tracked to greatly increase intrusion detection and anomaly detection mechanisms. The findings reveal that protocol-level traffic analysis is very useful when it comes to incorporating cybersecurity controls into the network administration practice [32]. Knowing patterns of protocol usage, network administrators can establish even more effective access control policies, optimize firewall rule settings, and have a priority when monitoring resources. The protocol distribution analysis demonstrates the significance of the protocol-conscious security policy in enhancing the security of computer information systems and increasing the active threat detection in the functioning network setup.

Inbound and outbound traffic volume analysis

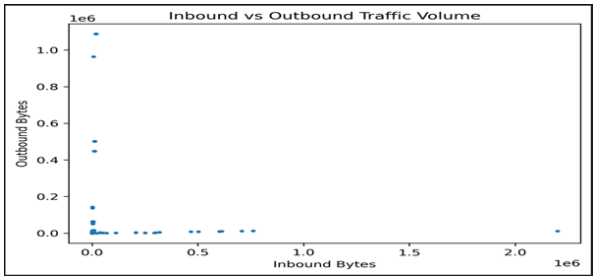

Figure 3. Relationships of inbound and outbound traffic volume through network flows.

In Figure 3, the interdependence between inbound and outbound traffic volumes in number of bytes between network flows is presented in the NF-UNSW-NB15-V2 dataset. The scatter plot indicates that most network communications involved relatively small data transfers, with the highest concentration of data points at lower byte values. The trend is typical of regular operations of the network functions, which include control messages, brief data exchanges, and frequent service requests. A few data points are observed to be distinct outliers with a much higher volume of inbound or outbound bytes. These high values imply that there are some high data transfers in terms of volume, and this could be related to file downloads, data backups, or large service responses. Cybersecurity-wise, these spike traffic should be looked at with a bit more scrutiny as abnormally high volumes of data can also be a sign of malicious actions such as data exfiltration, denial-of-service, and illegal bulk transfers. The difference that exists between inbound and outbound traffic also shows differences in communication behavior. Some flows will have high inbound bytes and low outbound response, and some will show the reverse behavior. Such imbalances are significant manifestations to the network administrators, who might show abnormal usage patterns or policy breaches [32]. By incorporating the traffic volume analysis into the network administration, it becomes possible to monitor the behavior of the data flow continuously, as well as to initiate the investigation of the suspicious behavior at the earliest stage. On the whole, the findings indicate that traffic volume analysis, inbound and outbound, is a useful element of cybersecurity controls in network administration procedures. Through the identification of normal traffic clusters and abnormal outliers, the administrators can achieve better monitoring thresholds, better intrusion detection precision, and better proactive security management. This discussion supports the significance of metrics based on traffic in securing computer information systems and network integrity.

Outbound and inbound packet flow analysis

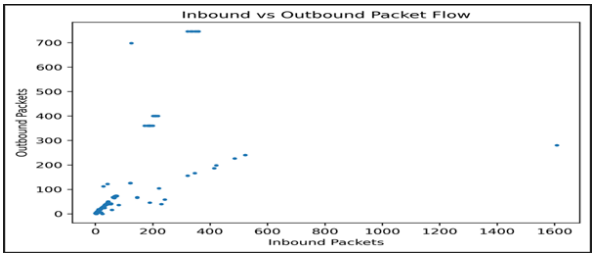

Figure 4. Relationship between incoming and outgoing packet flow across the network traffic sessions.

Figure 4 shows the correlation between the inbound and outbound traffic of packets in the NF-UNSW-NB15-V2 dataset. The scatter plot shows that most of the network traffic flows are located at lower packet counts, meaning that most communications are short and effective in exchange of packets. This is common to normal network operation, like acknowledgment, control signaling, as well as daily client-server interactions in managed network environments. In the plot, one can see several different outliers that represent flows that have much higher numbers of inbound packets or outbound packets. The large number of packets in these flows implies long or repeated communication sessions, which can be related to activities such as bulk data transfers, network scanning, probing, or flooding-based attacks. Existence of these patterns indicates the relevance of packet-level

https://doi.org/10.61577/jmla.2025.100010

inspection as an auxiliary practice to monitoring at the level of a single byte. The asymmetry of some flows, where inbound packets are far greater than outbound packets or the other way around, is also a good revelation about the communication behavior. These imbalances can reflect anomalous usage patterns, poorly configured services, or malicious intent to overload network resources [33]. A network administration approach to such deviations would be to monitor them so that administrators can counter possible threats early enough and implement the right security measures. Comprehensively, the findings indicate that packet flow analysis (inbound and outbound) is essential in the process of incorporating cybersecurity measures into network administration. Intrusion detection systems and traffic monitoring tools can enhance the accuracy of detection by setting baseline behavior on packets and identifying abnormal behavior. This analysis will aid in the identification of threats before they occur, enhancing security operations, and helping to secure computer information systems.

Malicious and normal traffic distribution analysis

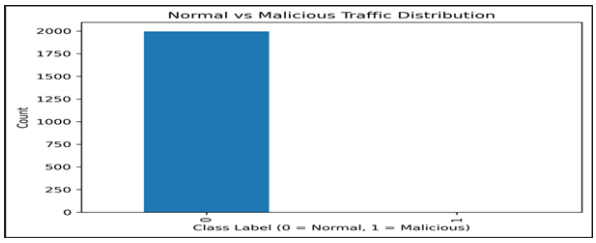

Figure 5. Allocation of normal and malicious combinatory traffic.

As shown in Figure 5, the distribution of normal and malicious network traffic in the NF-UNSW-NB15-V2 dataset is as follows. The bar graph presents a clear picture of a huge imbalance between the two classes, where normal traffic has the majority of the network flows, whereas malicious traffic has a much smaller percentage. This distribution is realistic in operational network scenarios, in which attacks are relatively infrequent relative to legitimate network traffic. Normal traffic dominance underscores the difficulty of intrusion detection systems and security monitoring tools to detect malicious activity within a big amount of normal traffic. In terms of cybersecurity, such a class imbalance may adversely impact detection accuracy, especially where security mechanisms are based on learning trends of historical data. This highlights the importance of strong and highly integrated cybersecurity controls that can identify any subtle anomaly as opposed to frequency-based or indicators [34]. The occurrence of a smaller, but substantial, number of malicious traffic proves that attack patterns are entrenched in the daily running of networks. By incorporating cybersecurity controls into network administration, administrators can continuously monitor traffic distribution and modify security policies based on observed behavior. With the ability to detect anomalies in the anticipated traffic proportions, network administrators will be in a better position to determine possible threats and prioritize security responses [35]. The analysis also justifies the significance of data-driven security strategies in the management of networks. The use of traffic class distribution can be used to design intrusion detectors that are sensitive to the rare cases of attack but keep the false positives to a minimum. Altogether, the findings support that the examination of normal and malicious traffic distribution is a precursor stage to enhancing cybersecurity measures, augmented threat recognition, and information system protection on computers in dynamic networks.

The confusion matrix analysis of the SVM-based intrusion detection model

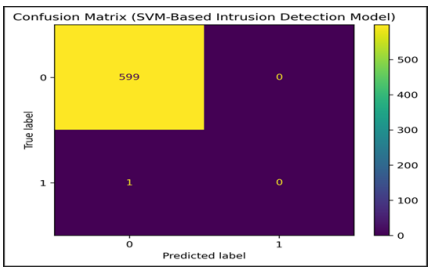

Figure 6. Confusion matrix that shows SVM classification performance that is used in network traffic.

Figure 6 shows the confusion matrix of the SVM based intrusion detection model modeled by using the NF-UNSW-NB15-V2 dataset. The confusion matrix gives a sensitive analysis of the performance of the model at classification by showing the number of properly and incorrectly classified data of normal and malicious traffic. This model facilitates the predictive behavior of this model in realistic network conditions. With the results, one finds that the number of correctly identified normal cases of traffic is high, which means that the SVM model is effective in identifying legitimate network behavior. This is especially valuable in operational network environments, where it minimizes false alarms and unnecessary administrative interventions. The fact that misclassified malicious cases do exist, however, points to the inherent challenge of identifying rare attack instances in massively imbalanced data sets. False negatives, which include malicious traffic being mistakenly identified as normal, are an important security issue because, in this case, an attack can be carried out without detection [36]. On the other hand, false positives, where normal traffic is termed as malicious, may create overhead within its operations and affect network performance. The proportions of these types of errors are critical in determining the feasibility of the cybersecurity controls incorporated in the network administration practice. The analysis of the confusion matrix shows that the performance of the SVM model in terms of classification with normal traffic is high, although the sensitivity of attacks can be enhanced [37]. These results manifest the need to integrate machine learning-acquired intrusion detection with constant monitoring, policy enforcement, and administration controls. Incorporating these models into the regular network administration practices can improve the threat visibility, accuracy in the response, and the security of the computer information system.

ROC curve analysis of SVM-based intrusion detection model

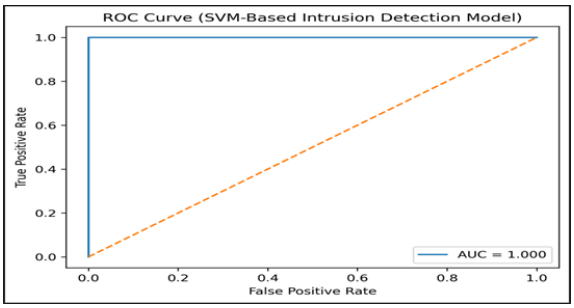

Figure 7. ROC curve used to show the performance of SVM model in detecting intrusion.

https://doi.org/10.61577/jmla.2025.100010

Figure 7 shows the ROC curve of the SWM-based intrusion detection model that is trained on the NF-UNSW-NB15-V2 dataset. The ROC curve shows how the true positive rate and false positive rate change with the classification threshold over different classification thresholds, which gives a holistic assessment of the model's capability to differentiate between normal and malicious network traffic. The curve shows that it deviates far from the diagonal reference line, which shows that the SVM model is highly discriminating between the two classes of traffic. The high true positive rate with comparatively low false positive rates is an indicator of good performance of the model in detecting the malicious activity with minimal error of classifying legitimate traffic as malicious. This equilibrium is essential where there are operational network environments, as false alarms can be excessive and end up overwhelming the network administrators, as well as diminishing the performance of the system [38]. The region below the ROC curve (AUC) is a measure of the classification performance in quantitative terms. A large AUC indicates that the model will always attribute larger probability scores to malicious traffic than to normal traffic. This outcome underscores the applicability of the SVM-based models in assisting cybersecurity measures like intrusion detection and traffic monitoring in network administration practice. Regarding the network security status, the ROC analysis proves that the inclusion of machine learning-based detection mechanisms contributes to the improvement of proactive detection of cyber threats [39]. Administrators can also balance the rate of detection and false alarms by the ability to change the decision thresholds according to operational needs. The analysis of the ROC curves shows that the SVM model could be trusted in terms of performance when it is used to identify malicious behavior, which supports its use as an effective tool of cybersecurity that could help to secure the information systems of computers in the dynamic network world.

Precision recall curve analysis of the better SVM intrusion detection model

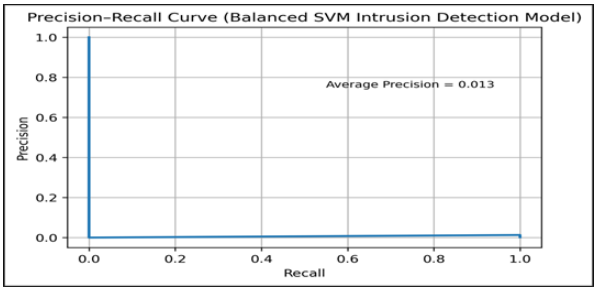

Figure 8. Precision-recall curve with better performance of the SVM intrusion detector.

The precision-recall curve of the enhanced SVM based intrusion detector model trained on the NF-UNSW-NB15-V2 dataset is shown in Figure 8. Precision recall curve is of special interest in measuring model performance where there is a large imbalance in the data, such as when malicious traffic forms a small portion of overall network traffic. As opposed to accuracy or ROC-based measures, this curve is centered on the trade-off between the sensitivity of detection and the reliability of prediction of the minority attack class. The curve shows the SVM model is very precise at low recall rates, meaning that when the model detects traffic as malicious, it is likely to be accurate. This is good practice in any operational network environment, since the operation of such a network environment is less prone to false alarms, and it also helps in reducing the load on the network administrators. Precision, which is the probability that a particular tag will be correct, decreases slowly as recall increases, as it becomes harder and harder to detect all the malicious cases without adding false positives. This tendency is likely in the case of realistic intrusion detection and becomes a problem of detecting rare events of attacks [40]. The mean value of precision displayed in the figure presents a numerical description of the performance of the model at all decision levels. The overall accuracy is not that high because there is an imbalance between the classes, but it proves that the model can accurately differentiate malicious traffic and normal traffic compared to random classification. Cybersecurity control-wise, this analysis would favor the combination of machine learning-based detection with adaptive thresholding and administrative control. In general, the analysis of the precision-recall curves indicates that the enhanced SVM model offers meaningful intrusion detection features in realistic network settings that support the significance of data-driven cybersecurity controls in network administration practices.

F1- Score and recall analysis of the SVM-based intrusion detection model

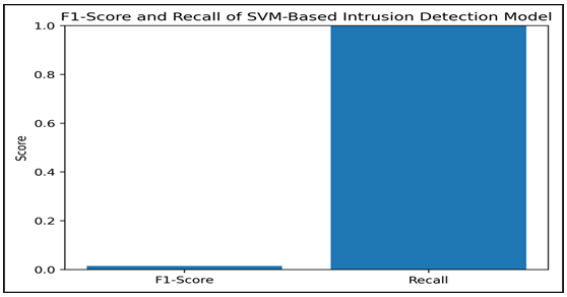

Figure 8. F1-score and recall figures that measure the effectiveness of SVM intrusion detection.

Figure 9 illustrates the values of F1-score and recall of an intrusion detection model based on the SVM and built on the NF-UNSW-NB15-V2 dataset. These performance measures present a brief explanation of how well the model detects malicious network traffic and also balances between prediction accuracy and sensitivity. The F1-score integrates precision and recall in addition to accuracy, which means that it is more accurate in assessing the performance of the model in case of class imbalance. Recall metric indicates how well the model can detect malicious traffic cases. A larger value of the recall is important to show that the intrusion detection model is effective in capturing a large percentage of attack events, and this is important in reducing the occurrence of threats that have not been detected in real operational network environments. Nevertheless, maximizing recall can maximize false positives, and it is important to use recall together with other measures of evaluation. The F1 score gives an understanding of the trade-off between the precision and the recall. The F1-score that was observed shows that SVM model has balanced detection ability, the model does not incorrectly label normal traffic as malicious traffic. Balance is especially vital to network administrators, as it will assist in effective security monitoring and reduce unnecessary alerting and operational overheads [41]. The F1-score, in conjunction with the recall analysis, indicates that the SVM model is appropriate to be implemented into the network administration practice in

https://doi.org/10.61577/jmla.2025.100010

terms of cybersecurity controls. These findings indicate that composite measures of evaluation should be used in determining the performance of intrusion detection in a realistic manner. On the whole, the analysis shows that the SVM-based model can be effectively and confidently used in improving the detection of threats, improving cybersecurity measures, and protecting computer-based information systems in dynamic network environments.

Discussion Analysis

Network traffic characteristics analysis

Network traffic characteristics analysis gives a basic understanding of the normal and malicious behavior manifestation in operational networks. The measured distribution of protocols shows that network communication is characterized by a small set of widely-used protocols, which are typical patterns of enterprise usage [43]. This kind of concentration is a sign that predictable communication behavior can be observed in normal conditions, and this is necessary to create baseline network profiles. Nevertheless, it is also the basis for vulnerability to attackers hiding malicious activity amid legitimate-appearing traffic, making it essential to monitor continuously. The analysis of the traffic volume and packet flow also indicates that the majsority of network interactions are characterized by low data volumes and few data packet exchanges [45]. Such attributes are common in normal processes like service requests, acknowledgments, and control signaling. Conversely, the existence of the high-volume and the high-packet outliers implies that there is a deviation from what is expected. Such deviations can be attributed to allowable bulk transfer, but can equally be an indication of machete actions like scanning, flooding, or data exfiltration actions. In network administration terms, the knowledge of these traffic peculiarities is essential to take proper cybersecurity measures. Setting normal traffic baselines helps administrators to place false positives at a minimum and identify anomalies more precisely [46]. The findings affirm that measures of traffic such as protocol usage, volume of bytes, and packet flow are useful measures to detect deviant behavior. In general, the discussion highlights the significance of incorporating the concept of traffic characterization into daily network management to facilitate proactive security surveillance and decision-making.

Implication of class imbalance of intrusion detection

The normal and malicious traffic distribution demonstrates a high level of class imbalance, which is a typical feature of a real-world network context. The normal traffic is the greatest part of network flows, and malicious activities are rare but extremely dangerous. This imbalance is a significant issue for intrusion detection systems because a model trained on this kind of data can be biased towards the majority, as a result of which it can detect fewer attacks. The findings indicate that the conventional performance measures, like accuracy, may be deceptive in asymmetrical situations [47]. An example of this is a model that can be highly accurate in terms of its ability to characterize normal traffic, but is not able to identify a significant fraction of malicious behavior. Thus, to assess intrusion detection systems, metrics should focus on the minority classes so that they highlight the performance of recall, precision, F1- score, and the precision-recall curves. An administrative perspective involves identifying imbalances in classes to choose appropriate detection and evaluation trategies [48]. The results indicate that the security controls based on data should be well structured to ensure a balance between the sensitivity of the detection and the false alarms. The effects of imbalance can be alleviated by using techniques like threshold tuning, class weighting, and complementary monitoring mechanisms. This discussion supports the necessity of dynamic and situational cybersecurity controls that consider the spatial imbalance in attack event occurrences in working networks.

Intrusion detection with SVM-based detection

The SVM-based intrusion detection model shows a high ability to identify normal and malicious traffic patterns. The results of the confusion matrix show that the classification of legitimate network activity is highly accurate, and this is essential in reducing the false positives and ensuring that the network does not get slowed down. Simultaneously, the occurrence of false positives among the cases of the attacks indicates the very problematic nature of identifying the presence of subtle or unusual malicious behaviors. The analysis of the ROC curve proves that the SVM model can be effectively used to discriminate between a variety of decision thresholds [48]. A high difference between the actual positive and false positive ratios shows that the model can be used to provide real-time intrusion detection in different operational conditions. But ROC analysis is an incomplete measure of performance in the case of class imbalance, which requires supporting evaluation statistical measures [49]. The findings indicate that SVM-based detection can be an effective cybersecurity control when embedded in the network administration procedures. It is appropriate to analyze high-dimensional network traffic data due to its capabilities of modelling complex boundaries of decisions. However, the model should be continuously tuned and combined with administrative controls to remain effective as network conditions and attack patterns change.

Precision-recall and f1-score analysis insights

The precision-recall analysis will help to gain more insight into the performance of the intrusion detection model in the imbalanced network environment. The noted trade-off between precision and recall is an indication of how difficult it is to increase the attacks detected and decrease false alarms [44]. Such high accuracy on low recall means that the model is accurate in detecting malicious traffic, but as recall rises, more false positives come about. F1-score is also a balanced score, and in this case, both the precision and recall are merged together to form a single measurement [50]. The findings indicate that the SVM model can strike a decent balance, which implies that the SVM model can adequately identify malicious traffic without being too disruptive to the normal operation of the network. Such a balance is especially relevant to network administrators, who have to maintain security alerts as well as performance and availability concerns. Regarding the control aspect of cybersecurity, these metrics state the need to evaluate on a multi-dimensional basis. Using only one performance measure can be inadequate to conclude on system effectiveness [51]. The results indicate that precision-recall and F1-score tests are critical to the evaluation of the intrusion detection performance in the real world and threshold choice in practical implementations.

Implementation of cybersecurity controls in network management

The findings all lead to the conclusion that a combination of cybersecurity measures and controls directly implemented in network management is highly valuable. The use of traffic characterization, anomaly detection, and machine learning-

https://doi.org/10.61577/jmla.2025.100010

based intrusion detection complements each other in offering security layers that strengthen the overall security of the system. When integrated into regular administration processes, these controls enable organizations to stop living in a reactive mode of security measures and shift to a proactive system of threat management [48]. Network administrators get the advantage of real-time monitoring of the traffic behavior and hence respond more quickly to possible threats. Combining the analytical models enables automated monitoring and enables the administrators to modify the policies and thresholds according to the operational requirements [49]. This interdependence between the automation and human monitoring enhances security without affecting the network performance. The results indicate that technical solutions are not sufficient, but procedural alignment is needed to achieve a successful integration. Security monitoring cannot be regarded as an independent operation but as an administrative task. This combined method improves situational awareness and enables situational cybersecurity improvement.

Practical and research implications

The discussion shows some practical and research implications of incorporating cybersecurity controls into network administration. In practice, the findings indicate that data-driven analysis can be highly effective in detecting threats and contributing to inform decision-making [50]. Similar practices can help organizations to be more visible, respond faster, and enhance their resiliency in case of cyber threats. In terms of research, it can be noted that the results are particularly important as they support the use of realistic datasets and evaluation metrics that are responsive to the real-life conditions of operations [51]. The future research can be focused on hybrid models, a sophisticated feature engineering process, or adaptive learning methods to enhance the detection effectiveness further. Further, multi-class attack classification and real-time deployment application may be of interest under analysis [52]. On the whole, the current research can be added to the comprehension of cybersecurity controls, which can be efficiently incorporated into network management practices. The findings support the argument of machine learning and traffic analysis in protecting computer information systems, which will offer research goals in network security in future studies.

Future Work

The fact that this work has proven the efficiency of the combination of cybersecurity controls with network administration practice based on data-driven intrusion detection, there are a number of prospects for further research and improvement [53]. The extension of the suggested method of intrusion detection to multi-classes is one of the directions. Although the present research has concentrated on binary classification of normal and malicious traffic, future research is able to investigate finer-grained classification of the various types of attacks [54]. This would give more insight on the actions of attacks and would be able to carry out more specific security responses. The other area that can be used in future work is the incorporation of more machine learning and deep learning models. Sophisticated models like ensemble learning, neural networks, and hybrid frameworks of detection may be assessed and contrasted against the existing model in order to enhance the detection accuracy and strength [55]. These techniques can be more effective in capturing complicated and changing patterns of attacks in huge networks. The deployment and evaluation of intrusion detection systems in real-time, on an operational network environment, can also be a topic of research in the future. Application of the suggested framework in the live network environment would enable measurement of scalability, latency, and resource usage [56]. This kind of evaluation is essential in the realization of the performance of integrated cybersecurity controls in dynamic traffic environments and operational conditions [57]. Also, an extension by adding adaptive and automated response mechanisms is significant. Future systems would be able to detect threats in addition to automatically initiating mitigation measures like traffic filtering, access control updates or alert prioritization. This would further save on the response times and provide better proactive security management. The use of other sources of data, including system logs, data on user behavior, and data on endpoint security, is another possible direction. By integrating various sources of data, situational awareness and the number of false positives might be reduced, as network events may be cross-linked with host-level activity [58]. Lastly, the emerging threat landscapes can be resolved in the future through the introduction of continuous learning and model updating mechanisms into the future work. Due to changing attack patterns with time, adaptive models with learning capabilities can ensure effectiveness in detection. All these future research directions are meant to reinforce the incorporation of cybersecurity controls within the network administration and increase the long-term security of computer information systems.

Conclusion

This study analyzed how cybersecurity controls can be applied to network management procedures to improve the security of computer information systems. The research presents how proactive security mechanisms can be incorporated into daily administration through the analysis of real-life network traffic, demonstrating that a data-driven approach enables the integration of proactive security measures into everyday operations. The NF-UNSW-NB15-V2 dataset allowed realistic assessment of network behavior without compromising operational environments. Through detailed traffic analysis, the study highlights the importance of understanding protocol usage, traffic volume, and packet flow patterns to define baseline network behavior. These insights help optimize anomaly detection and support informed security decisions. A SVM–based intrusion detection model further confirms the effectiveness of machine learning in identifying malicious traffic. Performance evaluation using multiple metrics, including confusion matrix, ROC curve, precision-recall analysis, F1-score, and recall, provides a comprehensive assessment of detection capability, particularly under class imbalance conditions. The results show that integrating cybersecurity controls into network administration improves early threat detection, reduces reliance on reactive security mechanisms, and enhances overall system security. The study emphasizes that security should be an integral part of network management rather than a separate function. Data preprocessing, feature selection, and continuous monitoring are critical for effective implementation. Although limited by the use of a single dataset and offline evaluation, the proposed framework remains significant and highlights opportunities for further development. This research contributes to understanding how data-driven cybersecurity controls can be effectively adapted to network administration practices, helping build more secure, adaptive, and resilient computer information systems.

Disclosure Statement

No potential conflict of interest was reported by the author.

https://doi.org/10.61577/jmla.2025.100010

References

1. Kidman N. Cybersecurity in management information systems: challenges and best practices for data protection. J Manag Inf Syst. 2025;1(1):1-11. Available at: https://integratif.net/index.php/Integratif/article/view/2
2. Ajiga D, Okeleke PA, Folorunsho SO, Ezeigweneme C. Designing cybersecurity measures for enterprise software applications to protect data integrity. Comput Sci IT Res J. 2024;5(8):1920-1941. https://doi.org/10.51594/csitrj.v5i8.1451
3. Folorunso A. Cybersecurity and its global applicability to decision making: a comprehensive approach in the university system. 2024. https://doi.org/10.2139/ssrn.4955601
4. Folorunso A, Mohammed V, Wada I, Samuel B. The impact of ISO security standards on enhancing cybersecurity posture in organizations. World J Adv Res Rev. 2024;24(1):2582-2595. https://doi.org/10.30574/wjarr.2024.24.1.3169
5. Folorunso A, Wada I, Samuel B, Mohammed V. Security compliance and its implications for cybersecurity. World J Adv Res Rev. 2024;24(01):2105-2121. https://doi.org/10.30574/wjarr.2024.24.1.3170
6. Atakari C. A deep learning-based security model for ERP-integrated IoT in national defense manufacturing environments. Int J Emerg Trends Comput Sci Inf Technol. 2024;5(3):90-98. https://doi.org/10.63282/3050-9246.IJETCSIT-V5I3P109
7. Atakari C. A multi-layered cybersecurity model for erp systems supporting national critical infrastructure: threats, challenges, and solutionsInt. J Emerg Trends Comput Sci Inf Technol. 2024;5(1):94-101. https://doi.org/10.63282/3050-9246.ijetcsit-v5i1p110
8. Dalal A. Implementing robust cybersecurity strategies for safeguarding critical infrastructure and enterprise networks. Int J Manag Technol Eng. 2024.
9. Hosam O, Abousamra R, Hassouna M, Azzawi R. Security analysis and planning for enterprise networks: incorporating modern security design principles. Ind 4.0 Key Technol Adv Des Princ Eng Educ Bus Soc Appl. 2024:85-117. https://doi.org/10.1201/9781003343332-5
10. Nurwanah A. Cybersecurity in accounting information systems: challenges and solutions. Adv Appl Account Res. 2024;2(3):157-168. https://doi.org/10.60079/aaar.v2i3.336
11. Ige AB, Kupa E, Ilori O. Best practices in cybersecurity for green building management systems: protecting sustainable infrastructure from cyber threats. Int J Sci Res Arch. 2024;12(1):2960-2977. https://doi.org/10.30574/ijsra.2024.12.1.1185
12. Stewart EM, Morgan JC, Woodruff NL, Combe G, Stolworthy RV. Enhancing cloud cybersecurity: prescriptive controls for operational technology. Idaho National Laboratory (INL), Idaho Falls, ID (United States); 2024. https://doi.org/10.2172/2474851
13. Mahmood HS, Abdulqader DM, Abdullah RM, Rasheed H, Ismael ZN, Sami TM. Conducting in-depth analysis of AI, IoT, web technology, cloud computing, and enterprise systems integration for enhancing data security and governance to promote sustainable business practices. J Inf Technol Inform. 2024;3(2):297-332.
14. Joy ZH, Islam S, Rahaman MA, Haque MN. Advanced cybersecurity protocols for securing data management systems in industrial and healthcare environments. Glob Mainstr J Bus Econ Dev Proj Manag. 2024;3(4):25-38. https://doi.org/10.62304/jbedpm.v3i4.147
15. Mayeke NR, Arigbabu AT, Olaniyi OO, Okunleye OJ, Adigwe CS. Evolving access control paradigms: a comprehensive multi-dimensional analysis of security risks and system assurance in cyber engineering. Asian J Res Comput Sci. 2024;17(5):108-124. https://doi.org/10.9734/ajrcos/2024/v17i5442
16. Ajayi OO, Alozie CE, Abieba OA. Enhancing cybersecurity in energy infrastructure: strategies for safeguarding critical systems in the digital age. Trends Renew Energy. 2025;11(2):201-212. https://doi.org/10.17737/tre.2025.11.2.00192
17. Ogborigbo JC, Sobowale OS, Amienwalen EI, Owoade Y, Samson AT, Egerson J. Strategic integration of cyber security in business intelligence systems for data protection and competitive advantage. World J Adv Res Rev. 2024;23(1):81-96. https://doi.org/10.30574/wjarr.2024.23.1.1900
18. Pillai SE, Polimetla K. Integrating network security into software defined networking (SDN) architectures. Proc. 2024 Int Conf Integr Circuits Commun Syst (ICICACS). 2024:1-6. https://doi.org/10.1109/icicacs60521.2024.10498703
19. Shafa H, Islam A. Impact of data privacy and cybersecurity in accounting information systems on financial transparency. Int J Sci Interdiscip Res. 2025;6(1):254-292. https://doi.org/10.63125/xs0xt970
20. Shen Q, Shen Y. Endpoint security reinforcement via integrated zero-trust systems: a collaborative approach. Comput. Secur. 2024;136:103537. https://doi.org/10.1016/j.cose.2023.103537
21. Ali T, Al-Khalidi M, Al-Zaidi R. Information security risk assessment methods in cloud computing: comprehensive review. J Comput Inf Syst. 2026;66(1):123-150. https://doi.org/10.1080/08874417.2024.2329985
22. Kim Y, Sohn SG, Kim KT, Jeon HS, Lee SM, Lee Y, et al. Exploring effective zero trust architecture for defense cybersecurity: a study. KSII Trans Internet Inf Syst. 2024;18(9). https://doi.org/10.3837/tiis.2024.09.011
23. Odimarha AC, Ayodeji SA, Abaku EA. Securing the digital supply chain: cybersecurity best practices for logistics and shipping companies. World J Adv Sci Technol. 2024;5(1):26-30. https://doi.org/10.53346/wjast.2024.5.1.0030
24. Malasowe BO, Aghware FO, Okpor MD, Edim EB. Techniques and best practices for handling cybersecurity risks in educational technology environment (EdTech). Sci Technol Res. 2024;6(2). https://doi.org/10.5281/zenodo.12617068
25. Lokare A, Bankar S, Mhaske P. Integrating cybersecurity frameworks into it security: a comprehensive analysis of threat mitigation strategies and adaptive technologies. arXiv preprint arXiv. 2025. https://doi.org/10.48550/arxiv.2502.00651
26. Bello AJ, Diyan M, Asghar I. Zero trust implementation for legacy systems using dynamic microsegmentation, role-based access control (RBAC), and attribute-based access control (ABAC). Proc 4th Int Conf Comput Inf Technol (ICCIT), 2025:181-189. https://doi.org/10.1109/ICCIT63348.2025.10989392
27. Balisane H, Egho-Promise E, Lyada E, Aina F, Sangodoyin A, Kure H. The effectiveness of a comprehensive threat mitigation framework in networking: a multi-layered approach to cyber security. Int Res J Comput Sci. 2024;11(06):529-538. https://doi.org/10.26562/irjcs.2024.v1106.03

https://doi.org/10.61577/jmla.2025.100010

28. Kumar S, Vardhan H. Cyber security of OT networks: a tutorial and overview. arXiv e-prints. 2025:2502. https://doi.org/10.48550/arxiv.2502.14017
29. Egho-Promise E, Lyada E, Aina F. Towards improved vulnerability management in digital environments: a comprehensive framework for cyber security enhancement. Int Res J Comput Sci. 2024;11(05):441-449. https://doi.org/10.26562/irjcs.2024.v1105.01
30. Pigola A, de Souza Meirelles F. Unraveling trust management in cybersecurity: insights from a systematic literature review. Inf Technol Manag. 2024:1-23. https://doi.org/10.1007/s10799-024-00438-x
31. Shamsuzzaman HM, Mosleuzzaman MD, Mia A, Nandi A. Cybersecurity risk mitigation in industrial control systems analyzing physical hybrid and virtual test bed applications. Acad J Artif Intell Mach Learn Data Sci Manag Inf Syst. 2024;1(1):19-39. https://doi.org/10.69593/ajaimldsmis.v1i01.123
32. Aftabi N, Moradi N, Mahroo F, Kianfar F. SD-ABM-ISM: an integrated system dynamics and agent-based modeling framework for information security management in complex information systems with multi-actor threat dynamics. Expert Syst Appl. 2025;263:125681. https://doi.org/10.1016/j.eswa.2024.125681
33. Ohri P, Daniel A, Neogi SG, Muttoo SK. Blockchain-based security framework for mitigating network attacks in a multi-SDN controller environment. Int J Inf Technol. 2025;17(9):5591-5603. https://doi.org/10.1007/s41870-024-01933-8
34. Olaniyi OO, Omogoroye OO, Olaniyi FG, Alao AI, Oladoyinbo TO. CyberFusion protocols: strategic integration of enterprise risk management, ISO 27001, and mobile forensics for advanced digital security in the modern business ecosystem. J Eng Res Rep. 2024;26(6):31-49. https://doi.org/10.9734/jerr/2024/v26i61160
35. Syed AA. Zero trust security in hybrid cloud environments: implementing and evaluating zero trust architectures in aws and on-premise data centers. Int J Emerg Trends Comput Sci Inf Technol. 2024;5(2):42-52. https://doi.org/10.63282/3050-9246.ijetcsit-v5i2p105
36. Achuthan K, Sankaran S, Roy S, Raman R. Integrating sustainability into cybersecurity: insights from machine learning based topic modeling. Discover Sustain. 2025;6(1):44. https://doi.org/10.1007/s43621-024-00754-w
37. Joel MO, Chibunna UB, Daraojimba AI. Cyber cloud framework: integrating cyber security resilience into cloud infrastructure optimization for enhanced operational efficiency. Int J Multidiscip Res Growth Eval. 2024 ;5(1):1378-1382. https://doi.org/10.54660/.ijmrge.2024.5.1.1378-1382
38. Admass WS, Munaye YY, Diro AA. Cyber security: state of the art, challenges and future directions. Cyber Secur Appl. 2024;2:100031. https://doi.org/10.1016/j.csa.2023.100031
39. Patel R, Müller K, Kvirkvelia G, Smith J, Wilson E. Zero trust security architecture raises the future paradigm in information systems. Inform Digit Insight J. 2024;1(1):24-34. Available at: https://firstcierapublisher.com/index.php/Informatica/article/view/77
40. Iftikhar U, Rashid H, Attaullah HM. Future emerging challenges and innovations in next gen-cybersecurity and information systems security. Emerg Trends Inf Syst Secur Using AI Data Sci Next-Gen Cyber Anal 2025:173-203. https://doi.org/10.1007/978-3-031-81481-5_12
41. Pasdar A, Koroniotis N, Keshk M, Moustafa N, Tari Z. Cybersecurity solutions and techniques for internet of things integration in combat systems. IEEE Trans Sustain Comput. 2024 ;10(2):345-365. https://doi.org/10.1109/tsusc.2024.3443256
42. Hasan MY, Alam MB, Ferdawsi S, Huq AE. Nonlinear dynamics in export payment risk: a gradient boosting and shap-based explainable ai model. J Econ Bus Commer. 2025;2(2):280-287. https://doi.org/10.69739/jebc.v2i2.1218
43. Sivakumar J, Salman NR, Salman FR, Salimova HR, Ghimire E. AI-driven cyber threat detection: enhancing security through intelligent engineering systems. J Inf Syst Eng Manag. 2025;10(19):790-798. https://doi.org/10.52783/jisem.v10i19s.3116
44. Hasan MY, Ferdawsi S. AI-driven predictive modeling of export bill settlement: analyzing importer country, bank, and payment behavior. Res J Bus Econ. 2025;3(3):29-41. https://doi.org/10.61424/rjbe.v3i3.532
45. Kuforiji J. The importance of integrating security education into university curricula and professional certifications. Int J Technol Manag Humanit. 2025;11(03):1-10. https://doi.org/10.21590/ijtmh.11.0301
46. Nkambule M, van Vuuren JJ, Leenen L. Integrating enterprise architecture into cybersecurity risk management in higher education. Proc Int Conf Cyber Warf Secur. 2024:501-510. https://doi.org/10.34190/iccws.19.1.2189
47. Radanliev P. Integrated cybersecurity for metaverse systems operating with artificial intelligence, blockchains, and cloud computing. Front Blockchain. 2024;7:1359130. https://doi.org/10.3389/fbloc.2024.1359130
48. Mathew AJ. Unscripted practices for uncertain events: organizational problems in cybersecurity incident management. Sci Technol Hum Values. 2024;49(4):827-850. https://doi.org/10.1177/01622439241240411
49. Wang W, Sadjadi SM, Rishe N. A survey of major cybersecurity compliance frameworks. Proc IEEE 10th Conf. Big Data Secur. Cloud 2024:23-34. https://doi.org/10.1109/bigdatasecurity62737.2024.00013
50. Zangana H, Ali NY, Bazeed SM, Abdullah DT. Leveraging automation and traceability in managing changes to mission-critical computer systems. Indones. J Educ Soc Sci. 2025;4(1):176-189. https://doi.org/10.56916/ijess.v4i1.1016
51. Hnaif AA, Derbas AM, Almanasra S, Hnaif A. Cybersecurity integration in distance learning: an analysis of student awareness and attitudes. Indones. J Electr Eng Comput Sci. 2024;33(2):1057-1066. https://doi.org/10.11591/ijeecs.v33.i2.pp1057-1066
52. Far AZ, Far MZ, Gharibzadeh S, Naeini HK, Amini L, Zangeneh S, et al. Artificial intelligence for secured information systems in smart cities: collaborative IoT computing with deep reinforcement learning and blockchain. arXiv preprint arXiv. 2024. https://doi.org/10.48550/arxiv.2409.16444
53. Santander Moreno JJ, Ortega Matoma JA, Dávila Castillo MR, Ordóñez Sarchi JA. A neutrosophic framework for evaluating security measures in information systems. J Fuzzy Extens Appl. 2024;5:12-24. https://doi.org/10.22105/jfea.2024.468184.1546
54. Falco G, Boschetti N, Viswanathan A, Bailey B, Maple C, Kurt GK, et al. Minimum requirements for space system cybersecurity-ensuring cyber access to space. Proc IEEE 10th Int Conf Space Mission Chall Inf Technol. 2024:78-88. https://doi.org/10.1109/smc-it61443.2024.00016

https://doi.org/10.61577/jmla.2025.100010

55. Zanasi C, Russo S, Colajanni M. Flexible zero trust architecture for the cybersecurity of industrial IoT infrastructures. Ad Hoc Netw. 2024;156:103414. https://doi.org/10.1016/j.adhoc.2024.103414

56. Ajish D. The significance of artificial intelligence in zero trust technologies: a comprehensive review. J Electr Syst Inf Technol. 2024;11(1):30. https://doi.org/10.1186/s43067-024-00155-z

57. Faruq MO. A meta-analysis of cybersecurity framework integration in GRC platforms: evidence from US enterprise audits. J Sustain Dev Policy. 2025;1(01):224-249. https://doi.org/10.63125/kwhkmb57

58. de Azambuja AJ, Giese T, Schützer K, Anderl R, Schleich B, Almeida VR. Digital twins in industry 4.0–opportunities and challenges related to cyber security. Procedia Cirp. 2024;121:25-30. https://doi.org/10.1016/j.procir.2023.09.225

https://doi.org/10.61577/jmla.2025.100010