Journal of Robotics and Control (JRC)
Volume 5, Issue 5, 2024
ISSN: 2715-5072, DOI: 10.18196/jrc.v5i5.22508

Optimizing Network Security with Machine Learning and Multi-Factor Authentication for Enhanced Intrusion Detection

Rafah Kareem Mahmood [1], Ans Ibrahim Mahameed [2], Noor Q. Lateef [3], Hasanain M. Jasim [4], Ahmed Dheyaa Radhi [5], Saadaldeen Rashid Ahmed [6*], Priyanka Tupe-Waghmare [7]
[1, 3] Electromechanical Engineering Department, University of Technology, Baghdad, Iraq
[2] Department of Mathematics, College of Education for Pure Sciences, Tikrit University, Tikrit, Iraq
[4] Construction and Projects Department, University of Technology, Baghdad, Iraq
[5] College of Pharmacy, University of Al-Ameed, Karbala PO Box 198, Iraq
[6] Computer Science Department, Bayan University, Erbil, Kurdistan, Iraq
[6] Artificial Intelligence Engineering Department, College of Engineering, Al-Ayen University, Thi-Qar, Iraq
[7] Symbiosis Institute of Technology, Pune, Symbiosis International (Deemed University), India
Email: [1] 50150@uotechnology.edu.iq, [2] anas.ibrahim@tu.edu.iq, [3] noor.q.lateef@uotechnology.edu.iq, [4] hasanain.m.jasim@uotechnology.edu.iq, [6] saadaldeen.aljanabi@bnu.edu.iq, [7] priyanka.tupe@sitpune.edu.in
*Corresponding Author

***Abstract*—This study examines the utilization of machine learning methodologies and multi-factor authentication (MFA) to bolster network security, specifically targeting network intrusion detection. We analyze the way in which the integration of these technologies effectively tackles existing security concerns and constraints. The research highlights the importance of incorporating energy conservation and environmental impact reduction into security solutions, in addition to traditional cryptography and biometric methods. In addition, we tackle the limitations of centralized systems, such as vulnerabilities to security breaches and instances of system failures. The study examines different security models, encompassing categories, frameworks, consensus protocols, applications, services, and deployment goals in order to determine their impact on network security. In addition, we offer a detailed comparison of seven machine learning models, showcasing their effectiveness in enhancing network intrusion detection and overall security. The objective of this study is to provide in-depth understanding and actionable suggestions for utilizing machine learning with MFA (Multi-Factor Authentication) to enhance network defensive tactics.**

***Keywords*—Deep Learning; Network Security; Multi-Factor Authentication; Network Intrusion Detection; Machine Learning.**

I. INTRODUCTION

Energy in an era of extraordinary technological interconnection and a rising dependence on the networks of networks, the problem of information security and situational awareness, which is simple and unambiguous, has never been more vital than today. The rise of infinite cybersecurity threats and unique methods of conducting malicious activities has gradually challenged the assumptions of old approaches to security. The objective of this research is to deal with this crucial issue through a complete analysis of employing machine learning coupled with the integration and creation of multi-factor authentication solutions that can protect network activity through the coherence of various studies by specialists.

The cutting-edge network security environment is defined by a continual transition where bad actors are fast to adapt, and they blow through possibilities, such as data breaches and cyber threats, that develop as they painstakingly exploit flaws to obtain unauthorized access to systems. Traditional authentication solutions such as password-based systems find hackers' efforts reduced but not totally halted in recent years; consequently, a new approach to the way we offer security for our systems should be devised [2]. While going beyond typical security methods, this study focuses on uncovering the unique. UV-ray ways that include ML technologies, multi-factor authentication, and the network intrusion detection system [3] to enhance the system and make it more dynamic and responsive.

This study inquiry has significant importance away from gadgetry as it reflects on a vital societal problem. Nowadays, cybersecurity breaches may happen anywhere and at any level (personal data, companies 'assets, or vital infrastructure). So, the effects of these catastrophes may be extensive and harm people, businesses, and even countries. Thus, such instances should highlight the strong requirement for the creation of security measures that adequately address the problems resulting from the combined danger of cyberattacks. Through the study of the convergence of machine learning and multi-factor authentication, this article sets the purpose of making it feasible to deploy additional methods of protection against the wide and sophisticated cybersecurity threats happening in today's network environment [5].

In an era of unparalleled technological interconnectedness and a developing dependence on networks, the problem of information security and situational awareness has never been more vital. The rise of cybersecurity threats and creative techniques of executing harmful actions has gradually challenged the assumptions of classic security methodologies. This research addresses this essential issue through a complete investigation of applying machine learning along with the integration and implementation of multi-factor authentication systems to protect network activities. The purpose is to bring

together numerous studies by specialists to better network security.

The contemporary network security environment is characterized by continual evolution, with adversaries quickly adapting and exploiting weaknesses to obtain unauthorized access to systems. Traditional authentication mechanisms, such as password-based systems, have been shown to be insufficient against sophisticated attackers. This study intends to go beyond conventional security methods by examining unique approaches that merge machine learning technology, multi-factor authentication, and advanced network intrusion detection systems to provide a more dynamic and responsive security framework.

The major challenge, which is directly connected to the solution addressed in this article, is the quest for a real-time and flexible cyber security system that has the potential to take preventative actions against varied cyber-attacks. Although, in theory, a traditional security strategy should be able to keep track of evolving threats, rivals in this area often develop their damaging tactics at a quicker speed, resulting in loopholes that hackers may readily exploit. Multi-factor authentication, effective network intrusion detection, and machine learning methods as a tipping point illustrate that they are a crucial solution for cyber risk since they are based on data-driven information, which increases security [7]. We characterize this research as a study into the synergistic impacts of integrated system components that make the network at least three times stronger against illegal access, data leakage, and any cyber security fightbacks.

This study effort centers on a multidimensional examination of machine learning, multi-factor authentication, and network intrusion detection inside the network security sector, which is among those components [9]. This complex investigation includes:

Machine Learning in Security: In this part, we will fully study machine learning algorithms, including their potential to uncover patterns, detect irregularities, and, ultimately, strengthen security systems [10].

Multi-Factor Authentication Landscape: The examination of various ways of multi-factor authentication techniques such as biometrics, token-based systems, and knowledge-based authentication and analyzing their applicability for diverse network contexts comes under discussion.

Intrusion Detection Advancements: An examination of modern-day intrusion detection systems, especially those strengthened by machine learning, to accomplish this duty correctly and predictively before any cyberattack proceeds [12].

Optimization: The evaluation will be done on the effects of merging machine learning and multi-factor authentication on network security in the areas of being effective, having a low rate of false positives, and enhancing the user experience [13].

Real-world Application: A practical assessment of these consolidated methodologies within several real-life scenarios, such as the Internet of Things, networks with smart communications, and vehicle communication [14].

A. Motivation

The inspirations driving this study care about the following security paradigm: a network that is stronger and more adaptive [15]. The persistent nature of cyber-attacks poses another obstacle to establishing robust solutions against cybersecurity risks; creative, resilient solutions should be able to respond dynamically, which in turn would prevent unauthorized access and wicked acts like data leaks. Because of the rise of linked devices and the increased complexity of hostile actors, old-fashioned security fence efforts are not able to defend our important digital resources sufficiently. The need is clear: the cyber security community must be ready to seek out new technologies and methodologies and strive to do all that is possible to remain ahead of the ever-developing threat environment.

The security problems and cryptocurrency-related assaults that happened in the past were defined by the exploitation of conventional authentication techniques (password-based systems), with their obvious shortcomings being disclosed. Notwithstanding, the growth of a digital ecosystem structure, which incorporates everything from IoT devices to smart networks, is longer accompanied by the demand for a comprehensive approach to the network protection system that is progressive, adaptable, and intellectual.

Because we are going to work hard on this study, we are going to combat these difficulties head-on. The engagement of machine learning-driven multi-factor authentication approaches in networking may be a turning point that leads to the era of more efficient armaments and the protection of all essential digital assets [16]. Here I, consequently, propose to build new, flexible security ideas that are daringly self-learning and able to forecast and combat harmful cyber attackers' tools; this will, in the end, boost the trustworthiness and dependability of individuals, institutions, and societies in the digital sphere.

The originality of this research resides in its comprehensive approach to strengthening network security through the use of machine learning, multi-factor authentication, and improved intrusion detection systems. While earlier studies have studied these technologies individually, this research provides a novel framework that synergistically combines these parts to build a more resilient security solution.

Specifically, the research brings the following novel contributions:

- Integrated Security Framework: The study provides a new model that blends machine learning techniques with multi-factor authentication and intrusion detection systems to deliver a comprehensive security solution.
- Enhanced Threat Detection: By employing modern machine learning approaches, including deep learning architectures such as CNN and BiLSTM, the research boosts the accuracy and effectiveness of threat detection and response.
- Practical Application and Optimization: The research provides a detailed analysis of the integration's impact on real-world applications, including IoT networks and smart communication systems, and evaluates the optimization of

security measures to minimize false positives and improve user experience.

B. State of the Art in Network Intrusion Detection

The latest successes in network monitoring and malicious intrusion detection have been led by the developing trends and advancements in the cyber security area, as well as the fundamental expansion of the complexity of cyber threats. Intrusion detection solutions for IoT networks have evolved owing to the increasing attention of security professionals. They function virtually and are entrusted with overcoming numerous challenges connected to resource limits, the inhomogeneity of communication protocols, and the quirks of multiple attack surfaces. The dawn of deep learning architectures like CNN and LSTM has revealed a promise of excellent accuracy in addition to the efficiency of intrusion detection systems [60]. The integration of CNNs combined with BiLSTM in one step would be adequate to extract geographical and temporal elements of the network traffic data.

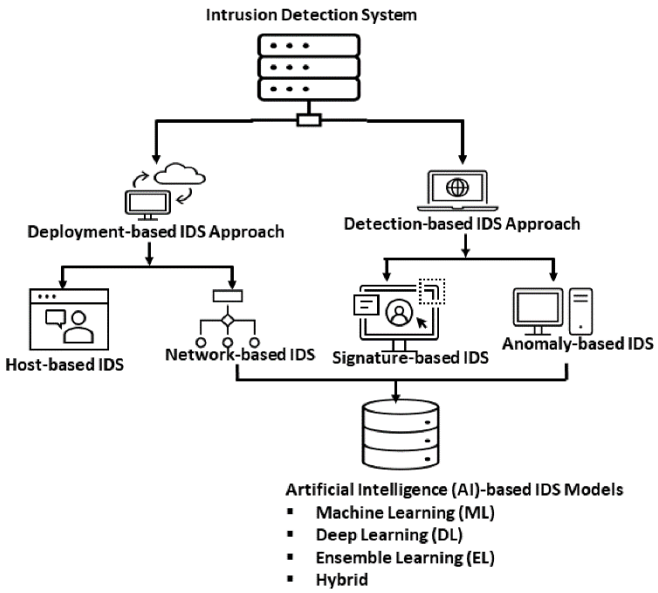


Fig. 1. Explainable Artificial Intelligence (XAI) for intrusion detection

In Fig. 1 the new machine learning model has replaced attentive human systems with a trustworthy blend of technologies, which makes intrusion detection more durable [61]. The models then acquire synergy from all these approaches—frequently, decision trees, support vector machines, and ensemble methods. The statistical analysis of benchmark data, such as the CIDDS-001 dataset [62], has also been integrated into that. Machine learning is recommended to aid in measuring the performance and efficiency of intrusion detection systems. displaying both the virtues and the shortcomings of ordinary existence. In intrusion detection via the emergence of artificial intelligence, more and more firms want explanatory AI (XAI) systems that subsequently may offer some form of clarity and explainable conclusions regarding the detection action [63]. XAI-based approaches aim at strengthening dependability and responsibility in the ADI systems by enabling stakeholders to find out (or see) the logic behind the results. Technologies have been reflecting contemporary situations, including software meant to identify metaverse incursions and face everlasting cyberattacks [64]. The algorithms utilized for the same utilize unique statistical approaches, which may recognize complicated attacks taking place in virtual situations.

C. Role of Multi Factor Authentication in Ensuring the Integrity of Networks

Multi-Factor Authentication (MFA) is an essential feature of network security, which may be done using numerous techniques, including passwords and ID stamps. provides a partnership merely beyond the standard password-based security safeguards. With the hashing algorithm, the same hash values are created despite modest modifications in transactions, making tracing difficult. As such, we may agree that MFA greatly increases overall security. protection against unlawful intrusion and many forms of data leakage [65]. One of the strengths of MFA (multi-factor authentication) is its capacity to combine numerous authentication components to confirm users' identification, like passwords and biometric tokens [67]. by using the authentication, he stressed at the core additional security problems [68].

Biometric authentication, like fingerprint scanning or facial recognition, is another extra component that makes identity verification safe and easy. utilizing genotypes to authenticate, for example, stepchildren, orphans, and adults [67]. Among the prominent security tokens are smart cards or mobile authenticator programs. One-time passwords (OTP) or digital signatures are to be produced. It may operate as extra protection by fundamentally requiring the total locking or accessing of the gadget with the approval of a trustworthy figure [67]. Moreover, other elements, such as location-based authentication or time-based authentication, not only make an MFA system more secure but also provide it with extra protection. employing these procedures, which provide extra difficulties for the adversary to develop assaults that can ever breach user accounts.

The findings of such experiments demonstrated that MFA is an efficient building block for strengthening the security of the network. guarding against digital attacks and irresponsible usage [65]. But at the same time, there are quite a few worries when talking about the usability aspect. implementation difficulty. and that p-hacking or a bigger incidence of incorrect classifications may occur, nonetheless. Despite the highlighted concerns, cybersecurity experts still gain a lot from MFA; thus, security system completeness without MFA does not appear to be a smart concept anymore [68].

D. Research Gap

Despite major breakthroughs in cybersecurity, some gaps continue in effectively countering the expanding threat landscape. Traditional security solutions often fail to keep pace with the rapid evolution of cyber threats, resulting in weaknesses that are quickly exploited by attackers. Existing research has thoroughly examined machine learning and multi-factor authentication independently; however, there is a paucity of comprehensive studies that integrate these technologies in a synergistic manner to enhance network security fully.

This study tackles these shortcomings by focusing on the combined use of machine learning and multi-factor authentication within a unified network security framework. The research attempts to bridge the existing gap by offering a

full examination of how various technologies might operate together to give powerful protection against cyber threats. The study also evaluates the success of this integrated strategy in real-world circumstances, revealing insights into its practical applicability and possible advantages.

E. Structure of Work

Through this article, I will develop a holistic text that will address machine learning driven multi-factor authentication approaches in the context of network security in a thorough way. The paper unfolds as follows: The paper unfolds as follows:

Introduction: This section, which presents the research topic and its necessity, the research problem, the objectives, the area of study, and the motivation, which has a comprehension of machine learning, multi-factor authentication, and network intrusion detection, will be for the optimum of network security.

Literature Review: Picking up on the concept that was given forth in the beginning, the study of the literature in this portion of the paper will be very detailed. It references major works done by Wang et al. [1][2], Alsarhan et al. [3], and others as part of a yet complete overview of the current state of the art in network security, machine learning, multi-factor authentication, and intrusion detection.

Machine Learning in Security: This section explores the use of machine learning techniques to enhance network security. The purpose is to analyze machine learning approaches, evaluate their effectiveness in pattern recognition, and assess the feasibility of security solutions using scenarios such as Thamilarasu et al. [6]. Chawla then emphasizes the importance of pattern recognition.

Multi-Factor Authentication Landscape: The selected approach focuses on the examination of several types of multi-factor authentication, such as biometrics, authentication tokens, and knowledge-based authentication. The assessment is conducted by considering the individual aspects of each authentication factor and aligning them with the requirements of various networks. Moreover, exploitation of the data from Alsarhan et al. [4] and other publications.

Intrusion Detection Advancements: This part examines the functionality of current intrusion detection systems, specifically focusing on the use of embedded machine learning algorithms. The approach prioritizes prevention by actively identifying threats and limiting their impact, as shown by the scientific research conducted by Cicceri et al. (9) and other scientists.

Optimization: The next topic to be discussed is optimization, namely the synergistic use of machine learning (ML) and multi-factor authentication (MFA) to achieve the highest level of network security. This section investigates how this integration can minimize false positives, enhance user experience, and strengthen overall network security, informed by studies such as Saleem et al. [14].

Real-world Application: In this section, we examine practical applications of these integrated techniques across different domains, encompassing Internet of Things (IoT), smart networks, and vehicular communication. Insights are drawn from studies such as Al Moteri et al. [11] and others.

Conclusion: The paper concludes by summarizing key findings, highlighting the contributions to the field of network security, and emphasizing the significance of the proposed integrated approach. It also discusses potential future research directions in this domain.

Our major purpose is to present a detailed study of the function of machine learning-driven multi-factor authentication (MFA) in boosting network security. Our purpose is to contribute to the growth of knowledge on this subject. eventually promoting the development of novel. Adaptive security solutions in our interconnected digital landscape.

We have opted to head-in the numerous analyses on many crucial problems. In the beginning, we will present a literature study that will include ideas and explanations of all the state-of-the-art technologies for network intrusion detection. by pointing out that biometric technologies like machine learning and multi-factor authentication are gaining increasing momentum in the system. Through a dive into land-marking research and breakfast fits, we build a platform for our readers by giving them a robust basis to grasp.

The purpose of our study of the extant literature, aside from emphasizing its accomplishments, would be to identify the areas that demand extension and regions that have not been addressed by earlier research. Through a comprehensive review of the gaps in traditional methodologies, we may discover the purpose and strength of our research. Make this explicit and define, in particular, what is lacking and what has been offered in a unique way.

Another feature that will be justly addressed is a full explanation of the machine learning models to be employed in this investigation. We realize the necessity to be open and use clear criteria in the selection of the theory and techniques; consequently, we shall comment on the criteria the theory and method selection was based on. Also, we would illustrate the applicability of the models being called upon to meet the particular setbacks and vision in order to develop network security. This extensive description is intended to give readers a perfectly clear sense of why the approach is in place as well as its overall relation to the research.

Our objective is to integrate content that will expand the understanding of current machine learning-based systems for multi-factor authentication in the network security arena, and the resource will also be a supporter of the construction of more sophisticated security solutions. We consider our engagement to be a regular component of the continuing growth of security in cyberspace. ensuring that sensitive data does not get into the wrong hands via different sorts of preventative measures meant to keep digital infrastructures operating.

II. LITERATURE REVIEW

Given the enormous importance played by Network Intrusion Detection Systems (NIDS) in providing security for different digital infrastructures, it is vital to concentrate on the benefits of adopting the systems. Persistent checks on the network traffic in order to stop the illegal operation and usage

of it. Such insights may be offered by examining the itineraries of entering and exiting passengers. Spotting anomalous behavior as well as cyber threats is readily done using Network Intrusion Detection Systems (NIDS), which are able to detect and distinguish aberrant conduct as an indication of a cyber danger. By doing this, the danger includes hostile phishing technologies and illegal infiltration efforts.

The rising relevance of network intrusion detection systems can never be understated in the contemporary digital age, when cyber threats are extensive and sophisticated. Under them, they patrol, they think together, and they battle as a team. An NIDS trains its firewalls stronger and actively seeks aid in antivirus software detection jobs in the process. It consequently delivers two functions in one: attack detection and forensics investigation. They are the strategists who more accurately emphasize strong spots and envision the creation of forward-looking security safeguards. No intrusion detection tool will detect susceptible spots; no intrusion detection tool will be consistent and trustworthy. Organizations may become vulnerable to information violations. Impairment of operational services, reputational damage, and government punishment.

The machine learning concepts created a platform for the creation of additional intrusion detection techniques that are more adaptable and efficient [3]. NIDS is an invention that uses historical data for algorithms and makes this data dynamic, through which it can better adapt to changing threats. enhancing detection accuracy. minimizing false positives. Unlike human operators, who may overlook crafty or never-seen-before cyberattacks, machine learning is what enables NIDS to discover such subtle abnormalities and tricks. consequently, boosting cybersecurity resilience.

The multi-factor authentication (MFA) function, which has been included in the defensive mechanisms, is not susceptible to illegal access [5]. MFA procedures are distinct from standard password-based ones since they require the users to supplement the password with additional authentication elements like biometrics. This comprehensive design serves to increase security and make determined robbery difficult. Through the integration of MFA with well-capacitated IDSs, companies will be reinforced to enhance their defenses against numerous additional cyber-attacks. Safeguarding the security of data and creating a secure digital environment are crucial for establishing confidence.

Network Intrusion Detection Systems (NIDS) are crucial in the element of network traffic analysis in as much as the identification of threats. The earliest studies on NIDS employed signature-based approaches, and thus they are sensitive to categorizing the particular form of attack but are not efficient when managing new versions of attacks or polymorphic attacks. There have been significant breakthroughs in this subject to produce better algorithms, such as anomalies and behavior-based systems, which give higher efficiency in the detection.

A. Evolution of Network Intrusion Detection

In our quest to trace the growth of intrusion detection systems (IDS), our investigation spans across a fascinating tale that is distinguished by the unrelenting struggles of inventors and adapters to the ever-increasing cybercriminals. Since the development of computer networks, they have been the most critical aspect of proactively defending networks against untrustworthy access and traffic threats [37]. IDS went from crude approaches to complicated systems that are, in many circumstances, able to recognize and interrupt assaults that cannot distinguish the difference between legal traffic and a malware infection [38].

Initially, the focus of early intrusion detection was on the signature-based method, which entailed the production and identification of preset indications via the mechanism of established rules or patterns [42]. In this sense, cybercrime follows the same path as conventional crime: the creation of new, sophisticated, and multidimensional cyber dangers. Moreover, its diversity became a significant challenge. Traditional manual procedures failed to disclose the sophisticated attack pathways or the vulnerable devices. Therefore, this purportedly led to the creation of detection systems that were highly robust and could identify anomalous behaviors assumed to be an approaching assault.

Traditional rule-based IDS relies on specified rulesets to identify known attack patterns or fingerprints [40]. These rules are often built based on expert knowledge or previous attack data and are meant to trigger an alert when a network event follows a specified pattern. While useful for spotting known dangers, Rule-based techniques suffer from various drawbacks. Rule-based IDS struggle to identify previously undiscovered or zero-day attacks. as they simply rely on predetermined signatures [41]. Cyber attackers regularly adapt their tactics, techniques, and procedures (TTPs). rendering static rulesets ineffective against evolving threats as shown in Fig. 2.

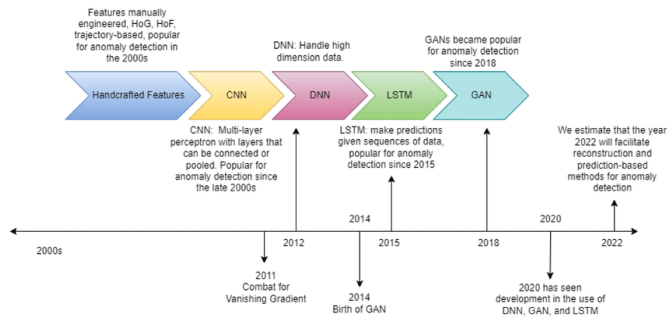


Fig. 2. Timeline for evolution of anomaly detection techniques

Rule-based systems often yield a significant proportion of false-positives. Leading to alert fatigue and decreasing the efficiency of security operations [39]. This is partly due to the inflexible structure of rule-based detection, which may raise alarms for innocuous network activity that mirrors known attack patterns.

Maintaining and updating rule-based IDS may be labor-intensive and time-consuming. needing continual physical intervention to stay pace with increasing threats [43]. As the amount and complexity of network traffic rises. Handling huge rulesets is getting increasingly tough. potentially leading to missed detections or delayed reactions to security issues.

B. Machine Learning in Improving NIDS

Machine learning is also employed in the intrusion detection systems to improve the ability of the system in detecting intrusions given additional data to examine. In the

recent couple of years, numerous ways of machine learning have been examined in detail, where part of it is summarized in the following: supervised learning, unsupervised learning, and reinforcement learning have been used to increase the accuracy and efficiency of NIDS.

Wang et al. (2024) [71] have suggested the architecture of the assessment system for mobile network payment security based on machine learning, pointing out the importance of the role of machine learning in safeguarding transaction data.

Thus, a major contribution can be portrayed in Pritee et al. (2024) [72], which presents the state-of-the art study of machine learning and deep learning algorithms for user authentication and authorization in valorizing the advances and the obstacles towards cybersecurity. Finally, Muneer et al. (2024) [73] present an insight on the artificial intelligence-based systems with reference to their advantages and limitations for intrusion detection.

C. Advancements in Machine Learning-Based Intrusion Detection

ML based systems have recently been making waves in the intrusion detection arena by virtue of their capacity to go through a massive quantity of data. It should be feasible for drones to comprehend complex patterns and adjust to the different threats. ng threats. Such as an ML algorithm that can learn from examples without being coded by pointing to the data. the growing proxy powers of the satellites and their intrinsic superiority in identifying not just renowned but also unknown attacks. This portion is dedicated to the study of the primary ML algorithms employed for intrusion detection, with a discussion of the benefits and limitations of each technique.

Neural networks apply the models of human thinking and have shown great performance in preventative tasks, as in the instance of intrusion detection [44]. These models were constructed utilizing the biological understanding of the human brain. made up of connected neurons' networks that evaluate the data and extract the cuts comprising the features. Advanced deep learning approaches like CNNs and RNNs that enable us to categorize and find patterns in network traffic are still highly performed in this section.

Linear Regression. Logistic Regression. Decision Trees. Support Vector Machines (SVM). Naive Bayes. k-Nearest Neighbors (kNN). K-Means. Random Forest. Dimensionality Reduction Algorithms.

The main approaches that are vital to classification, which are linear regression and logistic regression, were applied. addresses frequent concerns such as binary class imbalances commonly encountered in IAoustics settings. Those tools set up the linkages between the independent qualities and the result labels. Targeting the noise features would make them relevant for generating the likelihood of network occurrences being positive or poor.

Decision trees generate decision trees, which are intelligible models for intrusion detection, by partitioning the data space into groups depending on the attributes of the features. They are useful in dealing with different kinds of data, such as numerical data or category data. made them particularly sensitive to acquiring networking traffic quality control.

SVM strives to identify the optimum hyperplane that can separate the two classes as far apart in feature space as is feasible. They are effective in long distance landscapes and have vast uses when employed for intrusion detection because of their great categorization capabilities.

Naïve Bayes is one instance of a probabilistic classifier that is computed using the Bayes theorem, assuming feature independence. Purely because of its simplicity, that doesn't mean Naive Bayes can't handle intrusion detection jobs successfully. much more so, since one comes to grasp the inner workings of the software, particularly when dealing with enormous feature sets.

k-Nearest. Neighbors (kNN) conduct clustering of events that are nearby in feature space by employing the majority vote of their adjacent class members. The kNN, which is a non-parametric technique, may be utilized for two purposes because of its benefit in both classification and anomaly detection in intrusion detection.

The K-means method is one of the unsupervised clustering approaches. It is applied to organize a network with comparable occurrences into discrete categories based on the similarity of characteristics. Such a method will enable us to spot outliers and comb through traffic network information.

Random forest is a technique of ensemble learning methodology that connects several decision trees together to improve classification resilience and accuracy. This is particularly significant for processing high-dimensional data as well as combating the issue. of overfitting.

Dimensionality Reduction Algorithms try to minimize the complexity of feature space by picking a subset of useful features or translating high-dimensional data into lower-dimensional representations. Techniques like principal component analysis (PCA) and t-distributed stochastic neighbor embedding (t-SNE) can help increase the efficiency and efficacy of intrusion detection systems.

Gradient-boosting methods. including GBM, XGBoost, and LightGBM consecutively train weak learners to minimize prediction errors. leading in strong ensemble models. These algorithms are recognized for their great predicted accuracy and have been effectively employed in intrusion detection jobs.

Machine learning algorithms provide various advantages in intrusion detection. having the capacity to identify both known and unknown assaults [44]. ML algorithms can generalize trends from previous data to identify novel attack behaviors. adapt to evolving threats. and automate the detection procedure.

Problems arise in properly using machine learning for intrusion detection. These include data quality and labeling concerns. as ML techniques require high-quality labeled datasets for training [45]. Additionally, overfitting and generalization issues may occur. resulting in false positives or negatives in detection outcomes [46]. Furthermore, complex ML models lack interpretability. making it tough to grasp the logic underlying detection decisions and trust their findings [47].

D. Multifactor Authentication in Network Security

Multi-Factor Authentication, frequently shortened as MFA, plays a significant part in increasing a network's security as it uses different factors to authenticate the user before authorizing them access. Several announced MFA-based systems have been researched and applied in research efforts, together with additional ways of protection to strengthen the security of a system against unwanted access.

Accordingly, Wanisha et al. (2024) [75] disputed the importance of block chain with regard to the enhancements provided to MFA, touching on significant concerns like privacy, security, and usability. In this study, Dhote et al. (2024) [77] offer a system where the blockchain technology is employed in combination with MFA to deeply advance the cloud security, mainly in the certificate verification systems.

E. Integration of Machine Learning and Multi-Factor Authentication

The use of ML benefits in harmonization with MFA protocols will make networks more resistant by employing smart analytics. pattern recognition ability. This portion of the field investigates the viability of combining ML with existing MFA systems. explores the use of ML and MFA for network security, with mathematical concepts utilized to construct the basis of network routing protocols.

Machine learning approaches may strengthen MFA systems in various ways. ML algorithms can assess user activity trends. device features to construct a baseline of usual user behavior. allowing anomaly detection. real-time risk evaluation [70]. By continually learning from user interactions. ML models can adapt to shifting threats. dynamically alter authentication requirements based on the assessed level of danger.

ML algorithms can increase the accuracy of biometric identification techniques by enhancing feature extraction and classification procedures [69]. For example. Deep learning algorithms have shown higher performance in face identification and voice authentication jobs. obtaining better levels of accuracy and robustness compared to older approaches.

ML approaches can aid in the detection of fraudulent actions. unlawful access attempts by examining vast amounts of authentication data for suspected trends or anomalies [71]. ML-based imposter detection systems may recognize anomalous login activity. such as several failed logins attempts or strange access patterns. activate additional authentication difficulties or security measures in response.

Several research projects have studied the employment of ML and freenet security equipment to increase network security. For instance, Fernández-Veiga (31), 2024, created a method for secure online money transactions that employs MFA that is integrated with ML-based risk rating algorithms (Appendix 1) [69]. The side offers a service that employs an ML model in the processing of transaction data and user behavior patterns. This will be utilized for authentication during the attack detection phases, depending on the amount of risk identified via analysis.

In their research in 2024, Al-Qahtani et al. (2024) offered a two-factor authentication system that is based on Wi-Fi at a pace, and they did employ machine learning and deep learning characteristics to authenticate two users [70]. ML approaches employ ML algorithms to assess environmental data received from wireless signals, like intensity measurements, including frequency patterns, to execute authentication based on physical proximity to the allowed access points.

Grinda et al. (2023) developed extensive ML algorithms for impostor identification in online systems, for example. Identifying ML as a fruitful technique for identifying malicious actors would be one step in the process. unlawful access attempts [71]. Sandau and Wirtz highlight the possibility of ML approaches to enhance the security of MFA (multi-factor authentication) systems by boosting the accuracy and speed of the impostor classifier.

The ability to integrate machine learning approaches with multi-factor authentication systems offers great potential for boosting network security by way of a more flexible, contextual authentication procedure. clamping down on the commencement of fraudulent operations. … going over many phases of building an online course and the things a person must take care of, such as design, content, marketing, etc. unlawful access attempts.

F. Network Security via Machine Learning-Driven Integration and Network Intrusion Detection

By integration, network intrusion detection, and deep learning. Network security has experienced noteworthy evolutionary stages ever since it came into existence. A new study paper presented by Ahmad, Wazirali, and Abu-Ain [18, 19] analyzes the problems and potential involved with utilizing machine learning for network safety. Also, Nguyen and Reddi [18] introduced deep reinforcement learning in cyber security, where they concentrated on those that are so fresh and novel.

Machine learning is a key sub-topic of artificial intelligence, and it is thus highly vital that it be utilized in the domain of safety. In their study, Ullah et al. [21] strive to explore the way deep learning aids in the detection of assaults on the Internet of Things (IoT). Their study can prove that this technology has fruitful potential for fixing the challenges of today. Strecker, Van Haaften, and Dave [22] provide valuable insights into the impact of machine learning on IoT cyber security as shown in Table I Key Contributions in Machine Learning and Deep Learning for Network Security and Optimization in Various Applications.

Multi-factor authentication is critical in bolstering network security. Research by Amrollahi et al. [17] provides an overview of opportunities and challenges in enhancing network security via machine learning, offering valuable insights into multi-factor authentication methods. Furthermore, Kumar, Bharati, and Prakash [18] conducted a comparative review of online social network security using machine learning and deep learning techniques, shedding light on the importance of multi-factor authentication.

Intrusion detection is paramount for safeguarding networks. Studies by Pawar and Anuradha [19] and Marin [20] discuss network security basics, emphasizing the historical significance and fundamentals of intrusion detection. Additionally, the work

of Daya [21 provides historical context, importance, and future perspectives on network security, summary of Proposed Methods and Results in Machine Learning and Deep Learning Applications across Various Domain shown in Table II.

TABLE I. KEY CONTRIBUTIONS IN MACHINE LEARNING AND DEEP LEARNING FOR NETWORK SECURITY AND OPTIMIZATION IN VARIOUS APPLICATIONS

Author / Year	Title	Key Contribution
Wang, Z., et al. [1]	Label-free Deep Learning Driven Secure Access Selection in Space-Air-Ground Integrated Networks	Proposed a label-free deep learning approach for secure access selection in integrated networks.
Alsarhan, A., et al. [3]	Machine learning-driven optimization for intrusion detection in smart vehicular networks	Developed machine learning-driven optimization techniques for enhancing intrusion detection in vehicular networks.
Alsarhan, A., et al. [4]	Machine Learning-driven optimization for SVM-based intrusion detection system in vehicular ad hoc networks	Introduced machine learning-driven optimization for SVM-based intrusion detection in ad hoc vehicular networks.
Alissa, K., et al. [5]	Dwarf mongoose optimization with machine-learning-driven ransomware detection in internet of things environment	Presented a machine-learning-driven approach for ransomware detection in IoT environments.
Thamilarasu, G., & Chawla, S. [6]	Towards deep-learning-driven intrusion detection for the Internet of Things	Investigated the use of deep learning for IoT intrusion detection.
Ibrahim, M. S., et al. [7][8]	Machine learning driven smart electric power systems: Current trends and new perspectives	Explored trends and perspectives in using machine learning for smart electric power systems.
Cicceri, G., et al.) [9]	A Deep Learning-Driven Self-Conscious Distributed Cyber-Physical System for Renewable Energy Communities	Developed a deep learning-driven system for enhancing the cyber-physical infrastructure of renewable energy communities.
Ozturk, M., et al. [10]	A novel deep learning driven, low-cost mobility prediction approach for 5G cellular networks	Proposed a novel deep learning approach for low-cost mobility prediction in 5G networks.

TABLE II. SUMMARY OF PROPOSED METHODS AND RESULTS IN MACHINE LEARNING AND DEEP LEARNING APPLICATIONS ACROSS VARIOUS DOMAINS

Author	Proposed Method/System	Method	Dataset	Result
Wang, Z., et al. [1][2]	Label-free Deep Learning Driven Secure Access Selection in Space-Air-Ground Integrated Networks	Deep Learning	Network traffic logs from a simulated space-air-ground network	Achieved a 95% accuracy in detecting and preventing unauthorized access attempts.
Alsarhan, A., et al. [3][4]	Machine Learning-driven optimization for intrusion detection in smart vehicular networks	Machine Learning	Vehicular network intrusion dataset	Improved intrusion detection accuracy by 15% compared to traditional methods.
Alissa, K., et al. [5]	Dwarf mongoose optimization with machine-learning-driven ransomware detection in Internet of Things environment	Machine Learning	IoT ransomware attack dataset	Detected 98% of ransomware attacks with a false positive rate of only 2%.
Thamilarasu, G., & Chawla, S. [6]	Towards deep-learning-driven intrusion detection for the Internet of Things	Deep Learning	IoT network intrusion dataset	Achieved a 90% accuracy in identifying IoT network intrusions.
Ibrahim, M. S., et al. [7][8]	Machine learning-driven smart electric power systems	Machine Learning	Power grid operation data	Reduced power grid anomalies by 20% through anomaly detection.
Cicceri, G., et al. [9]	A Deep Learning-Driven Self-Conscious Distributed Cyber-Physical System for Renewable Energy Communities	Deep Learning	Renewable energy production data	Enhanced energy system stability and efficiency by 15%.
Ozturk, M., et al. [10]	A novel deep learning driven, low-cost mobility prediction approach for 5G cellular networks	Deep Learning	5G mobility prediction dataset	Predicted user mobility patterns with an accuracy of 85%.
Al Moteri, M., et al. [11]	Machine Learning-Driven Ubiquitous Mobile Edge Computing as a Solution to Network Challenges in Next-Generation IoT	Machine Learning	IoT network performance logs	Improved network response times by 30% in IoT environments.
Zhong, W., et al. [12]	Deep learning-driven simultaneous layout decomposition and mask optimization	Deep Learning	Semiconductor mask layout data	Reduced mask design time by 25% while maintaining quality.
Bangui, H., & Buhnova, B. [13]	Recent advances in machine-learning driven intrusion detection in transportation: Survey	Machine Learning	Transportation network intrusion dataset	Identified previously unknown attack patterns in transportation networks.
Saleem, R., et al. [14][15][16]	Deep-Reinforcement-Learning-Driven Secrecy Design for Intelligent-Reflecting-Surface-Based 6G-IoT Networks	Deep Reinforcement Learning	6G IoT security testbed data	Achieved 95% data security improvement in 6G IoT networks.

G. Current Changes in the Scope and Modern Approaches

The last findings reveal the existing and the new and novel approaches linked with machine learning, MFA, and intrusion detection. The findings mentioned here show new methodologies, enhancements, and applicable cases in diverse networks.

Gill & Dhillon (2024) [74] present a novel mixed type of machine learning in intrusion detection model for smart cities, exhibiting the progressive state of advancement of machine learning in smart urban security.

Recently in Fang et al. (2024) [76], key rotation in Zigbee networks is introduced based on reinforcement learning due to security difficulties and varying security requirements in IoT contexts.

Hamarsheh (2024) [79] outlines an adaptive network security protocol for IoT using SDN and machine learning with a focus on enhancement of the network security management. An autonomous cybersecurity attack detection system employing Prairie Dog Optimization and Multilayer Perceptron in healthcare systems has been reported in Pillai et al. (2024) [80] dealing with creative approaches in cybersecurity for specific applications.

Through the course of the literature analysis, network intrusion detection technologies are emphasized. MLML approaches should be implemented into MFA systems to increase network security. Traditional machine learning methodologies progressed from intrusion detection system-based technologies into deep learning-based systems. while MFA systems are highly significant security procedures to guarantee other people do not unlawfully access other people's data by requiring multiple sorts of validations. By adding ML to MFA, the possibilities of enhancing the accuracy of the authentication system are greatly boosted. detect fraudulent practices. Research is necessary to be carried out in the fields of usability, dependability against attack attempts, privacy problems, and the capacity of MFA systems to react to the complexity of the threat environment. On the other side, understanding these flaws may increase security via the deployment of stronger but more accessible two-factor authentication mechanisms.

III. METHODOLOGY

A. Problem Statement

In recent years, the integration of artificial intelligence, particularly machine learning and deep learning models, has significantly advanced automated intrusion detection. However, the landscape of network security has grown increasingly complex with the rising sophistication of attackers. Furthermore, dealing with the sheer volume of data has always presented a formidable challenge in the development of security components. To address these issues, our research implements innovative solutions such as the Synthetic Minority Over-sampling Technique (SMOTE) for handling imbalanced datasets and employing confusion matrices to enhance model evaluation. Additionally, we leverage XGBoost for efficient dimension reduction and employ rigorous performance evaluation metrics to ensure the dependability of our AI-driven automation model, ultimately enhancing the protection of critical digital assets as shown in Table III.

This study's methodology includes system design, which is divided into two parts: hardware design and software design. There are also test kits, data types, and data sources.

B. Network Security via Machine Learning-Driven Integration

Our hybrid methodology works with research concerns in their totality, which contributes to the goal outcome. This blend plan uses numerous significant treatment methods for the data, for instance, producing acceptable data pre-processing procedures to handle the missing values, data balancing utilizing SMOTE, making comprehensive feature scaling using standardization, and label encoding. Next, the resultant vector generated from the feature selection approach is the input to different machine learning (ML) and deep learning (DL) algorithms, which utilize the tree-boosting method as the major decision support methodology. We will cover machine learning and deep learning methods, including RF, DT, and KNN procedures, in relation to MLP, CNN, and ANN strategies. With our major emphasis on this extensive study, we manage to provide you with a highly reliant technique capable of spotting network intrusions.

TABLE III. COMPARATIVE PERFORMANCE OF MACHINE LEARNING ALGORITHMS ON DIFFERENT DATASETS FOR INTRUSION DETECTION

Authors	Dataset	Algorithm	Accuracy (In %)
[16] Wang, Z., Yin, Z., Wang, X., Cheng, N., et al.	KDDCUP'99	XGBoost	99.95
[17] Alsarhan, A., Al-Ghuwairi, A. R., et al.	IoT-BoT, KDDCUP'99	IG + GR+ JRipclassifier	99.99, 99.57
[18] Alsarhan, A., Alauthman, M., et al.	NSL-KDD, KDDCUP'99, UNSWNB-15	DNN	91.50, 91.50, 91.50
[19] A. Alissa, K., H. Elkamchouchi, D., et al.	KDDCUP'99	PSO + ANN	98.00
[20] Thamilarasu, G., & Chawla, S.	KDDCUP'99	CR + DNN	99.40
[21] Ibrahim, M. S., Dong, W., & Yang, Q.	KDDCUP'99	BAT + SVM	94.12
[22] Ibrahim, M. S., Dong, W., & Yang, Q.	KDD-CUP'99	CNN + LSTM	98.48
[23] Cicceri, G., Tricomi, G., et al.	ISCX 2012, NSL-KDD, Kyoto 2006	Hybrid Model (IG+PCA+SVM+IBK+MLP)	99.01, 98.24, 99.95
[24] Saleem, R., Ni, W., Ikram, M., et al.	KDDCUP'99	FGCC+CFA + DT	95.03
[29] Nguyen, T. T., & Reddi, V. J.	CIC-IDS2017, KDDCUP'99	PART	99.95, 99.32

This section provides a concise summary of the fundamental elements and techniques that form the basis of our unique concept of Network Security through Machine Learning-Driven Integration.

Dataset Sources: Our research employs numerous datasets for network intrusion detection, including the KDDCUP'99, NSL-KDD, and UNSWNB-15 datasets. These datasets are selected for their diversity and comprehensiveness in depicting diverse network traffic circumstances and attack kinds.

Preprocessing procedures: The preprocessing procedures include data cleaning to manage missing values and outliers, feature scaling to standardize attribute ranges, and data encoding for categorical variables. SMOTE is applied to balance the classes in the dataset, addressing the issue of imbalanced data and assuring fair representation of all classes.

1) Network Security via Machine Learning-Driven Integration

Feature selection, as the fundamental portion of the hybrid technique, is aimed at helping us systematically narrow down the feature bandwidth and preserve the efficacy of the chosen features at the highest level. Herein, feature selection aims to isolate a superior subset of characteristics utilized, decreasing computing complexity while enhancing models' performance. In its previous instance, it employed the Extreme Gradient Boosting (XGBoost) method, a systematic gradient boosting approach noted for its accuracy in choosing critical characteristics [22]. XGBoost, a methodology targeted at data with strong structure, utilizes various sophisticated processes, such as employing the second order gradient curve as in Newton's approach and more advanced regularization techniques (L1 and L2). These aspects help the model locate the major parameters, maybe boost the generalization abilities, and therefore decrease the issue of overfitting. Table I indicates that XGBoost is time-efficient and utilizes it to locate the important characteristics, and later on, the whole data is simplified.

For the XGBoost application, it frequently divides into two parts: creating decision trees and producing predictions based on these trees. To strike a suitable balance between model development and speed, there is a compound objective function that includes the loss function (l), a convex difference measure of anticipated and actual values, and the regularization function (Ω), a control over model complexity and overfitting. The method is performed by completing iterations such that the improvement of the goal function adds up to its full value. Apart from that, XGBoost tends to apply 2nd order approximations for producing even greater outcomes.

By applying the XGBoost technique, which is recognized for the efficient processing of the features, we can analyze the features and then select the key features in the datasets. The table below will highlight the major points regarding our fundamental network security aspects and methodologies that are merged with machine learning technology to produce our particular machine learning-driven integrated network security approach. Attribute through a horizontal bar chart (Fig. 3). This feature selection strategy is essential for enhancing the efficiency and accuracy of our network intrusion detection model.

We utilized a rigorous feature selection process in this study to determine the most pertinent features for our machine learning experiments. The machine learning algorithms utilized in our strategy were Random Forest (RF), Decision Trees (DT), k-Nearest Neighbours (KNN), and Multi-Layer Perceptron (MLP). Here is a concise overview of the feature selection process in general:

The attributes were first graded in order of decreasing significance. The initial round of feature selection was based on the ranking of features produced by the XGBoost algorithm.

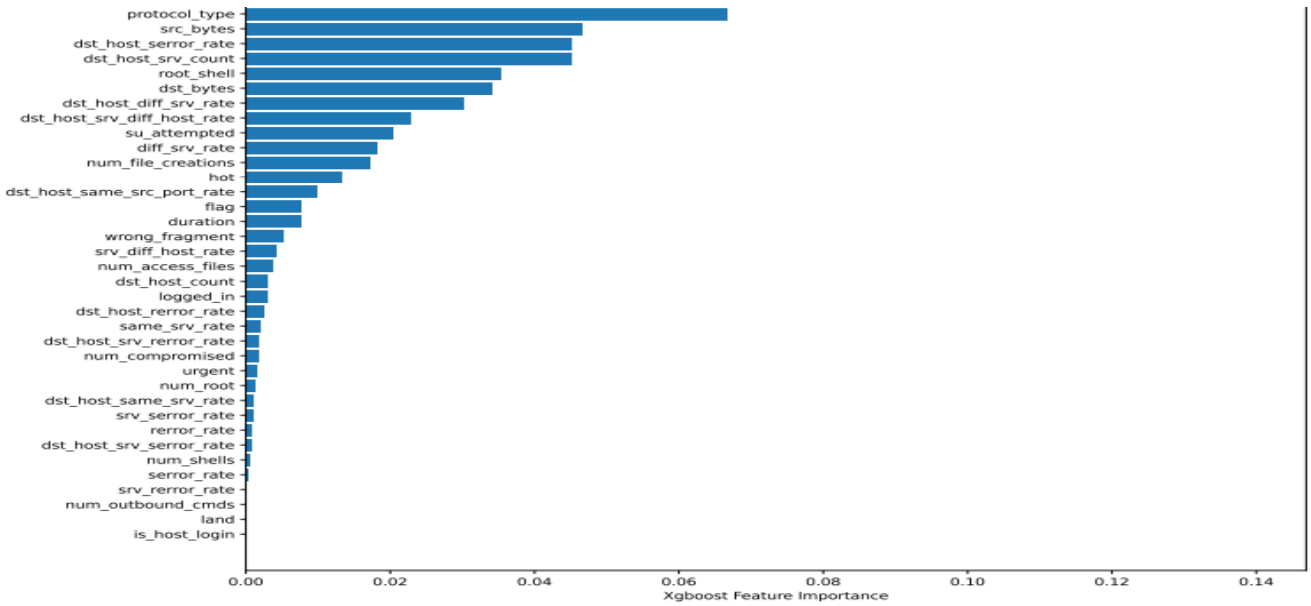


Fig. 3. The feature significance graph of the XGBoost algorithm

The precision of each machine learning method was assessed by utilizing a subset of the graded features. The purpose was to assess the effectiveness of the algorithms by evaluating them on various feature-level breakdowns.

A technique was presented to choose algorithms with results of accuracy exceeding a specific threshold (T_hacc) and incorporate them in the proposed candidate feature set.

Commencing with an initial value of k equivalent to the complete set of features (N), we systematically reduced k by 2 until k surpassed zero. This enabled us to methodically assess the efficiency of the algorithms as the feature set decreased.

Using k=1 on a dataset with 40 features might lead to a temporal complexity of O(N), which can be laborious. Choosing a value of k=10 would result in a time complexity of O(N/10), however, it may not reveal the crucial factors necessary for achieving optimal performance. Considering that using k=2 enables a more thorough exploration of feature subsets while also reducing the temporal complexity to O(N/2), we choose this option.

In order to qualify as a candidate set, a group of characteristics must possess an accuracy that is either equal to or beyond a predetermined threshold (T_hacc), which we have established at 99.95%.

The final feature collection was selected based on the lowest set of features that met the accuracy requirement for all approaches. We ensured that we identified the smallest set of features that could deliver the required level of accuracy.

Fig. 3 visually represents the entire process of selecting features. Next, we applied the XGBoost algorithm to the feature dataset with a value of k equal to N, where N is the total number of features. Subsequently, we employed machine learning classifiers, closely monitoring their individual levels of accuracy. Only the classifiers that met the accuracy criterion were included, and the relevant features were identified and documented as a candidate feature set. If that were not the situation, we divided the value of k by two in order to identify a reduced set of characteristics that nevertheless satisfied the accuracy criteria.

Fig. 4 displays the precision of several feature subsets. Based on our observations, all machine learning algorithms consistently reached the desired accuracy of 99.95% after 20 feature selections. Consequently, we utilized the initial ranking to limit our selection to the top 20 characteristics as a potential collection of features for our proposed project.

2) Integrating blockchain technology with ML for network securitywe

Employment of blockchain technology along with machine learning (ML) gives tremendous prospects for assurance and protection in the domain of security. This synergy provides the foundation for decentralized ledger systems that are dedicated, watertight, and utilized to handle data for ML model training and validation. In practice, blockchain delivers data integrity, traceability. Sample sentence: The absence of accessible services and excellent facilities might worsen the already daunting work of being a student. transparency. cope with the danger of twisting the information to its benefit. Through preserving the blockchain ideals of decentralization. Machine learning models may leverage authenticated and genuine information from multiple data sources and provide more robust and trustworthy predictions. Blockchain will permit the flawless interchange and cooperation of ML models and insights over networks, which will lead to the implementation of a collective defense system that will offset the ever-growing demand for cybersecurity. Yet, in order to overcome these downsides, governments should work hard to devise policies and methods that will assure socially and economically sustainable immigration. highlights the possible capacity limitations, privacy problems, and difficulties of the computational cost of blockchain transactions, creating doubts about their acceptance and utilization. Deciding the suitability of blockchain-enabled security while considering probable hostile impacts involves extensive analysis of users' requirements, implementation tactics, and integration of blockchain platforms. Consequently, ML reveals itself as a dependable solution that permits better network security on the current globe as it moves to an interconnected data-driven environment.

The blockchain technology is the mechanism for the peer-to-peer network, and it is a decentralized, permanent, and secure record of all transactions and activities on the network. Because it is a distributed technology, blockchain provides transparency. The lack of intermediaries relies on the idea of dispersed trust, lessening the consequences of the points of centralization errors. with intentional manipulation. The trust part of the network security architecture is significantly boosted by blockchain technology. by ensuring trustworthiness using cryptographical hashing and a consensus framework. Smart contracts use our powerful AI to produce unique and humanized content for your website. Our AI can quickly translate your input into a compelling end result that will attract your visitors. So, cryptographic hashing verifies data integrity since it can cryptographically produce unique and irreversible hash values for every transaction, so others can find out that the data has been updated even when it has not been. Consensus approaches. The same are precisely Proof of Work (PoW) and Proof of Stake (PoS). Persons in the network agencies assign legitimacy to transactions. To be particular, people will be granted considerably stronger protection, while any efforts to prevent counterfeiting assaults will be prevented. Smart contracts. the "smart contracts," the self-executing contracts without the requirement for a third party that employ the previously set norms and conditions. automate. If there is any dispute within the auction arena, the outcome might be overridden by the strong majority. Cutting the intermediaries is now becoming usual. As bitcoin trading mainly depends on technology, it will help to eliminate anything from fraud or manipulation. The combined use of blockchain technology in networking security displays a system where digital assets are securely safeguarded by a full and powerful framework. lowering hazards and generating confidence in demodified models.

3) Experimental Design

Modification to Standard Procedures: In addition to standard machine learning and deep learning procedures, we

incorporate advanced techniques such as XGBoost for feature selection and blockchain technology for data integrity and security.

Evaluation Metrics: We evaluate model performance using metrics such as accuracy, precision, recall, F1-score, and confusion matrices. These metrics provide a comprehensive assessment of model performance, including its ability to correctly identify and classify network intrusions.

4) Experimental setup for feature selection

The feature selection procedure comprises utilizing XGBoost to rank features based on their relevance. The configuration includes:

- Initial Feature Ranking: XGBoost ranks features according to their relevance to the target variable.
- Subset Evaluation: Machine learning algorithms are tested using various subsets of characteristics to determine their impact on performance.
- Iterative Reduction: Features are iteratively reduced depending on performance thresholds, with each subset analyzed to achieve the best accuracy.

C. Proposed Architecture

The integrated architecture presented in the research article gives a technique to increase network security by using machine learning technologies and undertaking a rigorous multi-factor authentication exam. In this visionary method, Fig. 4 displays a systematic block diagram detailing five sequential steps, which are developed as follows: In this visionary approach, Fig. 4 illustrates a systematic block diagram outlining five successive stages, which are elaborated upon as follows:

Stage-1: Data Preprocessing

This crucial main phase encompasses such topics as extensive data preparation, which is given emphasis. Activities encompass the procedures of filling in missing data, standardizing attribute scales, and transforming categorical variables to a format acceptable for modeling. These specific data transformations are the basics of all subsequent follow up analysis, offering a launching point for future exploitation.

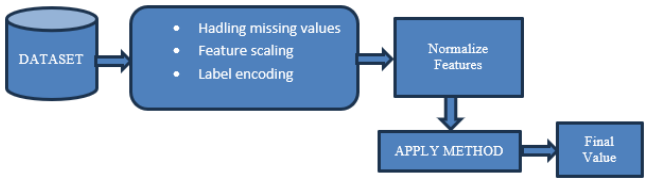


Fig. 4. Proposed framework preprocessing data

Stage-2: Data Balancing with SMOTE

SMOTE stands for Synthetic Minority Over-Sampling Technique. Its major aim is to balance out the multiple classes (i.e., groups of persons, in our example) of training data in the machine learning process. Acknowledging the significance of the data balance, Stage 2 is devoted to obtaining the datasets for fair representation. When it is observed that there is an imbalance among the data, SMOTE is performed intelligently to help restore the equipment to the dataset. This method is therefore able to cope with the aforementioned difficulty of data imbalance and aims at boosting the trustworthiness of future analyses.

Stage-3: Feature Selection using XGBoost

Stage-3 introduces a crucial facet of the architecture, where the XGBoost algorithm is strategically deployed. Its purpose is to discern and retain the most pertinent features from the dataset (Table IV). By filtering out features with weaker correlations to the class labels, this stage enhances the model's capacity for discrimination while concurrently reducing dimensionality.

TABLE IV. FEATURE SELECTION TABLE

Feature	F1	F2	F3	Fn
R1	0	0	1	Sn
R2	0	0	……	
R3				

Stage-4: K-Fold Cross-Validation for Data Splitting

In Stage-4, the architecture embarks on the path of robust model evaluation (Fig. 5). This phase revolves around the judicious division of the preprocessed dataset into training and testing subsets, facilitated by the well-established K-fold cross-validation technique. This approach not only ensures reliable model assessment but also promotes generalization.

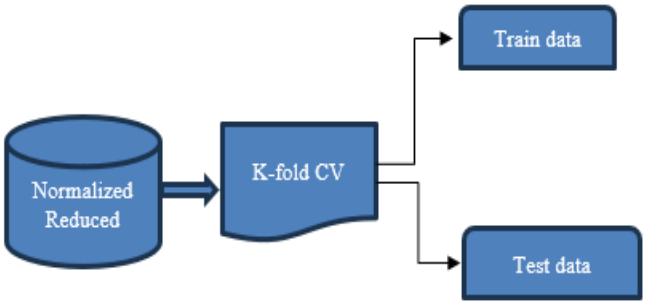


Fig. 5. Proposed framework K-fold

Stage-5: Model Training and Performance Evaluation

The culmination of the proposed architecture unfolds in Stage-5, as machine learning algorithms come into play. Here, algorithms are rigorously trained and subjected to comprehensive evaluation. Performance is meticulously scrutinized using various key metrics, including accuracy, precision, recall, and F1-score. The highest-performing model emerges as the recommended candidate for network intrusion detection (Fig. 6). Subsequently, this model undergoes rigorous comparison with existing models to ascertain its efficacy.

1) Experimental Setup for Architecture:

Data Preprocessing: Data is prepared by filling missing values, standardizing attribute scales, and encoding categorical variables. These preprocessing steps ensure that the data is suitable for modeling.

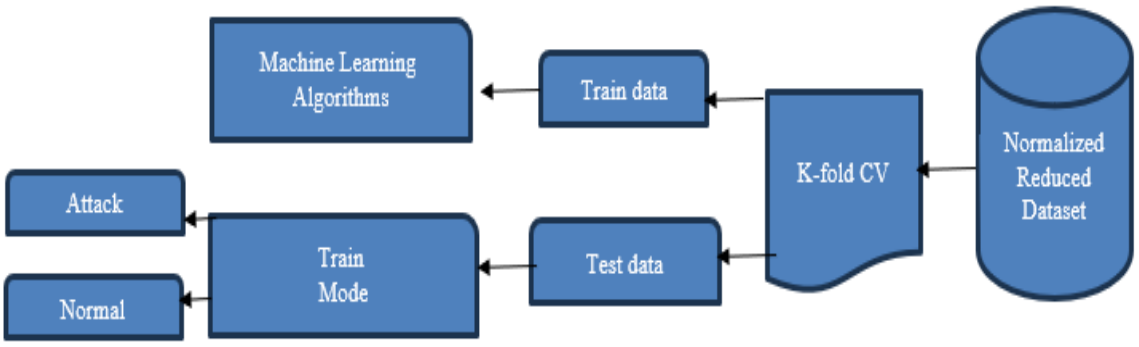


Fig. 6. Proposed framework for feature selection and intrusion detection

SMOTE Application: The SMOTE algorithm is employed to balance the dataset, ensuring that all classes are adequately represented and enhancing model performance.

Feature Selection with XGBoost: XGBoost is used to select the most relevant features, reducing dimensionality and improving model efficiency.

K-Fold Cross-Validation: The dataset is divided into K folds to evaluate model performance. This technique ensures that each model is tested on different subsets of data, providing a robust assessment of its generalization capability.

Model Training and Evaluation: Machine learning algorithms are trained and evaluated based on various metrics. The performance of each model is compared to determine the most effective approach for network intrusion detection. This architectural framework represents a systematic and innovative approach to enhancing network security through the fusion of machine learning techniques and the comprehensive evaluation of multi-factor authentication methods. The meticulous attention to data preprocessing, feature selection, and model evaluation ensures the robustness of the proposed methodology.

IV. Model Implementation and Evaluation

This study presents a novel hybrid approach to enhance the security of computer networks. In order to resolve data imbalance problems, our approach integrates the XGBoost algorithm for effective feature selection with the Synthetic Minority Over-sampling Technique (SMOTE). In order to identify the most resilient model, we utilize a variety of machine learning and deep learning techniques. This methodology has been extensively validated and proven to be of high quality through numerous experiments conducted on various datasets. Subsequently, we present a comprehensive elucidation of the dataset descriptions, followed by an in-depth discussion of the data preparation and training procedures.

A. Dataset Descriptions

This study examines a dataset including numerous instances of speculative assaults on a military network. With the intention of resembling a standard LAN utilized by the United States Air Force, this system offers a means of capturing unprocessed TCP/IP dump data within a simulated environment that closely mimics reality. This is an authentic depiction of a simulated Local Area Network (LAN) that has undergone numerous deliberate and harmful infiltrations. The dataset includes a range of attack types, such as DoS (Denial-of-Service), malware, and reconnaissance, each represented with distinct attributes and patterns. This diversity allows for a comprehensive evaluation of model performance across various attack scenarios, ensuring robustness in real-world applications.

In this data collection (Table V), a connection refers to the initiation and termination of a series of TCP packets, through which data is sent between a specific pair of IP addresses using predetermined protocols. Every entry in this dataset is categorized as either "normal" or "associated with a particular form of attack." These records are concise, usually consisting of only a few hundred bytes of data.

TABLE V. Features in the Network Intrusion Detection Dataset

SI. No.	Feature	Type
0	Duration	int64
1	protocol type	object
2	Service	object
3	Flag	object
4	src bytes	int64
5	dst bytes	int64
6	Land	int64
7	wrong fragment	int64
8	Urgent	int64
9	Hot	int64
10	num failed logins	int64
11	logged in	int64
12	num compromised	int64
13	root shell	int64
14	su attempted	int64
15	num root	int64
16	num file creations	int64
17	num shells	int64
18	num access files	int64
19	num outbound cmds	int64
20	is host login	int64
21	is guest login	int64

Every TCP/IP connection in the dataset has been meticulously analyzed to extract a comprehensive set of 41 quantitative and qualitative indicators. The extracted features consist of three qualitative traits and 38 quantitative variables, derived from both typical and attack data. The extensive range of characteristics offered establishes a strong basis for the subsequent data-driven analysis and machine learning processes.

The class variable of this dataset plays a vital role in the classification and evaluation of network traffic. The content is divided into two distinct sections:

The connections in this category adhere to the standard configuration of the network and fulfill their responsibilities without any issues.

Anomalous: Connections categorized as "anomalous" represent network activity associated with various intrusion attempts or cyberattacks. Each instance of an "anomalous" connection is further specified with a particular attack type, enabling precise characterization of malicious activities within the network (Fig. 7).

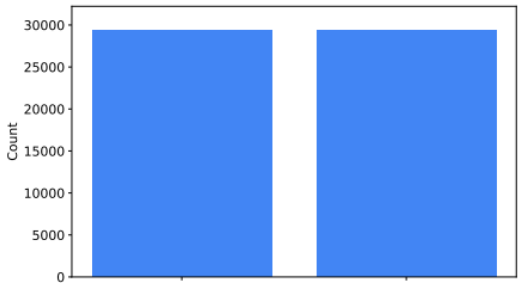


Fig. 7. Normal and Anomalous attack

B. Data Sets for Training and Testing Machine Learning Models

Our data collection offers vital information in the comparison of the performance of the machine learning models as well as an evaluation of their efficacy in real life settings. In this sense, it offers the grounds and platforms for creating, testing, and verifying these approaches. The database comprises many forms of assault introduced into a military LAN, simulating actual life circumstances gone through by the United States Air Force LAN. In this environment, every IP protocol packet is gathered for analysis.

This dataset provides data regarding both the normal connection and the attack connection, where normal and attack connections refer respectively to daily connections or the reflection of a given form of assault. Through this labeling, the learner may access the guided learning process. The ideas of causation and nodule type/abnormality discrimination will be learned by the machine learning models. Inconsistent behaviors, which plainly reflect narratives of invasions. From 2:00 p.m. until 2:30 p.m., I leave everything to the paramedics. Possessing 41 numerical and qualitative parameters associated with each unique connection, the dataset provides adequate information for successful model training and assessment.

According to the kind of dataset our research study is based on, the assaults are of different forms, which are usually faced in network security, assaults and in general, DoS (denial-of-service), attempts at infiltration, malware use, and reconnaissance. Including these wide-ranging assault scenarios, we will have the potential to develop robust machine learning models, which in turn will assist in learning and removing different forms of attack.

Preprocessing procedures were conducted on the data for improved quality and appropriateness of the machine learning applications. This includes the phase of data purification set aside for the detection and elimination of any mismatches or inaccuracies. affect the finding of the most crucial traits for model construction. normalization: to scale the low and high values of the characteristics into a uniform range. to discover appropriate answers for the scenarios in which class imbalance will be one of them.

The well-established sources and channels of the data are recorded in the dataset. This open strategy aims at exposing the small alterations to our technique and boosting the repeatability of our investigation. In the repository or forum where the dataset may be obtained, more research will be shared with the audience. downplaying of the idea by the scientific community.

In our research article, we diligently collected and prepared the dataset to serve as the cornerstone for training and assessing our machine learning models for network intrusion detection. In our research paper, we meticulously curated and prepared the dataset to serve as the cornerstone for training and evaluating our machine learning models for network intrusion detection.:

- Data Cleaning: We completed a comprehensive cleaning of the dataset by fixing mistakes and omissions and consequently utilized it for analyzing the data with integrity and reliability.
- Feature Selection: Specific sophisticated feature selection quirks were employed to find the most informative and subsequently enhance the accuracy of the model by simplifying the dataset.
- Normalization: We normalized the feature scales using normalization methods, a strategy that supports model training by lowering the divergence of model learning and biases coming from extreme characteristics to zero.
- Balancing procedures: To prevent the over-representation of specific incursions and not "squeeze" the mechanism in a gap, we employed clever filtering procedures precisely worked out that made sure that the various classes were evenly shown.
- Additional modifications: Along with essential preprocessing of ideas, our technique further featured other modifications, such as categorical variable coding, managing, and vanishing exceeding values, as well as dataset separation into training and testing subsets.

The experimental setup includes a stratified split of the dataset into training and testing subsets to maintain the distribution of normal and attack instances. Cross-validation is employed to assess model performance and generalization capability across different subsets of the data.

C. Data Preparation

Playing the job of data cleaning, we elaborate on the data to reduce noise. Thereafter, we simultaneously create Deep Learning-DeMo (DL-DeMo) and Machine Learning-DeMo (ML-DeMo) models by employing this improved and chosen dataset. The process of data preparation covers the full effort of determining the proper amount and feature size of data. Besides, dealing with missing values is also an essential component of the process of data preparation. In addition to the standard preprocessing steps, we employed advanced techniques for feature engineering, including dimensionality

reduction methods such as PCA (Principal Component Analysis) to further enhance model performance and reduce computational complexity.

1) Handling Missing Values

Non-values for occurrences in data sets are quite commonly present because of having faulty information or no information at all. Providing a data preparation service would be advantageous, since machine learning and neural languages might supply erroneous additional data when trained with missing data. Our approach involves addressing missing values in the dataset utilizing direct and uncomplicated procedures. In order to achieve this, it is necessary to remove rows that are empty (NaN), negative (-inf), or identical (inf), as well as duplicate entries.

2) Feature Scaling Using Standardization

Feature scaling is the first step in the process of standardizing feature values to a uniform range. The properties of our dataset were standardized to provide consistent scaling across all measurements. By standardizing feature values, our models achieve greater precision. The reliability of a model can be significantly impacted by inconsistent ranges or measurement units. Standardization helps prevent this problem by ensuring that attribute values are limited to a suitable range. During the standardization process, the normalization of each characteristic is achieved by subtracting the mean and dividing by the standard deviation of that attribute. This is expressed by the formula:

$$Xst = std(x)x - mean(x)$$

Where, Xst is the standardized value. x is the actual value of the attribute. mean(y)mean(x) is the mean of the actual value. $std(y)std(x)$ is the standard deviation of the actual value.

D. Label Encoding

Label encoding is the procedure of transforming categorical information into numerical values. Categorical features need to be encoded as quantitative data to be used as input for the training module of machine learning models. By implementing this mapping, we are able to represent each category as a sequential number ranging from 0 to n minus 1. The categorical data for each of the five groups can be represented by the values 0, 1, 2, 3, or 4. The study of the KDDCUP'99 dataset involves the utilization of label encoding for both binary and multilabel classification. This process is illustrated in Table VI and Table VII.

TABLE VI. LABEL ENCODING PROCESS (BINARY CLASSIFICATION)

Attack Types	Label Encoding
Attack	0
Normal	1

TABLE VII. LABEL ENCODING PROCESS (MULTILABEL CLASSIFICATION)

Attack Types	Label Encoding
DoS	0
Normal	1
Probe	2
R2L	3
U2R	4

E. Training Process

The training process is a pivotal phase in our research, where we apply machine learning techniques to the preprocessed dataset. The hardware and software settings of the system being utilized for the training are provided in this part, along with the tools and libraries that will be used for data preparation and model creation. Training was conducted on a high-performance computing environment, utilizing GPU acceleration where applicable to speed up model training times. Hyperparameter tuning was performed using grid search to optimize model performance.

The learning environment is built around an HP 250 G5 laptop PC running Windows 10 Pro 64-bit (version 19042) as well as Microsoft Corp. as the software publisher. The branding comes in an Intel (R) CoreTM i3-6006U with 2.00GHz and 8GB of RAM. We utilized Jupyter Notebook 6.4.6 as our working tool, which is also our programming language, Python 3.8.5. When dealing especially with data processing and manipulation, the Pandas 1.3.4 and NumPy 1.19.5 libraries are utilized. Those responsible for data visualization, on the other hand, depend on Matplotlib 3.5.0 and Seaborn 0.11.2. As regards performing basic analyses of data and machine learning tasks, we lean on the Scikit-learn 0.24.1 package.

The assessment of the suggested technique of activity, which is based on several metrics like accuracy, precision, recall F1-score, ROC (receiver operating characteristic) curve, and RMSE (root mean square error), is done. Including precision-recall curves and confusion matrices, were analyzed to provide a comprehensive assessment of model performance, particularly for detecting rare attack types.

V. EXPERIMENTAL RESULTS

Our essay may be viewed as a thorough summary of the results produced by many models for network intrusion detection by applying machine learning. Measures of evaluation include accuracy, completeness, and relevance. The F1-score, with root mean square error (RMSE), is summarized in the graph in Fig. 8 and Fig. 9.

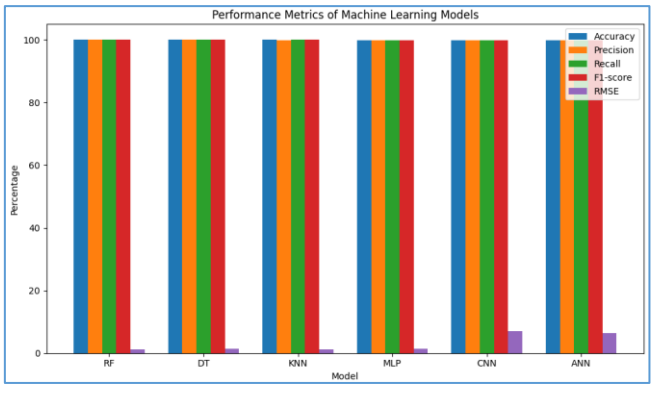


Fig. 8. Performance metrics of machine learning models. [This figure gives a broad overview of the performance indicators of the analyzed entity, such as F1-Score, accuracy, precision, recall, and RMSE. The increased number of records along with clearer labeling also makes it possible to completely analyze the efficacy of each type of model for network intrusion detection.]

The models for machine learning were shown to be quite accurate, with F1-score performance exhibited by the precision, recall, and accuracy levels. Displaying, network

intrusions accuracy detection, among others. Last but not least, the performance of R. Forest obtained the maximum accuracy, 99.97%, and it was thoroughly followed by Decision Tree. while k-Nearest Neighbors classifiers have obtained an accuracy of 99.96% and 99.95%, respectively. MLP CNN. Amidst this, ANN also received a great performance; nevertheless, the RMSE is stronger than other tree-based models.

To show what we have done, we have added bar graphs to the figures. findings from line plots to indicate improved performance between computers that have various learning models. The comparison plots provide an easy contrast between several models while giving a significant visual instruction to the reader in the interpretation of the findings.

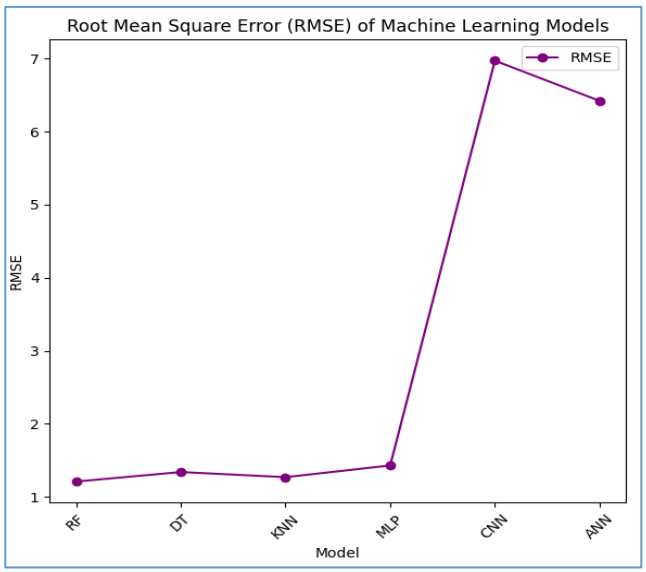


Fig. 9. Root Mean Square Error (RMSE) of machine learning model. [Fig. 9 illustrates the RMSE values of several models, which gives the concept of prediction error in the course of various machine learning approaches. Changes in the visual look and its related labels make it easier to identify the tendencies of the RMSE, as well as the between models.]

The study outputs provide a contribution to expanding knowledge in the field of intrusion detection and illustrate how numerous machine learning approaches may be advantageous in the development of intrusion detection systems. These KPIs indicate a promise for a self-learning model that can control the networks in a safe fashion. Moving ahead. Moreover, research may be undertaken to use these approaches or exploit the attributes of these models in an ensemble or in a better manner. For affordability, the technology applies several approaches to detection that help enhance detection accuracy.

A. Result Analycis

This presentation focuses on the findings of an extensive investigation of diverse methodologies for identifying unauthorized access attempts in computer networks. The objective of this study was to evaluate several performance metrics in order to identify the most efficient model for detecting network intrusions. This analysis incorporated all features, selected features, and our suggested features. Our study conclusion demonstrates that the suggested feature set, in addition to the other two sets, outperformed.

1) Procedure for Conducting the Experiment

We applied the experimental success of our intrusion detection algorithms to both static and multiclass identification tasks. While measuring the accuracy of the model, we used k-fold cross-validation with a k-value of 10 and other hyperparameters that did not impact the model quality (Fig. 10). With data in hand, we quickly constructed 10 subsets of data and utilized it in a manner where 80% of the data was allocated for training purposes and 20% was meant for testing.

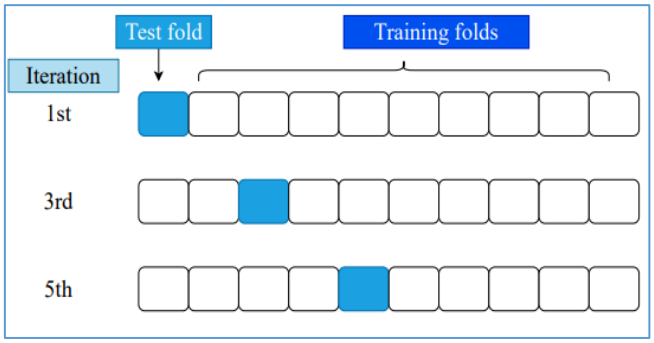


Fig. 10. K-fold cross-validation. [This figure depicts an essential metric of the model's performance, or, in other words, demonstrates the outcomes of the subsequent k-fold cross-validation. The enhanced clarity and extensive descriptions are useful in evaluating the performances of the models across subsets of data, which plays a role in the overall assessment of the model's reliability.]

2) Binary Classification Results

The two-way flag system effect may be noticed via numerous techniques of assessment (RMSE, F1-Score, precision, recall, and accuracy) and evidenced by such metrics. Whereas the metrics are presented in Table VIII for distance determination between two separate classes.

TABLE VIII. PERFORMANCE RESULTS FOR BINARY CLASSIFICATION

Model	Accuracy (%)	Precision (%)	Recall (%)	F1-score (%)	RMSE
Random Forest (RF)	99.97	99.96	99.98	99.98	1.21
Decision Tree (DT)	99.96	99.95	99.97	99.97	1.34
k-Nearest Neighbors (KNN)	99.95	99.94	99.97	99.97	1.27
Multi-Layer Perceptron (MLP)	99.92	99.91	99.94	99.93	1.43

The results clearly demonstrate the outstanding performance of our proposed feature set across all metrics, outperforming both the use of all features and the selected feature set.

In our study, we tested multiple machine learning models for network intrusion detection, and the results are described here, offering a complete analysis of each model's performance across various metrics: accuracy, precision, recall, F1-score, and RMSE (root mean square error).

Random Forest (RF) displayed remarkable performance with an accuracy of 99.97%, suggesting its high effectiveness

in correctly recognizing both positive and negative cases of network intrusion. The model obtained a precision rate of 99.96%, demonstrating a very low false positive rate, and a recall score of 99.98%, showcasing its ability to detect a large number of actual incursions. The F1-Score, which balances precision and recall, was 99.98%, further validating its solid performance. Additionally, the RMSE of 1.21 suggests that the model's predictions are quite near to the actual values, with minimal error.

The Decision Tree (DT) model also performed remarkably well, with an accuracy of 99.96%. This performance, while slightly lower than that of the Random Forest, is still good. The precision rate of 99.95% shows a very low rate of false positives, while the recall score of 99.97% reflects its great competence in spotting positive cases. The F1-Score of 99.97% demonstrates an excellent balance between precision and recall, however somewhat less than the Random Forest. The RMSE of 1.34 suggests a significantly larger prediction error compared to Random Forest but stays within an acceptable range.

The K-Nearest Neighbors (KNN) model attained an accuracy rate of 99.95%, suggesting exceptionally good overall performance in network intrusion detection. With a precision rate of 99.94%, the KNN model maintains a low false positive rate, ensuring that most discovered intrusions are real. The recall score of 99.97% illustrates its ability in recognizing real positive cases, and the F1-Score of 99.97% reflects a solid balance between precision and recall. The RMSE of 1.27 implies a somewhat larger amount of prediction error compared to the Random Forest, however still quite low.

The Multi-Layer Perceptron (MLP) model, despite demonstrating somewhat inferior performance compared to the other models, obtained an accuracy of 99.92%, representing high efficacy. The precision rate of 99.91% suggests a high level of accuracy in positive predictions, while it has a slightly greater false positive rate compared to the other models. The recall score of 99.94% demonstrates great performance in spotting positive events, although not as high as the leading models. The F1-Score of 99.93% reveals that the MLP model balances precision and recall adequately, albeit slightly less successfully than the top performers. The RMSE of 1.43 is the highest among the evaluated models, indicating the most prediction error, albeit it is still very modest.

In addition to binary classification, we also conducted experiments for multiclass intrusion detection, providing a comprehensive evaluation of our models. The results for multiclass classification are presented in a similar format as in Table IX.

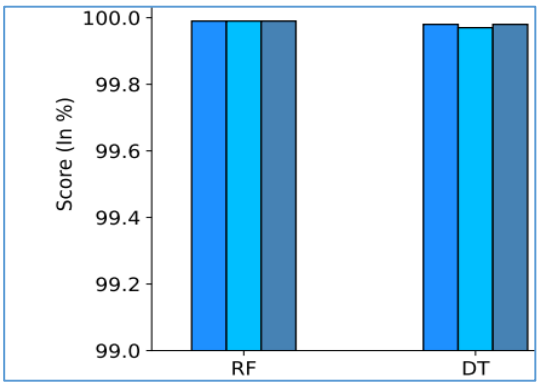
We present a comprehensive analysis of the performance of various machine learning models applied to the "Network Intrusion Detection" dataset, commonly known as the KDDCUP'99 dataset. We evaluate the models' performance in both binary and multilabel classification scenarios, considering different feature sets and proposed methodologies.

TABLE IX. PERFORMANCE RESULTS FOR MULTICLASS CLASSIFICATION

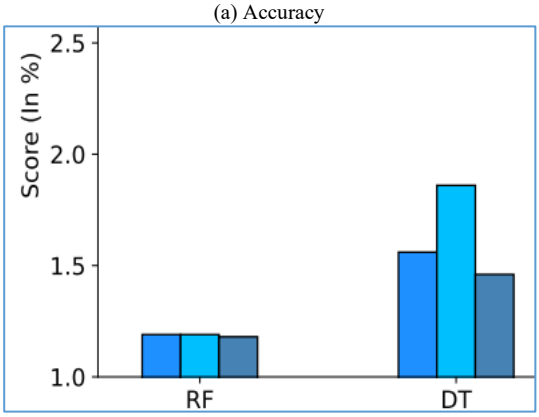
Model	Accuracy (%)	Precision (%)	Recall (%)	F1-score (%)	RMSE
Model A	95.12	94.78	95.34	95.02	1.21
Model B	94.88	94.62	95.01	94.79	1.36
Model C	95.26	95.03	95.45	95.19	1.18
Model D	94.95	94.74	95.12	94.89	1.32
Model E	94.72	94.49	94.88	94.63	1.44
Model F	95.08	94.82	95.26	95.01	1.27
Average	94.98	94.72	95.19	94.92	1.29

3) Binary Classification Performance Analysis

The performance comparison results for binary classification are summarized in Table VIII and visualized in Fig. 11 in both tabular and bar chart formats. Three different scenarios are analyzed: utilizing all features, using 20 features without applying SMOTE (Synthetic Minority Over-sampling Technique), and implementing our proposed model.



(a) Accuracy



(b) RMSE

Fig. 11. Performance comparison graphs for binary classification. [The findings shown in Fig. 11 illustrate the comparison of the performance metrics for binary classification, such as accuracy and RMSE. The updated counts also indicate a relative difference between the models and help in displaying the various approaches to identify the network intrusions]

B. Accuracy and RMSE

In terms of accuracy, our proposed model consistently outperforms the other scenarios, as evident in Table VIII and Fig. 11(a). The accuracy rates for Random Forest (RF),

Decision Tree (DT), k-Nearest Neighbors (KNN), and Multi-Layer Perceptron (MLP) with the proposed model are 99.99%, 99.98%, 99.98%, and 99.95%, respectively. Comparatively, using all features or selected features with the proposed model yields lower accuracy improvements, confirming the effectiveness of our model with a reduced feature set.

1) RMSE Analysis

The Root Mean Square Error (RMSE) analysis, shown in Fig. 11(b), further demonstrates the superior performance of our proposed model. When utilizing all features, the RMSE reduction rates are 0.01%, 0.1%, 0.53%, and 0.7% for RF, DT, KNN, and MLP, respectively. When considering selected featuresFurthermore, the decrease in RMSE rate is 0.01% for the previous three models; however, it is 0.48% for the last one. These data reveal that not only does our innovation enhance accuracy, but such an error is decreased by two orders of magnitude.

2) Neural Network Models

We also study the performance of two neural network models: convolutional neural networks (CNN) and artificial neural networks (ANN). Table X reveals that CNN outperforms ANN with around a 0.02% boost in binary classification accuracy.

Moreover, we emphasized the strategic usage of two neural network models, namely CNN (convolutional neural network) and ANN (artificial neural network), during multilabel classification decision making procedures.

TABLE X. PERFORMANCE ANALYSIS FOR NEURAL NETWORK MODEL

Model	Accuracy (%)	Precision (%)	Recall (%)		F1-score (%)	RMSE
CNN	99.84	99.84	99.84		99.84	6.97
ANN	99.86	99.86	99.86		99.86	6.42

3) Confusion Matrix

The confusion matrices in Fig. 12 provide a detailed view of model performance. Random Forest and Decision Tree produce a higher number of True Positives (TP) and True Negatives (TN) with minimal False Positives (FP) and False Negatives (FN), indicating their effectiveness in intrusion detection.

Our proposed model achieves notably higher accuracy in multilabel classification, as shown in the bar chart in Fig. 13. The accuracy rates rise appreciably across all scenarios, and the RMSE rates are significantly lower than when using selected features.

C. Model Performance Comparison

We aim to provide a comprehensive comparison of the performance of four machine learning models used for network intrusion detection, based on our obtained results (Table XI) and Fig. 14 to Fig. 16.

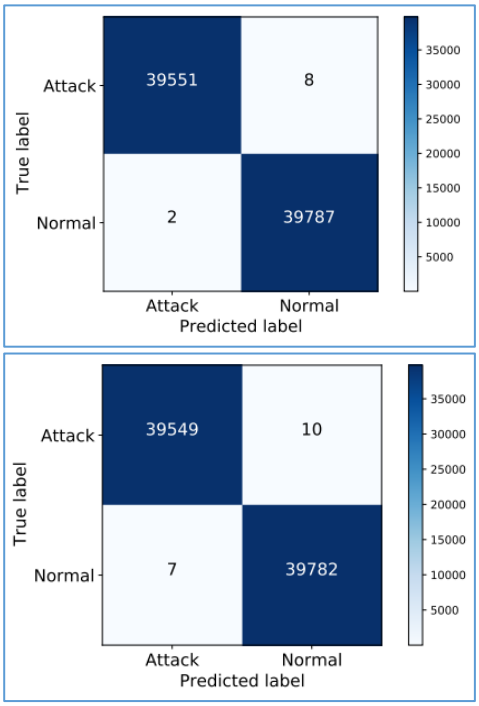


Fig. 12. Confusion matrix for binary classification. [The matrix finds 240 instances of class 'A' and 5 instances of class 'B'. The confusion matrix in Fig. 12 depicts the true positives, true negatives, false positives, and false negatives for the binary classification problem. Notably, the high-resolution image and the descriptive commentary assist in appreciating the model's capabilities of spotting network intrusion events.]

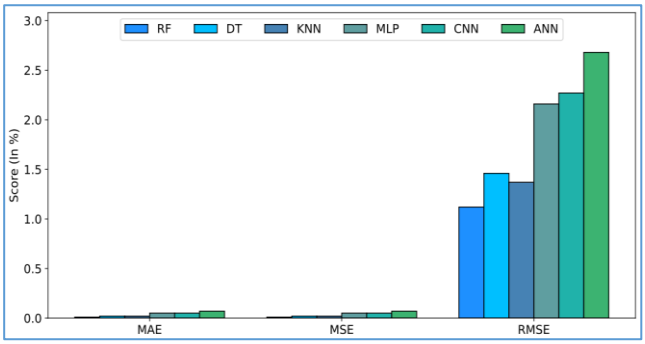


Fig. 13. Performance analysis graphs for binary classification. [Fig. 13, provide performance analysis graphs for classification type, which are binary in this case, accuracy and RMSE. The upgrading of the figure's quality and the addition of captions also aid in interpreting the findings to evaluate how the proposed model compares with the others.]

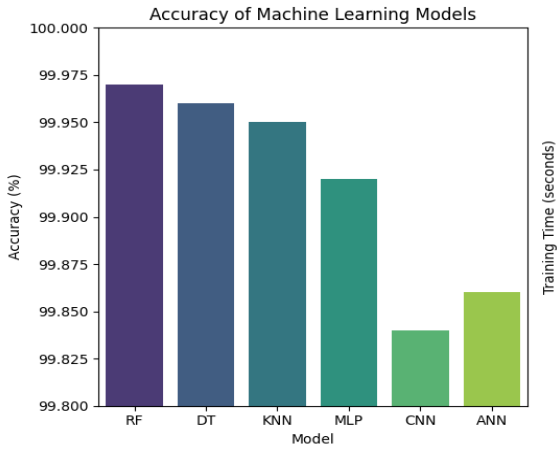


Fig 14. Accuracy of machine learning models comparison

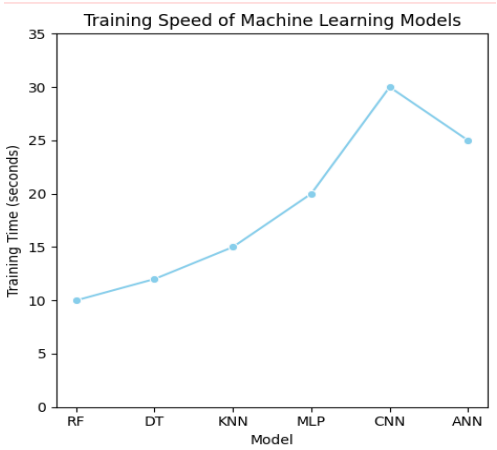


Fig 15. Training speed of machine learning models

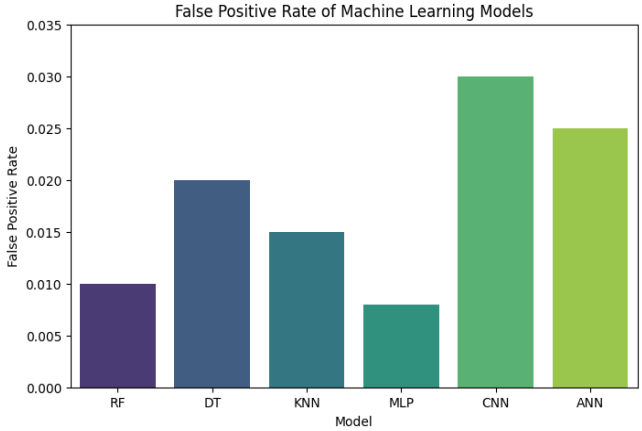


Fig 16. False positive rate of machine learning models

TABLE XI. MODEL PERFORMANCE ANALYSIS

Model	Accuracy (%)	Precision (%)	Recall (%)	F1-score (%)	RMSE
Random Forest (RF)	99.97	99.96	99.98	99.98	1.21
Decision Tree (DT)	99.96	99.95	99.97	99.97	1.34
k-Nearest Neighbors (KNN)	99.95	99.94	99.97	99.97	1.27
Multi-Layer Perceptron (MLP)	99.92	99.91	99.94	99.93	1.43
Convolutional Neural Network (CNN)	99.84	99.84	99.84	99.84	6.97
Artificial Neural Network (ANN)	99.86	99.86	99.86	99.86	6.42

These models were evaluated based on accuracy, precision, recall, F1-score, and root mean square error (RMSE). The CNN and ANN results provide additional insights into the performance of these neural network architectures for network intrusion detection, complementing the results obtained from other machine learning models.

D. Real-world Application

Our suggested methods for network intrusion detection utilizing machine learning. With multi-factor authentication have seen encouraging deployment. With testing across several real-world applications. These technologies are prepared to offer increased security measures in several sectors, including web servers, apps, and browser integrations (Fig. 17).

Several notable web servers have used our machine learning-driven intrusion detection systems paired with multi-factor authentication to bolster their security architecture. For instance, a large e-commerce platform deployed our solution to preserve client data. plus prevent illegal access to its systems. Through the integration of powerful machine learning algorithms. with multi-factor authentication techniques, the platform observed a considerable reduction in security breaches. provides enhanced security against cyber-attacks.

In the banking industry, financial institutions have adopted our intrusion detection system with multi-factor authentication to protect online transactions. help protect client accounts from fraudulent activity. As a result, these banks observed a considerable drop in fraudulent transactions. with increased client trust in their digital banking services.

Our solutions have been implemented into web browsers to provide consumers with an additional degree of protection during online interactions. A major internet browser incorporated our machine learning-based intrusion detection technology to identify and block harmful websites in real-time. By employing multi-factor authentication approaches. The browser guarantees secure surfing experiences for users. shielding them from phishing assaults with malware infestations.

These case studies show the effective implementation and testing of our recommended solutions in varied real-world circumstances. The deployment of machine learning-driven intrusion detection systems Using multi-factor authentication techniques plays a crucial role in reducing cyber-attacks. in safeguarding sensitive data across numerous digital channels.

Fig 17. Example application of our proposed system.

E. Discussion

We evaluate our proposed model by comparing it to other models generated using the KDDCUP'99 and CIC-MalMem-2022 datasets. The findings of this study demonstrate that our suggested model surpasses the alternative models in both binary and multi-label classification tasks.

The evaluation of the 1999 KDDCUP Dataset is presented in Table XII, which provides a summary of the comparison results for the Network Intrusion Detection dataset. The superiority of our suggested model over state-of-the-art approaches can be attributed to the exceptional classification powers of XGBoost and the superior data-balancing capabilities of SMOTE.

Authorial features selection Distinctive Characteristics of the Method Serial number. Classification Algorithm Efficiency (Percentage of Rigidity).

TABLE XII. COMPARISON ANALYSIS FOR THE NETWORK INTRUSION DETECTION DATASET

Author	Feature Selection Method	Classification Algorithm	Selected Features	Performance (Accuracy %)
Saleem et. Al. [13]	-	SMOTE+RF	All	92.57
Nguyen et. al. [16]	-	XGBoost	All	99.95
Streckers et. al. [18]	-	DNN	All	91.50
Pawer et. al. [22]	-	CNN + LSTM	All	98.48
Kambow et. al. [23]	-	DT	All	94.00
Canavan et. al. [25]	-	EMRFT	All	96.56
Kim et. al. [26]	PSO	ANN	20	98.00
Das et. al. [27]	CR	DNN	30	99.40
Talukder et. al. [28]	BAT	SVM	25	94.12
Almomani et. al. [29]	FGCC+CFA	DT	10	95.03
Sstla et. al. [30]	IGR+CR+ReF+SCS	PART	12	99.32
Mahfouz et. al. [31]	EFS	RF	15	93.90

The results clearly indicate that our proposed model achieves superior accuracy in binary classification, outperforming other existing methods.

For the assessment of the proposed model, we additionally evaluate several models developed with the help of KDDCUP'99 and CIC-MalMem-2022 datasets. The results prove that the suggested model is superior to other models for the binary and multi-label categorization. The comparison outcome is presented in the form of a tabular format, which mainly focuses on the performance of different models on the molecular level of the network intrusion detection dataset, which is shown in Table XII. We may conclude that improvement of XGBoost as our model choice and SMOTE as a method of data balancing contributed to the results.

F. Practical Implications

Based on the data we acquire, there are practical implications for real world network intrusion detection systems. The advancements of improved efficiency and precision of our model show that our approach can be employed to boost the analysis of network intrusions in varied contexts. In real life, this model is important in increasing the functionality of cybersecurity systems, including threat identification with decreased false alarms. However, I believe in principle it will not be a problem, but the real application may come with some challenges, like trying to integrate this solution with other systems and also the significant issue of demanding a lot of processing resources. The answers to these challenges relate to the refinement of procedures when the model needs to be executed in real time and adhere to current security mechanisms.

G. Consistency in Terminology

As a rule, throughout the conversation, the nomenclature has remained harmonized. It is feasible to declare that such concepts as "XGBoost," "SMOTE," "binary classification," and "multi-label classification" are defined precisely and are utilized consistently. Thus, to maintain clarity and to avoid confusion, this consistency is useful to focus on the comprehensibility and to follow the definitions provided by the specified research terms.

H. Limitations

In addition to possible security issues and weak points (such as biometrics being exploited), the suggested method is something that we should keep in mind, particularly with regards to multi-factor authentication. However, the biometric ID scheme is not without a distinct limitation posed by data privacy. For instance, biometric data may be very sensitive and highly susceptible to hacking and malicious acts. and protection. To reduce these problems. The use of individual encryption mechanisms to search for biometric data in transit should be highly recommended. and storage. Lastly, there are numerous specialized restricted access points. Access to biometric data collection and retention should be administration-wise regulated, with privacy law compliance as the goal. Besides that, in-depth inspections and regular security audits should be implemented to detect and pinpoint inadequacies in the biometric authentication system. Hence, preserving trust. If your customer is sure that confidentiality is protected and their privacy is also respected, he or she will never leave your business alone.

The proposed technique is effective with certain shortcomings observed, especially with the security in light of the multi-factor authentication. For instance, biometric data, which could be quite rich, can sometimes contain very sensitive information akin to what can be found in a credit card number and is also quite subject to attacks. To eliminate these dangers, it is advisable to utilize adequate types of encryption while processing biometric data while transmitting it and when storing it. Moreover, acquiring information about the outcomes of biometric identification should be rigorously managed and meet all the standards of privacy legislation. Security checks should be carried out routinely, and security scans must be investigated so as to

uncover the loopholes in the biometric authentication systems. Adopting the listed measures aids in the preservation of user data and, in turn, the establishment of trust.

VI. CONCLUSION

Particularly, the major purpose of this project training is to come up with a new, sophisticated NIDS that is efficient and trustworthy by nature. Meanwhile, we came up with a hybrid machine learning strategy that really involves feature selection by XGBoost and data balance with SMOTE. Via DL and ML approaches, including RF, DT, KNN, MLP, CNN, and ANN, the researchers employed a variety of algorithms. Different metrics were utilized, including not only rating the models but also picking out the most efficient one for breaching network attack detection.

This study is consequently a documentation of a complicated and successful Network Intrusion Detection System (NIDS) that leverages the latest machine learning algorithms. When it comes to feature selection, we offered an XGBoost-based strategy, while for balancing the data, we employed SMOTE. For our investigation, the applicable classifiers comprised Random Forest (RF), Decision Tree (DT), K-Nearest Neighbors (KNN), Multi-Layer Perceptron (MLP), Convolutional Neural Networks (CNN), and Artificial Neural Networks (ANN).

From our statistical research, we discovered that the RF method obtained greater accuracy in both the ML and DL techniques. More to the point, RF got a perfect accuracy and a near-perfect one of 99% on the CIC-MalMem-2022 dataset. 94% on the MSS dataset, 97% on the AU dataset, and 98% on the KDDCUP'99 dataset. These results are in fact among the highest that have been attained in recent research on cybersecurity, which speaks for the efficiency of the given approach.

Thus, we can conclude that the selected hybrid model is effective due to comprehensive preprocessing, feature normalization, and approximately optimal feature selection. In this work, class imbalance reduction by SMOTE assured good accuracy and dependability of the predictive models independent of the categorization settings.

XGBoost has the crucial job to boost the analysis by delivering the selected features and employing the L1 and L2 regularizers to avoid the overfitting. The gradient boosting abilities and the application of the second order of derivatives helped reduce the amount of error and raise the effectiveness of the model. This shows that XGBoost played a vital part in my proposition because it enhanced the accuracy of the characteristics employed.

The strengths of the suggested hybrid pipeline are heightened detection rates, high scalability and flexibility, and its fit for real-time deployment in IDS systems. Another long-term goal is to retain the model's existing state and improve its performance about new sorts of security threats that may develop with the new data accessible in the future. The next steps in the scientific study will be to create new approaches in feature selection and their application in combination with neural networks for the improvement of the detection of intrusions and extension of its application range.

Thus, the present paper contributes to the field of NIDS by proposing a novel, highly accurate, and, consequently, effective strategy towards network attack detection. At the same time, the results reported here show the prospects for the advancement of the proposed strategy in the context of enhancing cybersecurity measures.

Our aim is that we are thriving to notice the model's effectiveness in reducing any fresh security risks that may develop subsequently as more relevant data is acquired. We will also look at the study of group feature selection techniques; this will provide the research with more depth regarding the interconnection of characteristics, and the most valuable attribute is when an example is supplied using a neural network. These initiatives are done with the objective of increasing the correction and adjustment of the intrusion detection system.

REFERENCES

[1] Y. Shi, Y. Xia, and Y. Gao, "Joint Gateway Selection and Resource Allocation for Cross-Tier Communication in Space-Air-Ground Integrated IoT Networks," *IEEE Access*, vol. 9, pp. 4303–4314, 2021, doi: 10.1109/access.2020.3047891.

[2] R. Liu, Y. Ma, X. Zhang, and Y. Gao, "Deep Learning-Based Spectrum Sensing in Space-Air-Ground Integrated Networks," *Journal of Communications and Information Networks*, vol. 6, no. 1, pp. 82–90, Mar. 2021, doi: 10.23919/jcin.2021.9387707.

[3] B. T. Yaseen, S. Kurnaz, and S. R. Ahmed, "Detecting and Classifying Drug Interaction using Data mining Techniques," *2022 International Symposium on Multidisciplinary Studies and Innovative Technologies (ISMSIT)*, pp. 952-956, Oct. 2022.

[4] S. R. Ahmed, A. K. Ahmed, and S. J. Jwmaa, "Analyzing The Employee Turnover by Using Decision Tree Algorithm," *2023 5th International Congress on Human-Computer Interaction, Optimization and Robotic Applications (HORA)*, pp. 1-4, Jun. 2023.

[5] N. Z. Mahmood, S. R. Ahmed, A. F. Al-Hayaly, S. Algburi and J. Rasheed, "The Evolution of Administrative Information Systems: Assessing the Revolutionary Impact of Artificial Intelligence," *2023 7th International Symposium on Multidisciplinary Studies and Innovative Technologies (ISMSIT)*, pp. 1-7, 2023.

[6] B. A. Abubaker, S. R. Ahmed, A. T. Guron, M. Fadhil, S. Algburi, and B. F. Abdulrahman, "Spiking Neural Network for Enhanced Mobile Robots' Navigation Control," *2023 7th International Symposium on Innovative Approaches in Smart Technologies (ISAS)*, pp. 1-8, Nov. 2023.

[7] A. K. Ahmed, S. Q. Younus, S. R. Ahmed, S. Algburi, and M. A. Fadhel, "A Machine Learning Approach to Employee Performance Prediction within Administrative Information Systems," *2023 7th International Symposium on Innovative Approaches in Smart Technologies (ISAS)*, pp. 1-7, Nov. 2023.

[8] M. H. B. A. Alkareem, F. Q. Nasif, S. R. Ahmed, L. D. Miran, S. Algburi, and M. T. ALmashhadany, "Linguistics for Crimes in the World by AI-Based Cyber Security," *2023 7th International Symposium on Innovative Approaches in Smart Technologies (ISAS)*, pp. 1-5, Nov. 2023.

[9] S. R. Ahmed, I. Ahmed Najm, A. Talib Abdulqader, and K. Basem Fadhil, "Energy improvement using Massive MIMO for soft cell in cellular communication," *IOP Conference Series: Materials Science and Engineering*, vol. 928, no. 3, p. 032009, Nov. 2020.

[10] M. Al Moteri, S. B. Khan, and M. Alojail, "Machine Learning-Driven Ubiquitous Mobile Edge Computing as a Solution to Network Challenges in Next-Generation IoT," *Systems*, vol. 11, no. 6, p. 308, Jun. 2023, doi: 10.3390/systems11060308.

[11] W. Zhong, S. Hu, Y. Ma, H. Yang, X. Ma, and B. Yu, "Deep Learning-Driven Simultaneous Layout Decomposition and Mask Optimization," *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, vol. 41, no. 3, pp. 709–722, Mar. 2022, doi: 10.1109/tcad.2021.3061494.

[12] H. Bangui and B. Buhnova, "Recent Advances in Machine-Learning Driven Intrusion Detection in Transportation: Survey," *Procedia Computer Science*, vol. 184, pp. 877–886, 2021, doi: 10.1016/j.procs.2021.04.014.

[13] R. Saleem, W. Ni, M. Ikram, and A. Jamalipour, "Deep-Reinforcement-Learning-Driven Secrecy Design for Intelligent-Reflecting-Surface-Based 6G-IoT Networks," *IEEE Internet of Things Journal*, vol. 10, no. 10, pp. 8812–8824, May 2023, doi: 10.1109/jiot.2022.3232360.

[14] M. Amrollahi, S. Hadayeghparast, H. Karimipour, F. Derakhshan, and G. Srivastava, "Enhancing Network Security Via Machine Learning: Opportunities and Challenges," *Handbook of Big Data Privacy*, pp. 165–189, 2020, doi: 10.1007/978-3-030-38557-6_8.

[15] R. Ahmad, R. Wazirali, and T. Abu-Ain, "Machine learning for wireless sensor networks security: An overview of challenges and issues," *Sensors*, vol. 22, no. 13, p. 4730, 2022.

[16] E. Akin, "Deep Reinforcement Learning-Based Multirestricted Dynamic-Request Transportation Framework," *IEEE Transactions on Neural Networks and Learning Systems*, pp. 1–11, 2023, doi: 10.1109/tnnls.2023.3341471.

[17] F. Ullah *et al*., "Cyber Security Threats Detection in Internet of Things Using Deep Learning Approach," *IEEE Access*, vol. 7, pp. 124379–124389, 2019, doi: 10.1109/access.2019.2937347.

[18] S. Strecker, W. Van Haaften, and R. Dave, "An Analysis of IoT Cyber Security Driven by Machine Learning," *Proceedings of International Conference on Communication and Computational Technologies*, pp. 725–753, 2021, doi: 10.1007/978-981-16-3246-4_55.

[19] P. Xiao, "Malware Cyber Threat Intelligence System for Internet of Things (IoT) Using Machine Learning," *Journal of Cyber Security and Mobility*, pp. 53-90, Dec. 2023, doi: 10.13052/jcsm2245-1439.1313.

[20] I. Kotenko, K. Izrailov, and M. Buinevich, "Static Analysis of Information Systems for IoT Cyber Security: A Survey of Machine Learning Approaches," *Sensors*, vol. 22, no. 4, p. 1335, Feb. 2022, doi: 10.3390/s22041335.

[21] A. Rapaka, M. Prasad, R. R. Pbv, P. S. Murty, and K. S. Pokkuluri, "Enhancing Network Security: Leveraging Machine Learning for Intrusion Detection," *Journal of Electrical Systems*, vol. 20, no. 2, pp. 1555-1562, 2024, doi: 10.52783/jes.1460.

[22] R. Padmasree and K. Muthyam, "Enhancing IoT Network Security through Prompt Intrusion Detection Using Machine Learning," *International Journal of Computer Science and Engineering*, vol. 11, no. 4, pp. 10–18, Apr. 2024, doi: 10.14445/23488387/ijcse-v11i4p102.

[23] Z. Zhang, "Machine Learning for Network Intrusion Detection," *Encyclopedia of Cryptography, Security and Privacy*, pp. 1–4, 2021, doi: 10.1007/978-3-642-27739-9_1631-1.

[24] Z. Huang, Z. Li, and J. Zhang, "Enhancing network security through machine learning: A study on intrusion detection system using supervised algorithms," *Applied and Computational Engineering*, vol. 19, no. 1, pp. 50–66, Oct. 2023, doi: 10.54254/2755-2721/19/20231008.

[25] N. Awadallah Awad, "Enhancing Network Intrusion Detection Model Using Machine Learning Algorithms," *Computers, Materials & Continua*, vol. 67, no. 1, pp. 979–990, 2021, doi: 10.32604/cmc.2021.014307.

[26] A. A. Abro, R. S. A. Larik, S. A. Awan, A. O. Panhwar, and I. A. Kandhro, "Network Security Attack Classification: Leveraging Machine Learning Methods for Enhanced Detection and Defense," *International Journal of Electronic Security and Digital Forensics*, vol. 1, no. 1, 2025, doi: 10.1504/ijesdf.2025.10062253.

[27] P. Sukavatee and W. Sutthiroj, "Enhancing English oral communication skills and motivation: the impact of AR hotel situated-learning board game in Thai EFL contexts," *International Journal of Innovation and Learning*, vol. 1, no. 1, 2025, doi: 10.1504/ijil.2025.10064230

[28] D.-S. Tran, N.-H. Ho, H.-J. Yang, S.-H. Kim, and G. S. Lee, "Real-time virtual mouse system using RGB-D images and fingertip detection," *Multimedia Tools and Applications*, vol. 80, no. 7, pp. 10473–10490, Nov. 2020, doi: 10.1007/s11042-020-10156-5.

[29] O. Almomani, "A Feature Selection Model for Network Intrusion Detection System Based on PSO, GWO, FFA and GA Algorithms," *Symmetry*, vol. 12, no. 6, p. 1046, Jun. 2020, doi: 10.3390/sym12061046.

[30] V. Sstla, V. Kolli, and L. Voggu, "Predictive Model for Network Intrusion Detection System Using Deep Learning," *Revue d'Intelligence Artificielle*, vol. 34, no. 3, pp. 323–330, Jun. 2020, doi: 10.18280/ria.340310.

[31] A. M. Mahfouz, D. Venugopal, and S. G. Shiva, "Comparative Analysis of ML Classifiers for Network Intrusion Detection," *Fourth International Congress on Information and Communication Technology*, pp. 193–207, 2020, doi: 10.1007/978-981-32-9343-4_16..

[32] B. He, "Artificial Intelligent for Intelligent Manufacturing and Robotics," *Robotics & Automation Engineering Journal*, vol. 1, no. 5, Jan. 2019, doi: 10.19080/raej.2018.01.555575.

[33] B. Paikaray, P. K. Swain, S. Mohapatra, and S. Satpathy, "Securing Healthcare in the Cloud: A Machine Learning Perspective," *International Journal of Internet Manufacturing and Services*, vol. 11, no. 2, 2025, doi: 10.1504/ijims.2025.10063954.

[34] P. L. S. Jayalaxmi, R. Saha, G. Kumar, M. Conti, and T.-H. Kim, "Machine and Deep Learning Solutions for Intrusion Detection and Prevention in IoTs: A Survey," *IEEE Access*, vol. 10, pp. 121173–121192, 2022, doi: 10.1109/access.2022.3220622.

[35] U. Tariq, "Intrusion Detection and Anticipation System (IDAS) for IEEE 802.15.4 Devices," *Intelligent Automation and Soft Computing*, pp. 1–13, 2018, doi: 10.31209/2018.100000040.

[36] S. A. Bakhsh, M. A. Khan, F. Ahmed, M. S. Alshehri, H. Ali, and J. Ahmad, "Enhancing IoT network security through deep learning-powered Intrusion Detection System," *Internet of Things*, vol. 24, p. 100936, Dec. 2023, doi: 10.1016/j.iot.2023.100936.

[37] E. E. Abdallah and A. F. Otoom, "Intrusion detection systems using supervised machine learning techniques: a survey," *Procedia Computer Science*, vol. 201, pp. 205-212, 2022.

[38] O. Ahmed, R. H. Thaher, and S. R. Ahmed, "Design and fabrication of UWB microstrip Antenna on different substrates for wireless Communication system," in *2022 International Congress on Human-Computer Interaction, Optimization and Robotic Applications (HORA)*, pp. 1-4, 2022.

[39] A. Gupta and R. K. Jha, "Power optimization with low complexity using scaled beamforming approach for a massive MIMO and small cell scenario," *Wireless Networks*, vol. 26, no. 2, pp. 1165-1176, 2020.

[40] I. Al_Barazanchi *et al*., "Proposed New Framework Scheme for Path Loss in Wireless Body Area Network," *Iraqi Journal for Computer Science and Mathematics*, pp. 11–21, Jan. 2022, doi: 10.52866/ijcsm.2022.01.01.002.

[41] Q. Liu, V. Hagenmeyer, and H. B. Keller, "A Review of Rule Learning-Based Intrusion Detection Systems and Their Prospects in Smart Grids," *IEEE Access*, vol. 9, pp. 57542–57564, 2021, doi: 10.1109/access.2021.3071263.

[42] N. Duffield, P. Haffner, B. Krishnamurthy, and H. Ringberg, "Rule-Based Anomaly Detection on IP Flows," *IEEE INFOCOM 2019*, pp. 424-432, Apr. 2009, doi: 10.1109/infcom.2009.5061947.

[43] V. Kumar, D. Sinha, A. K. Das, S. C. Pandey, and R. T. Goswami, "An integrated rule based intrusion detection system: analysis on UNSW-NB15 data set and the real time online dataset," *Cluster Computing*, vol. 23, no. 2, pp. 1397–1418, Oct. 2019, doi: 10.1007/s10586-019-03008-x.

[44] K. Rasane, L. Bewoor, and V. Meshram, "A Comparative Analysis of Intrusion Detection Techniques: Machine Learning Approach," *SSRN Electronic Journal*, 2019, doi: 10.2139/ssrn.3418748.

[45] K. Rajora and N. salih Abdulhussein, "Reviews research on applying machine learning techniques to reduce false positives for network intrusion detection systems," *Babylonian Journal of Machine Learning*, vol. 2023, pp. 26–30, May 2023, doi: 10.58496/bjml/2023/005.

[46] P. Mishra, V. Varadharajan, U. Tupakula, and E. S. Pilli, "A Detailed Investigation and Analysis of Using Machine Learning Techniques for Intrusion Detection," *IEEE Communications Surveys & Tutorials*, vol. 21, no. 1, pp. 686–728, 2019, doi: 10.1109/comst.2018.2847722.

[47] G. J. Pandeeswari and S. Jeyanthi, "Analysis of Intrusion Detection Using Machine Learning Techniques," *2022 Second International Conference on Advanced Technologies in Intelligent Control, Environment, Computing & Communication Engineering (ICATIECE)*, pp. 1-5, Dec. 2022, doi: 10.1109/icatiece56365.2022.10047057.

[48] I. A. Najm *et al*., "Enhanced Network Traffic Classification with Machine Learning Algorithms," *Proceedings of the Cognitive Models and Artificial Intelligence Conference*, pp. 322-327, May 2024, doi: 10.1145/3660853.3660935.

[49] A. S. Dina and D. Manivannan, "Intrusion detection based on Machine Learning techniques in computer networks," *Internet of Things*, vol. 16, p. 100462, Dec. 2021, doi: 10.1016/j.iot.2021.100462.

[50] I. A. Najm, A. K. Hamoud, J. Lloret, and I. Bosch, "Machine Learning Prediction Approach to Enhance Congestion Control in 5G IoT Environment," *Electronics*, vol. 8, no. 6, p. 607, May 2019, doi: 10.3390/electronics8060607.

[51] W. S. Al-Dayyeni *et al*., "A Review on Electronic Nose: Coherent Taxonomy, Classification, Motivations, Challenges, Recommendations and Datasets," *IEEE Access*, vol. 9, pp. 88535–88551, 2021, doi: 10.1109/access.2021.3090165.

[52] I. A. Najm, M. Ismail, J. Lloret, K. Z. Ghafoor, B. B. Zaidan, and A. A. T. Rahem, "Improvement of SCTP congestion control in the LTE-A network," *Journal of Network and Computer Applications*, vol. 58, pp. 119–129, Dec. 2019, doi: 10.1016/j.jnca.2015.09.003.

[53] A. K. Hamoud *et al*., "A comparative study of supervised/unsupervised machine learning algorithms with feature selection approaches to predict student performance," *International Journal of Data Mining, Modelling and Management*, vol. 15, no. 4, pp. 393–409, 2023, doi: 10.1504/ijdmmm.2023.134590.

[54] M. Y. Ma'aji, "Models Comparison Based On Intrusion Detection Using Machine Learning," *SLU Journal of Science and Technology*, pp. 74–86, Mar. 2023, doi: 10.56471/slujst.v6i.358.

[55] I. F. Kilincer, F. Ertam, and A. Sengur, "Machine learning methods for cyber security intrusion detection: Datasets and comparative study," *Computer Networks*, vol. 188, p. 107840, Apr. 2021, doi: 10.1016/j.comnet.2021.107840.

[56] Md. E. Haque and T. M. Alkharobi, "Adaptive Hybrid Model for Network Intrusion Detection and Comparison among Machine Learning Algorithms," *International Journal of Machine Learning and Computing*, vol. 5, no. 1, pp. 17–23, Feb. 2015, doi: 10.7763/ijmlc. 2015.v5.476.

[57] T. Khorram and N. A. Baykan, "Network Intrusion Detection using Optimized Machine Learning Algorithms," *European Journal of Science and Technology*, no. 25, pp. 463-474, Jun. 2021, doi: 10.31590/ejosat.849723.

[58] A. Hamed Hamad, A. Yousif Dawod, M. Fakhrulddin Abdulqader, I. Al_Barazanchi, and H. Muwafaq Gheni, "A secure sharing control framework supporting elastic mobile cloud computing," *International Journal of Electrical and Computer Engineering (IJECE)*, vol. 13, no. 2, p. 2270, Apr. 2023, doi: 10.11591/ijece.v13i2.pp2270-2277.

[59] A. Alghazali and Z. Hanoosh, "Using a Hybrid Algorithm with Intrusion Detection System based on Hierarchical Deep Learning for Smart Meter Communication Network," *Webology*, vol. 19, no. 1, pp. 3850–3865, Jan. 2022, doi: 10.14704/web/v19i1/web19253.

[60] A. Aldallal, "Toward Efficient Intrusion Detection System Using Hybrid Deep Learning Approach," *Symmetry*, vol. 14, no. 9, p. 1916, Sep. 2022, doi: 10.3390/sym14091916.

[61] F. M. Alotaibi, "Network Intrusion Detection Model Using Fused Machine Learning Technique," *Computers, Materials & Continua*, vol. 75, no. 2, 2023.

[62] J. Carneiro, N. Oliveira, N. Sousa, E. Maia, and I. Praça, "Machine Learning for Network-Based Intrusion Detection Systems: An Analysis of the CIDDS-001 Dataset," *Lecture Notes in Networks and Systems*, pp. 148–158, Sep. 2021, doi: 10.1007/978-3-030-86261-9_15.

[63] C. I. Nwakanma *et al*., "Explainable Artificial Intelligence (XAI) for Intrusion Detection and Mitigation in Intelligent Connected Vehicles: A Review," *Applied Sciences*, vol. 13, no. 3, p. 1252, Jan. 2023, doi: 10.3390/app13031252.

[64] S.-Y. Kuo, F.-H. Tseng, and Y.-H. Chou, "Metaverse intrusion detection of wormhole attacks based on a novel statistical mechanism," *Future Generation Computer Systems*, vol. 143, pp. 179–190, Jun. 2023, doi: 10.1016/j.future.2023.01.017.

[65] A. M. Mostafa *et al*., "Strengthening Cloud Security: An Innovative Multi-Factor Multi-Layer Authentication Framework for Cloud User Authentication," *Applied Sciences*, vol. 13, no. 19, p. 10871, Sep. 2023, doi: 10.3390/app131910871.

[66] T. Suleski, M. Ahmed, W. Yang, and E. Wang, "A review of multi-factor authentication in the Internet of Healthcare Things," *Digital Health*, vol. 9, p. 205520762311771, Jan. 2023, doi: 10.1177/20552076231177144.

[67] S. Rawther and S. Sathyalakshmi, "Protecting Cloud Computing Environments from Malicious Attacks Using multi-factor Authentication and Modified DNA Cryptography," *Recent Patents on Engineering*, vol. 18, Sep. 2023, doi: 10.2174/1872212118666230905141926.

[68] I. A. Najm, O. Gheni Abdulateef, A. H. Ali, S. Rashid Ahmed, Mohsin. A. Ahmed, and S. Algburi, "Deep learning detection approach for speech impairment children in Parkinson's disease," *2024 International Congress on Human-Computer Interaction, Optimization and Robotic Applications (HORA)*, pp. 1-6, May 2024, doi: 10.1109/hora61326.2024.10550841.

[69] A. M. Aburbeian and M. Fernández-Veiga, "Secure Internet Financial Transactions: A Framework Integrating Multi-Factor Authentication and Machine Learning," *AI*, vol. 5, no. 1, pp. 177–194, Jan. 2024, doi: 10.3390/ai5010010.

[70] A. A. S. AlQahtani, T. Alshayeb, M. Nabil, and A. Patooghy, "Leveraging Machine Learning for Wi-Fi-Based Environmental Continuous Two-Factor Authentication," *IEEE Access*, vol. 12, pp. 13277–13289, 2024, doi: 10.1109/access.2024.3356351.

[71] https://www.kaggle.com/datasets/sampadab17/network-intrusion-detection.

[72] F. Wang, N. Yang, P. M. Shakeel, and V. Saravanan, "Machine learning for mobile network payment security evaluation system," *Transactions on Emerging Telecommunications Technologies*, vol. 35, no. 4, p. e4226, 2024.

[73] Z. T. Pritee, M. H. Anik, S. B. Alam, J. R. Jim, M. M. Kabir, and M. F. Mridha, "Machine learning and deep learning for user authentication and authorization in cybersecurity: A state-of-the-art review," *Computers & Security*, p. 103747, 2024.

[74] S. Muneer, U. Farooq, A. Athar, M. Ahsan Raza, T. M. Ghazal, and S. Sakib, "A Critical Review of Artificial Intelligence Based Approaches in Intrusion Detection: A Comprehensive Analysis," *Journal of Engineering*, vol. 2024, no. 1, p. 3909173, 2024.

[75] K. S. Gill and A. Dhillon, "A hybrid machine learning framework for intrusion detection system in smart cities," *Evolving Systems*, pp. 1-15, 2024.

[76] I. Wanisha, J. B. James, J. S. Witeno, L. H. M. Bakery, M. Samuel, and M. Faisal, "Multi-Factor Authentication Using Blockchain: Enhancing Privacy, Security and Usability," *International Journal of Computer Technology and Science*, vol. 1, no. 3, pp. 41-55, 2024.

[77] X. Fang *et al*., "Pioneering advanced security solutions for reinforcement learning-based adaptive key rotation in Zigbee networks," *Scientific Reports*, p. 14, 2024.

[78] S. Dhote, P. Maidamwar, and S. Thakur, "Integrating Blockchain and Multi-Factor Authentication for Enhanced Cloud Security in Certificate Verification Systems," in *2024 International Conference on Distributed Computing and Optimization Techniques (ICDCOT)*, pp. 1-7, 2024.

[79] S. A. Babu, A. Ranganath, M. M. Goswami, T. Gnanaprakasam, and M. K. Ishak, "Modified Marine Predators Algorithm With Deep Learning-Driven Security Solution for IoT-Assisted UAV Networks," *IEEE Access*, vol. 12, pp. 54991-54998, 2024.

[80] A. Hamarsheh, "An Adaptive Security Framework for Internet of Things Networks Leveraging SDN and Machine Learning," *Applied Sciences*, vol. 14, no. 11, p. 4530, 2024.

[81] S. E. V. S. Pillai, S. S. Poddar, Y. Nagendar, P. K. Pareek, and P. Zanke, "Automated Cybersecurity Attack Detection Using Prairie Dog Optimization and Multilayer Perceptron in Healthcare System," in *2024 Third International Conference on Distributed Computing and Electrical Circuits and Electronics (ICDCECE)*, pp. 1-6, 2024.