Indonesian Journal of Data and Science

Volume 6 Issue 2
ISSN 2715-9936
https://doi.org/10.56705/ijodas.v6i2.234

Research Article

Assessing Machine Learning Techniques for Cryptographic Attack Detection: A Systematic Review and Meta-Analysis

Bright G. Akwaronwu [1,*], Innocent U. Akwaronwu [2], Oluwabamise J. Adeniyi [3], Ayodeji G. Abiodun [4]

[1] Babcock University, Ilishan-Remo, Nigeria, akwaronwu0329@pg.babcock.edu.ng
[2] The University of Alabama in Huntsville, Alabama, USA, iua0001@uah.edu
[3] Babcock University, Ilishan-Remo, Nigeria, adeniyi0416@pg.babcock.edu.ng
[4] Babcock University, Ilishan-Remo, Nigeria, abiodun0208@pg.babcock.edu.ng

Correspondence should be addressed to Bright G. Akwaronwu; akwaronwu0329@pg.babcock.edu.ng

Received 02 February 2025; Accepted 08 June 2025; Published 31 July 2025

Abstract:

The detection of cryptographic attacks is a vital aspect of maintaining cybersecurity, especially as digital infrastructures become increasingly intricate and susceptible to sophisticated threats. This systematic review aims to examine and compare a range of machine learning approaches applied to cryptographic attack detection, focusing on their performance in terms of detection rates, efficiency, and overall effectiveness. A comprehensive review and meta-analysis were conducted, focusing on existing research that utilized machine learning models for identifying cryptographic attacks. The models included in the review were Naïve Bayes, C4.5, Random Forest, Decision Tree, K-Means, and Particle Swarm Optimization (PSO) combined with Neural Networks. Studies were selected based on their relevance to cryptographic security, with particular attention paid to performance metrics like classification accuracy, precision, recall, and area under the curve (AUC). The findings indicated that the C4.5 decision tree model achieved a high classification rate of 98.8%, while both Random Forest and Decision Tree models performed with an accuracy of 99.9%, making them highly suitable for real-time attack detection. Additionally, the PSO + Neural Network model showed enhanced detection precision, illustrating the value of integrating optimization techniques with machine learning models. The use of machine learning, especially with ensemble methods such as Random Forest and Decision Trees, proves to be highly effective for cryptographic attack detection. The study underscores the necessity for customized machine learning solutions in cybersecurity, balancing both high accuracy and operational efficiency. Further research should focus on the real-world deployment of hybrid models to confirm their practical effectiveness.

Keywords: Attack Detection, Cryptology, Cryptographic Security, Machine Learning Techniques, Risk Prediction, Vulnerability Analysis, Cybersecurity.
Dataset link: -

1. Introduction

The utilization of a network depends on its data integrity, confidentiality and availability, which are core elements in cybersecurity [1], [2]. A fundamental feature of this system is cryptology, which ensures the safeguarding of data both within and across the network [3]. Cyber technology has progressively enhanced data management and transmission processes by enabling a cryptographic platform that ensures secure communication [3], [4], [5]. This advancement in technology is designed to safeguard sensitive information from intruders by encrypting it using secure techniques that can only be decrypted by authorized users, thereby filtering out all malicious attempts to gain access [1].

Cryptology encompasses the scientific study of cryptography and cryptanalysis. It involves the development of secure communication techniques, principles, methods and processes designed to protect information and

communication through the use of codes and ciphers. This includes the comprehensive processes required to ensure secure communication [6], [7]. Cryptology is sub-divided into two fundamental branches which are Cryptography and Cryptanalysis [7].

Cryptanalysis is the study and practice of methods used to break cryptographic systems and algorithms that create codes and ciphers for secure communication [8]. This involves the application of various techniques to conduct a comprehensive analysis of cryptographic systems, aiming to identify vulnerabilities that could be exploited by intruders for malicious purposes [9], [10]. The aim of cryptanalysis is to identify and uncover vulnerabilities in cryptographic protocols and algorithms, preventing unauthorized access to confidential data [11].

Cryptographic attacks are malicious attempts by intruders to exploit vulnerabilities in a system, aiming to gain unauthorized access to confidential information for ulterior motives [12]. The aim of cryptographic attacks is to compromise the CIA triad of a system, which ensures its confidentiality, integrity, and availability [13]. These exploits are achieved through the discovery of weaknesses in the protocol(s), algorithm(s), or the implementation of cryptographic systems [14]. Another potential motive explored by intruders seeking illegitimate access is to impersonate a system, turning it into a zombie and thereby exploiting indirect attacks like Distributed Denial of Service (DDoS) attacks on other systems using the harvested zombie systems [15], [16].

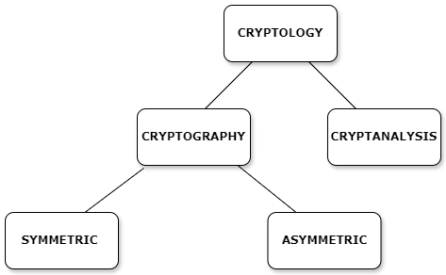

Figure 1. Cryptographic Relationship [17]

Cryptographic attacks are used to exploit vulnerabilities in systems and protocols [18]. These attacks which specifically target encryption and security protocols, include the Birthday Attack, Brute Force Attack, Chosen-plaintext Attack, Cipher-text Only Attack, Known-plaintext Attack, Padding Oracle Attack, and Side-Channel Attack. On the other hand, network attacks, which focus on exploiting network infrastructure and applications such as Cross-Site Scripting (XSS), Denial-of-Service (DoS), Distributed Denial-of-Service, Malware, Man-in-the-Middle, Packet Sniffing, Phishing Attack, and SQL Injection (SQLi) Attacks. These attacks aim to compromise system security by targeting vulnerabilities in confidentiality, integrity, or availability [19]. As networks and cryptographic attacks grow more implicit and complex to detect, the quest for enhanced techniques in protecting data across the network and the entire system also involves methods that will enhance cryptographic attack detection and highlight the intending vulnerable areas liable for exploit, needs continuous growth to ensure ownership of the system [20].

Dubious schemes are often employed to breach cryptographic systems, emphasizing the need for advanced techniques to enhance system protection. This calls for the application of complex methods and models to establish a robust security framework, ensuring access is restricted to authorized users only [21]. There is a progressive increase in exploits that navigate these bonds to gain illegal access, despite the techniques and models programmed to monitor the system. Intruders explore every vulnerable point and attempt to bypass security features for malicious purposes, thereby compromising confidentiality, integrity, and availability. This can result in significant losses, including data breaches, financial losses, and customer dissatisfaction [22].

The advanced utilization of machine learning (ML) techniques in cybersecurity have strengthened the capacity to identify patterns and prevent security threats [23], [24]. Machine learning (ML) is a prevailing technique for analyzing and identifying anomalies and intricate data patterns, enhancing the detection of cryptographic attacks. Its effectiveness in intrusion detection plays a vital role that ensures digital security, and safeguarding data storage [25]. Key features include:

a. Confidentiality: Confidentiality mitigates intrusion by ensuring that only the users with authentic access are capable of accessing the information, protecting data from unauthorized users (intruders) and keeping it safe from every third party [26].
b. Integrity: It ensures that data remain in their original format without alterations, transmission errors, or storage issues, safeguarding their integrity and maintaining consistency [27].
c. Availability: This is a vital asset in network security, ensuring the accessibility and usability of data by authorized users in the expected format. It guarantees reliability and consistency, even when under threat from intruders [27].
d. Authenticity: This confirms the identity of users, guarding against impersonation and ensuring valid and trusted communication. Authentication can be categorized into two forms;
    - Symmetric: This is a cryptographic technique in which the sender shares the same key with the receiver for both encryption and decryption of data on the network [17].
    - Asymmetric: A cryptographic technique, also known as public key cryptography, involves utilizing a pair of key; (i) A public key for encrypting data before sending it across the network, (ii) A private key for decrypting the data on the receiving end [17].
e. Non-Repudiation: This concept is a cryptographic mechanism that authenticates user identities, maintains logs of user actions for verification and accountability, and ensures the integrity and originality of data exchanges.

These machine learning features provide significant leverage in identifying patterns and anomalies on the network. Applying these capabilities to key areas such as cryptographic protocols, key management, hash functions, signature schemes, and side-channel attacks can facilitate the development of advanced detection methods, thereby strengthening the security of cryptographic systems [28]. This requires the development of models capable of learning from both known and unknown attack patterns, identifying anomalies, and uncovering underlying vulnerabilities. The intersection of cryptographic mechanisms and machine learning techniques has opened up a vast field of study, offering a variety of approaches and models to explore and apply in creating a secure environment for safeguarding the digital world [29]. This researech specifically analyzes best practices and recommend best possible machine learning algorithms for personalized and corporate applications.

Rationale

The rationale for conducting this systematic review is based on the need to gain understanding on the varieties of machine learning techniques utilized in detecting cryptographic attacks [30]. This research project will highlight potential vulnerabilities that affects secure storage and flow of data within and across cyber systems [12]. It will assess the effectiveness of utilizing machine learning techniques for proactive and adaptive defense response to prevent intending intrusion and mitigate the impact of cyber attacks and recommend best practices, strategies and possible aftermath for personalized and corporate application.

Aim and Objectives

This research aims to review recent articles that utilized machine learning techniques for cryptographic attack detection and vulnerability analysis to discover best practices and identifying potential pathways for future advancements. It utilizes the PICO recommended framework [31] to drive it objectives as seen in **Table 1**.

Table 1. Objectives of the research

SN	Item	Objectives
i.	Population	Cybersecurity systems and networks susceptible to cryptographic attacks and vulnerabilities.
ii.	Intervention	Implementation of machine learning techniques for cryptographic attack detection and vulnerability analysis.
iii.	Comparison	Comparative analysis of different machine learning algorithms, models, or methodologies applied to cryptographic attack detection and vulnerability analysis.
iv.	Outcome	Evaluation of the effectiveness, efficiency, and robustness of machine learning-based approaches in identifying and mitigating cryptographic attacks. Identification of best practices and strategies for enhancing cryptographic system security through machine

SN	Item	Objectives
		learning techniques.

2. Method:

The PRISMA 2020 Statement [32] method was employed in this research project with the Articles from Scopus and and Google Scholar retrieved on May 8, 2024 and May 13, 2024 respectively. Elimination criteria was applied to exclude articles not relevant to the research objectives, only final articles written in english language was considered for inclusion not negleting the eligibility criteria, inclusive and exlusive criterias listed below.

Eligibility Criteria

The eligibilty criteria for this research project followed the PICO framework [31] as seen in **Table 2**.

Table 2. Inclusion and Exclusion Criterias

SN	Item	Inclusion criteria	Exclusion criteria
i.	Population	Studies focusing on cybersecurity systems and networks vulnerable to cryptographic attacks, including but not limited to governmental and corporate institutions and its networks.	Studies that does not focus on cryptographic attacks and network vulnerabilities.
ii.	Intervention	Research articles and studies that implement machine learning techniques for cryptographic attack detection and vulnerability analysis	Research that did not utilize machine learning techniques to detect or mitigate cryptographic attacks.
iii.	Comparison	Studies comparing different machine learning approaches or traditional methods for cryptographic attack detection and vulnerability analysis	Studies that does not compare or is not eligible to be compared with other machine learning approaches.
iv.	Outcome	Articles reporting on the effectiveness, efficiency, and robustness of machine learning approaches in identifying and mitigating cryptographic attacks	Articles that did not implement machine learning approaches and has no outcome or reports on cryptographic attacks.

These criterias ensures that relevant studies are included while excluding studies that do not meet the specific objectives of the review.

Information Sources

a. Scopus - Wednessday May 8, 2024
   https://www.scopus.com/
b. Google Scholar - Monday May 13, 2024
   https://scholar.google.com/

Search Strategy

The search strategy was meticulously devised to encompass all facets relevant to the investigation of "Cryptographic Attack Detection and Vulnerability Analysis Using Machine Learning Techniques" within the domains of cybersecurity, machine learning, computer science, and related fields. It encompasses research spanning cryptographic attack detection, vulnerability analysis, and the application of machine learning in safeguarding digital systems. The search scope includes studies published in reputable journals and conferences, with a focus on English-language publications from 2013 to 2024.

This strategy aims to capture a comprehensive understanding of the intersection between cryptography, machine learning, and cybersecurity, exploring advancements in machine learning algorithms and methodologies for detecting and mitigating cryptographic attacks. Additionally, it seeks to uncover insights into emerging threats, novel detection techniques, and best practices for enhancing cryptographic system security in an ever-evolving threat landscape.

Selection Process

Table 3. Documents successfully retrieved from database for the research

Database		outcomes
Scopus	TITLE-ABS-KEY (((cryptograph* OR encrypt* OR cyber*) AND (attack OR vulnerability OR threat OR intrusion)) AND (detection OR discovery) AND (vulnerability AND (analysis OR evaluat* OR assessment)) AND ("machine learning" OR "artificial intelligence" OR ai OR "deep learning")) AND PUBYEAR > 2017 AND PUBYEAR < 2025 AND (LIMIT-TO (SUBJAREA , "COMP") OR LIMIT-TO (SUBJAREA , "ENGI") OR LIMIT-TO (SUBJAREA , "MATH") OR LIMIT-TO (SUBJAREA , "DECI") OR LIMIT-TO (SUBJAREA , "NEUR") OR LIMIT-TO (SUBJAREA , "ENVI")) AND (LIMIT-TO (DOCTYPE , "ar")) AND (LIMIT-TO (PUBSTAGE , "final")) AND (LIMIT-TO (SRCTYPE , "j")) AND (LIMIT-TO (LANGUAGE , "English"))	252
Google Scholar	“Cryptographic Attack Detection and Vulnerability Analysis using Machine Learning Technique,”	119

Data Collection Process

Documents retrieved from Scopus were exported in "Comma Separated Value" (CSV) and "Research Information Systems" (RIS) file formats, while documents sourced from Google Scholar were directly saved to Mendeley Reference Manager using the Mendeley browser extension. Both sets of documents were successfully imported into the Mendeley Reference Manager. The final search was conducted on Tuesday, May 14, 2024, and all references were exported to Hubmeta (https://hubmeta.com/) for duplication checks, title screening, and full screening. A total of 371 documents were submitted to Hubmeta for review. After applying both inclusion and exclusion criteria to select relevant articles, 77 articles were retrieved from Hubmeta for manual screening and review.

Data Items

Article bibliographies were retrieved from Scopus on May 8, 2024, using the query strings described in section 2.6, and from Google Scholar on May 13, 2024, using the research title as a query string. A total of 371 documents were retrieved from these two bibliographic databases as follows: Scopus (252) and Google Scholar (119). The screening process excluded files in the following stages: initially, 10 duplicates were identified, and 7 documents were deemed ineligible by the Hubmeta screening tool. The second stage of screening, involving titles and abstracts, excluded 252 documents that were not aligned with the research objectives. Additionally, the full text of 21 documents was unavailable, 1 document was retracted, and the content of 54 documents did not explicitly address the focus of this research project.

Risk of Bias Assessment

The anticipated methods for evaluating bias in each article were devised to align with the focus of the current research on "Cryptographic Attack Detection and Vulnerability Analysis Using Machine Learning Techniques." Bias assessment was conducted at both outcome and study levels, with a specific emphasis on examining the quality and methodology of studies pertaining to cryptographic attack detection and vulnerability analysis using machine learning techniques. At the outcome level, risk of bias was evaluated by scrutinizing the reporting and methodology related to the outcomes of interest, such as the effectiveness of machine learning algorithms in identifying and mitigating cryptographic attacks. This assessment encompassed factors such as the clarity and comprehensiveness of outcome reporting, the appropriateness of statistical analyses, and the potential for outcome misclassification or measurement bias.

Similarly, at the study level, the risk of bias was assessed by considering various factors that could influence the validity of the study findings in the context of cryptographic attack detection and vulnerability analysis. This evaluation included an examination of study design, participant selection methods, potential confounding variables, and sources of bias such as funding sources or conflicts of interest. The information gleaned from assessing the risk of bias in each article was integral to the data integration process, facilitating the analysis and interpretation of findings within the realm of cryptographic attack detection and vulnerability analysis using machine learning techniques. Articles deemed to have a high risk of bias were accorded less weight in the overall analysis, whereas studies with lower risk of bias were prioritized for inclusion, ensuring the robustness and validity of the research outcomes.

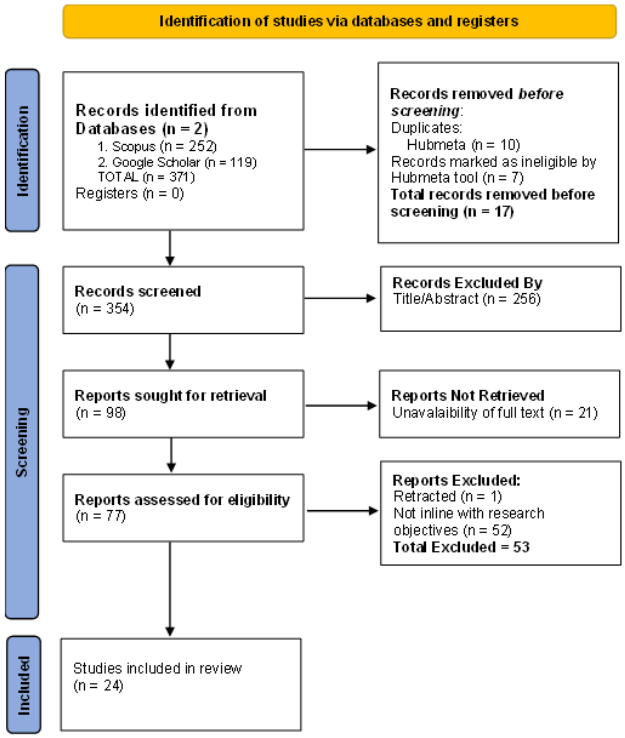

Figure 2. 2020 PRISMA Flowchart [32]

3. Results and Discussion

Results

This research presents a summary of 23 various studies (articles) that focus on different factors influencing the detection of cryptographic attacks, the analysis of vulnerabilities, and the application of machine learning techniques. The included studies analyzed how these factors contribute to outcomes such as the effectiveness of detection methods and the identification of vulnerabilities. By categorizing the studies based on these factors, the research seeks to provide an in-depth analysis of the research landscape in this particular area of study. The document highlights the importance of considering various factors, both technical and methodological, in understanding and improving cryptographic attack detection and vulnerability analysis. **Table 4** below identifies key themes across various studies, contributing to the broader understanding of system security.

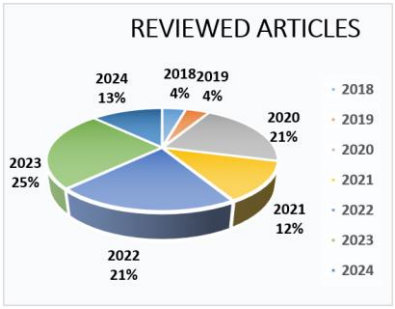

Figure 3. Distribution of Articles by Year (2018-2024)

Below is the comprehensive analysis of 24 articles, capturing key aspects such as their Title, Year of Publication, Methodology, Problem Statement, Identified Research Gap, Dataset used, Performance Metrics, and Results achieved;

Table 4. General Findings of Included Studies

SN	Ref./Yr	Methodology	Problem Statement	Performance
1.	[33] 2020	Text-CNN, XGB, LDA, RF, NB, SVM	The identification of anomalies through machine learning models to track attacka such as ransomware and it likes on user systems	Text-CNN gained an optimal accuracy of 0.989 with a low false positive rate of 0.03. XGB followed-up with 0.931 accuracy and 0.023 lowest false positive rate.
2.	[34] 2023	DT, KNN,	Although cloud computing seems reliable, it is subceptible to external attacks such as brute force attacks. Explosing the optimality of DT and KNN in detecting brute force attack will aid the mitigation of exploit.	The classification of FTP and SSH using DT and KNN yeilded high accuracy for Decision Tree with 0.99954 with a complimentary score of 0.99861 from k-NN. This scores good for both models.
3.	[35] 2021	NB, Bayes Net, KNN, RF and SVM	Conventional security approaches struggle against complex cyber-attacks. IoT devices and 5G networks increases attack exposures especially APT exploit.	The optimal performance with an accuracy of 91.1% is achieved using the Naïve Bayes classifier to detect Advanced Persistent Threat (APT).
4.	[36] 2024	RF, NB, LR	Brute Force Attacks, where attackers try to gain illegal access by attempting different key combinations, are one of the most prevalent network attacks.	DT C4.5D and C4.5N expounded strong performance with AUC values around 0.98-0.99 in both the with-ports and without-ports experiments.
5.	[37] 2023	deep learning-based approach (Bi-flow Features)	Problem of detecting brute force attacks on IoT networks.	The classification results were very high across both feature sets with 99.6% accuracy on Bi-flow feature set and 99.7% on Uni-flow feature set, using hold out validation method
6.	[38] 2023	Deep Learning-based Approach	The defficiency of traditional network security methods like Intrusion Detection systems in detecting complex attacks such as brute-force on FTP and SSH protocols, proposes deep learning-based model to improve detection accuracy and efficiency, and enhance network security.	The proposed model demonstrates optimal performance compared to the existing approaches recorded in the lieterature review.
7.	[39] 2024	Swarm Optimization merged with Support Vector Machine (PSO + SVM)	Need for improved cybersecurity by using machine learning techniques, specially through data preprocessing to counter increasing sophisticaed and frequency of cyber-attacks.	The benign and anomalies are more accurately classified using the SVM algorithm. Better performance metrics are produced by the recommended PCO-SVM techniques.
8.	[40] 2023	Random Forest and Decision Tree for attack detection and SGD for data classification.	Effective need of improved data protection and security within cloud computing environments. Traditional methods face deprivations such as inadequate preprocessing, issues with classifier choices, limited use of multiple classifiers, and reliance on outdated datasets.	The accuracy of RF and DT are 100% of attack detection each. and SGD for 98% accurate data classification. The encryption algorithms adopted are rivest cipher (RC4).
9.	[41] 2019	Decision tree-based Machine Learning techniques	To design an effective intrusion detection system using machine learning techniques, classify the network traffic data using anomalies detection.	Decision tree-based approach enhances IDS performance with improved accuracy and reduced model build time.
10.	[42] 2020	Deep learning model for balanced dataset construction and ensemble attack detection using DNN and DT classifiers.	Integration of IoT and communication networks in ICS raises vulnerability to cyber-attacks. Traditional IDSs lack balance in ICS datasets, resulting in low accuracy.	Outperforms RF, DNN, AdaBoost, and existing models, demonstrating superior attack detection in ICS environments.
11.	[43] 2020	Proposes DeepIDS, a DL approach for intrusion detection in SDN.	SDN promises a dynamic and cost-effective network solution but introduces vulnerabilities. Exploiting these vulnerabilities, attackers can conduct various attacks.	Deep-IDS demonstrates potential for efficient intrusion detection in SDN without affecting OpenFlow controller performance. Trained and tested on NSL-KDD dataset, achieving 80.7% and 90% accuracy with DNN and GRU-RNN models, respectively.
12.	[44] 2020	Online-learning-based DoS Attack Detection Approach	WSNs vulnerable to DoS attacks in hostile environments. Focus on online learning for continual adaptation to new data. Existing online algorithms lack consideration for internal and external data interference.	Proposed method competitive in terms of accuracy, precision, recall, and F1-score, improving DoS attack detection in WSNs.
13.	[45] 2020	Evaluation of Machine Learning Techniques for Phishing Website Detection	Identifying phishing websites is crucial for internet security as online resources become more prominent, aiming to prevent data breaches and ensure safe internet browsing.	Random Forest Classifier identified as the most effective technique for phishing website detection based on evaluation metrics.

SN	Ref./Yr	Methodology	Problem Statement	Performance
14.	[46] 2021	Feature-Based IDS for Smart Grid Systems	Smart grid systems vulnerable to cyber-attacks, risking network integrity and confidentiality. IDS crucial for secure smart grid operation.	Random Forest and Neural Network classifiers outperform others. Achieves 0.5% and 0.08% false alarm rates on KDD99 and NSLKDD datasets respectively. Average detection rate and testing accuracy of 99% for both datasets.
15.	[47] 2018	Self-Organizing Maps (SOM), Ensembles: Bayesian Hidden Markov Model k-Nearest Neighbors (k-NNs), Support Vector Machines (SVMs), Neural Networks (NNs)	To develop a network anomaly detection system (ADS) to identify and flag significant deviations from normal activity, caused by malicious or unauthorized users, and to address the limitations of signature-based automatic detection methods that are unable to detect new types of attacks.	The proposed system of K-means clustering and ID3 decision tree learning methods achieved good results in classification of benign and anomalies.
16.	[48] 2021	Low Power ML Techniques for IoT Botnet Detection	IoT raises security concerns, especially IoT botnet attacks, due to memory and processing limitations of IoT devices. Efficient detection methods needed.	Experimental results show accuracy rate of over 99.99%, true positive rate of 1.000, and false-negative rate of 0.000, indicating successful IoT botnet detection.
17.	[49] 2022	Derives relationship between request arrival time and throughput. Proposes mathematical and ML models for DDoS detection. Uses CAIDA 2007 Dataset and Weka for implementation.	DDoS attacks disrupt server resources, posing severe cyber threats. It applies mathematical and machine learning models to detect DDoS attack using CAIDA 2007 Dataset. Logistic Regression and Naive Bayes are compared.	Logistic Regression outperforms Naive Bayes. Both models contribute to efficient DDoS detection. Real-time datasets used for analysis. Machine learning models achieve 100% accuracy, slightly better than mathematical model (99.75%).
18.	[50] 2022	Proposed method utilizes two feature selection techniques and multiple machine learning classifiers. Evaluated on AWID dataset.	Rapid growth of smart cities reliant on IoT and 5G technologies. Security and privacy challenges arise due to oversight in IoT device security. Injection attacks pose significant threats.	Decision tree classifier achieves 99% accuracy in detecting injection attacks using proposed feature selection method. Outperforms related work.
19.	[51] 2022	Logistic Regression, Stochastic Gradient Descent, Sequential Minimal Optimization, Bayes Network, Instance-Based Learner, Multilayer Perceptron, Naive Bayes, J48	Identifying and preventing SQLIA, a significant cyber threat to web-based applications.	SMO, IBK, and J48 achieved accuracy values of 98.78%, 98.43%, and 98.30% respectively with Cross Validation, and 98.80%, 98.15%, and 100% with Hold-Out.
20.	[52] 2022	Composite of Convolutional Neural Network (CNN) with Long Short-Term Memory (LSTM)	Automatic vulnerability detection is crucial for information security, but traditional methods rely on manual feature definition. Leveraging code metrics and deep learning, a CNN-LSTM model is proposed for objective vulnerability detection.	The CNN-LSTM model outperforms other deep learning-based models with lower false-positive and miss rates, achieving 18% improvement in F1-score compared to previous research.
21.	[53] 2023	V-CNN, CWE (Common Weakness Enumeration) and CVE (Common Vulnerabilities and Exposures)	The increasing prevalence of vulnerabilities leading to actual breaches presents a significant challenge. The escalating number of breaches each year, coupled with the expanding array of vulnerabilities, underscores the urgent need for effective preventive measures.	The V-CNN model demonstrates excellent correctness detection performance in vulnerability detection, outperforming traditional static analysis methods.
22.	[54] 2023	Proposes an intelligent threat detector based on boosted tree algorithms specifically designed and evaluated for IIoT deployments.	Multi-access Edge Computing (MEC) further enhances IIoT by virtualizing networks and services, reducing costs. The proliferation of IIoT also brings an increase in threats and vulnerabilities, making it an attractive target for cybercriminals. IIoT devices, with their limited resources, pose challenges for traditional threat detection solutions designed for other paradigms.	The proposed intelligent threat detector offers a promising solution for addressing security challenges in IIoT environments, demonstrating high efficiency in threat detection and suitability for implementation in real-world scenarios.
23.	[55] 2022	Framework developed using ML and classical techniques. Implemented using Keras and TensorFlow-Learn.	Despite web app popularity, SQLI attacks persist, posing severe security threats. Traditional methods fail to address entire scope of problem.	Proposed framework improves SQLI attack detection and prevention. SVM and ANN identified as weak learners.

SN	Ref./Yr	Methodology	Problem Statement	Performance
		Hybrid approach (ANN and SVM).		
24.	[56] 2024	Evaluation of Machine Learning Algorithms for IDS Web Attacks Detection. Models: RF, NB, kNN	Effective detection of web attacks is crucial for the security of web applications, necessitating a robust intrusion detection system (IDS) with accurate traffic classification.	RF outperformed NB and KNN in average accuracy during training. KNN achieved the highest average accuracy of 99.4916% during testing. RF and KNN achieved 100% average precision and recall rates, identifying them as the most effective algorithms.

Findings

The methodology employed for the experiment includes OpenStack Juno as the open source software utilized in construction of public, private, and hybrid clouds. Oracle Virtual Box was used as base environment for the systems, and Hyping was utilized to generate attacks. For monitoring, Wireshark and IP Traffic monitoring were used. The experimental setup was done in a virtual environment with VMs and virtual LAN due to ethical and legal issues. This was utilizing to detect DDoS flooding attacks, and the generation of normal network traffic was done using a parameterized python-scripts [57].

The unsupervised anomaly detection system showed high performance and accuracy in detecting cyber-attacks in large-scale smart grids. The results show that the system can optimally detect an attack with about 99% accuracy and 98% True Positive Rate (TPR) [44]. The algorithm has very high TPR (94%) and Accuracy (90%) having about 35% dotted measure.

The Decision Tree and Random Forest classifier algorithm are recommended for DDoS flooding attacks [57]. In line with detecting cyber-attacks, Deep Neural Networks (DNNs) and Convolutional Neural Networks (CNNs) are effective for vulnerability detection, achieving high accuracy ratings [52], [53]. Both supervised and unsupervised learning methods are highlighted as effective for cyber threat detection. Supervised methods, such as Random Forests, K-Nearest Neighbor (KNN), Support Vector Machines (SVM), and Naive Bayes classifiers, are suitable for detecting phishing attacks [45]. Unsupervised methods, including Self-Organizing Maps (SOM) and it likes are useful in detecting threats like botnet attacks and false data injection attacks [42], [58], [59].

Valuable insights into the application of various machine learning models for different types of cyber threats serves as a quick reference for selecting appropriate machine learning techniques, classifier algorithms, and learning types to enhance cybersecurity measures.

Table 5. Classification Performance Measure

Ref.	SN	Models	Detection Time (sec)	Correct Classification (%)
[57]	1.	Naive Bayesian	1.25	91.4
	2.	C4.5	0.58	98.8
	3.	K-Means	1.12	95.9
[48]	4.	Random Forest (RF)	-	99.9
	5.	Decision Tree (DT)	-	99.9

Table 5 presents a comparative analysis of the performance measures for various machine learning models used in the detection of cyber threats. The key performance indicators assessed are detection time (in seconds) and correct classification percentage. The Naive Bayesian model [57] exhibits a relatively longer detection time of 1.25 seconds and a correct classification rate of 91.4%. This indicates that while it may not be the fastest, it maintains a reasonable level of accuracy, making it suitable for applications where computational speed is less critical than classification accuracy. The C4.5 decision tree algorithm [57] demonstrates a quick detection time of 0.58 seconds and a high correct classification rate of 98.8%. This makes it an excellent choice for real-time detection systems where both speed and precision are crucial. Similarly, the K-Means model [57] provides a balance between detection time and accuracy, with a detection time of 1.12 seconds and a correct classification rate of 95.9%, making it effective for environments

requiring moderately fast detection without significant loss of accuracy. Random Forest (RF) and Decision Tree (DT) models [48] achieve the highest correct classification rate of 99.9%. These models are highly reliable for accurate identification of cyber threats, making them ideal for scenarios where precision is paramount.

Table 6. Detection Rate (DR) Analysis

Ref.	SN	Models	DR
[46]	1.	PSO + KNN	99.7
	2.	PSO + Neural Network	99.2
	3.	PSO + Decision Tree	99.6
	4.	PSO + Random Forest	99.6

These ensemble learning techniques are particularly powerful for this application, demonstrating their superior ability to accurately classify cryptographic attacks. **Table 6** underscores the efficacy of ensemble methods in achieving optimal performance in cryptographic attack detection, offering valuable insights for selecting the most appropriate models for cybersecurity systems. The analysis reveals that the models have high detection rates ranging from 99.2% to 99.7%

Table 7. Performance Measure (AUC)

Ref.	SN	MODELS	AUC
[45]	1.	KNN	0.94
	2.	Logistic Regression	0.96
	3.	Stochastic Gradient Descent (SGD)	0.97
	4.	Logistic Regression CV	0.98
	5.	Bagging	0.99
	6.	Extra Trees	1.00
	7.	Random Forest	1.00
[33]	8.	Text-CNN	1.0
	9.	XGB	0.89

Table 7 presents the performance measures of various machine learning models used for cryptographic attack detection, focusing on the Area Under the Curve (AUC) metric. The AUC metric is crucial for evaluating the overall performance of classification models. The K-Nearest Neighbor (KNN) model achieves an AUC of 0.94, indicating a strong ability to distinguish between classes, though it is slightly less effective compared to the other models listed.

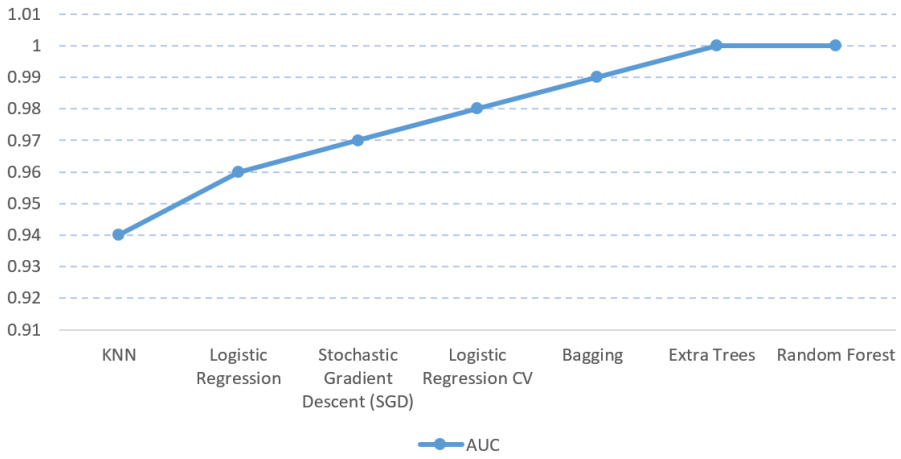

Figure 4. AUC Reference Distribution

Logistic Regression and Stochastic Gradient Descent (SGD) models show improved performance, with AUC values of 0.96 and 0.97, respectively. Logistic Regression CV, an extension of logistic regression with cross-validation, further enhances performance with an AUC of 0.98. These models are effective for cryptographic attack detection, providing a good balance between complexity and performance. Bagging, Extra Trees, and Random Forest models exhibit the highest AUC values, with Bagging achieving 0.99 and both Extra Trees and Random Forest achieving a perfect AUC of 1.00.

Table 8. Performance Measure (Accuracy %)

SN	Ref.	Models	Accuracy (%)	SN	Ref.	Models	Accuracy (%)
1.	[41]	MultinomialNB	90.69	14.	[43]	DNN	80.70
2.		BernoulliNB	95.33	15.		GRU-RNN	**90.00**
3.		GaussianNB	96.71	**16.**	[50]	Decision tree	96.81
4.	[42]	Gas Pipeline	95.86	17.		Random forest	98.88
5.		SWAT	99.67	**18.**		SVM	97.58
6.	[44]	J48	98.64	19.	[52]	CNN-LSTM	91.00
7.		MLP	98.63	20.	[53]	V-CNN	98.00
8.		Random Forest	98.10	**21.**		Random Forest	95.00
9.		Naïve Bayes	96.93	22.	[33]	Text-CNN	98.90
10.	[46]	PSO + KNN	99.30	23.		XGB	93.08
11.		PSO + Neural Network	99.20	24.	[34]	DT-Benign	100
12.		PSO + Decision Tree	99.50	25.		DT-FTP	100
13.		PSO + Random Forest	99.60	26.		DT-SSH	100

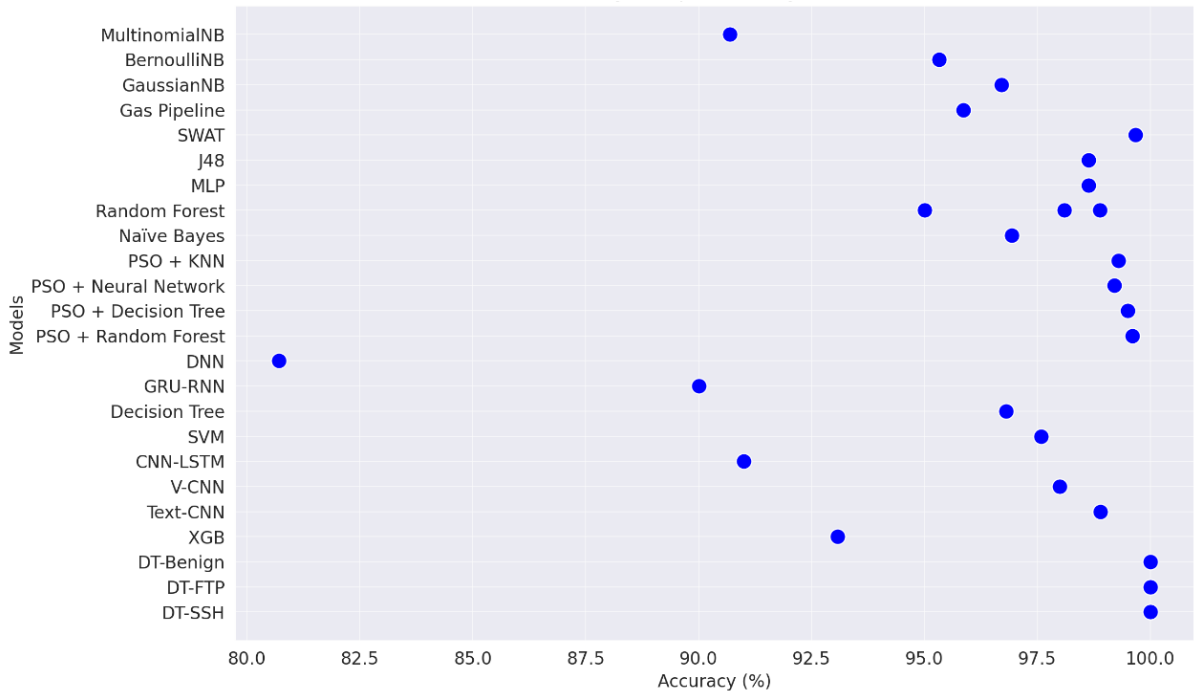

Figure 5. Accuracy Performance Across Model

Table 9. Performance Measure (Precision,Recall,F-Measure '%')

Ref.	SN	Models	Precision (%)	Recall (%)	F-Measure (%)
[41]	1.	MultinomialNB	86.74	81.97	84.30
	2.	BernoulliNB	96.45	90.33	93.29
	3.	**GaussianNB**	**97.28**	**94.90**	**96.02**
[42]	4.	Gas Pipeline	94.63	93.72	93.83
	5.	SWAT	**97.00**	**99.00**	**99.00**
[43]	6.	DNN	85.00	81.00	81.00
	7.	GRU-RNN	**89.00**	**89.00**	**89.00**
[45]	8.	Support Vector Machine	89.00	89.00	89.00
	9.	KNN (0.82-0.89 – 0.86)	86.00	86.00	86.00
	10.	Logistic Regression (0.85 to 0.9 – 0.88)	88.00	88.00	88.00
	11.	Stochastic gradient Descent (0.8 to 0.9 – 0.85)	85.00	85.00	85.00
	12.	logistic regressionCV	95.00	95.00	95.00
	13.	Bagging	98.00	98.00	98.00
	14.	**Random Forest**	**99.00**	**99.00**	**99.00**
[46]	15.	PSO + KNN	98.80	97.60	98.20
	16.	**PSO + Neural Network**	**95.40**	**99.60**	**97.50**
	17.	PSO + Decision Tree	98.50	99.20	98.80
	18.	**PSO + Random Forest**	**98.50**	**99.30**	**98.90**
[50]	19.	Decision tree	67.31	85.00	75.13
	20.	Random forest (2)	95.11	84.70	89.60
	21.	SVM	70.08	99.99	82.40
[52]	22.	CNN-LSTM	92.00	99.00	95.00
[33]	23.	Text-CNN	-	-	97.96
	24.	XGB	-	-	85.57
[34]	25.	**DT-Benign**	**99.97**	**99.97**	**99.98**
	26.	DT-FTP	99.87	98.96	99.13
	27.	DT-SSH	99.13	99.07	99.10

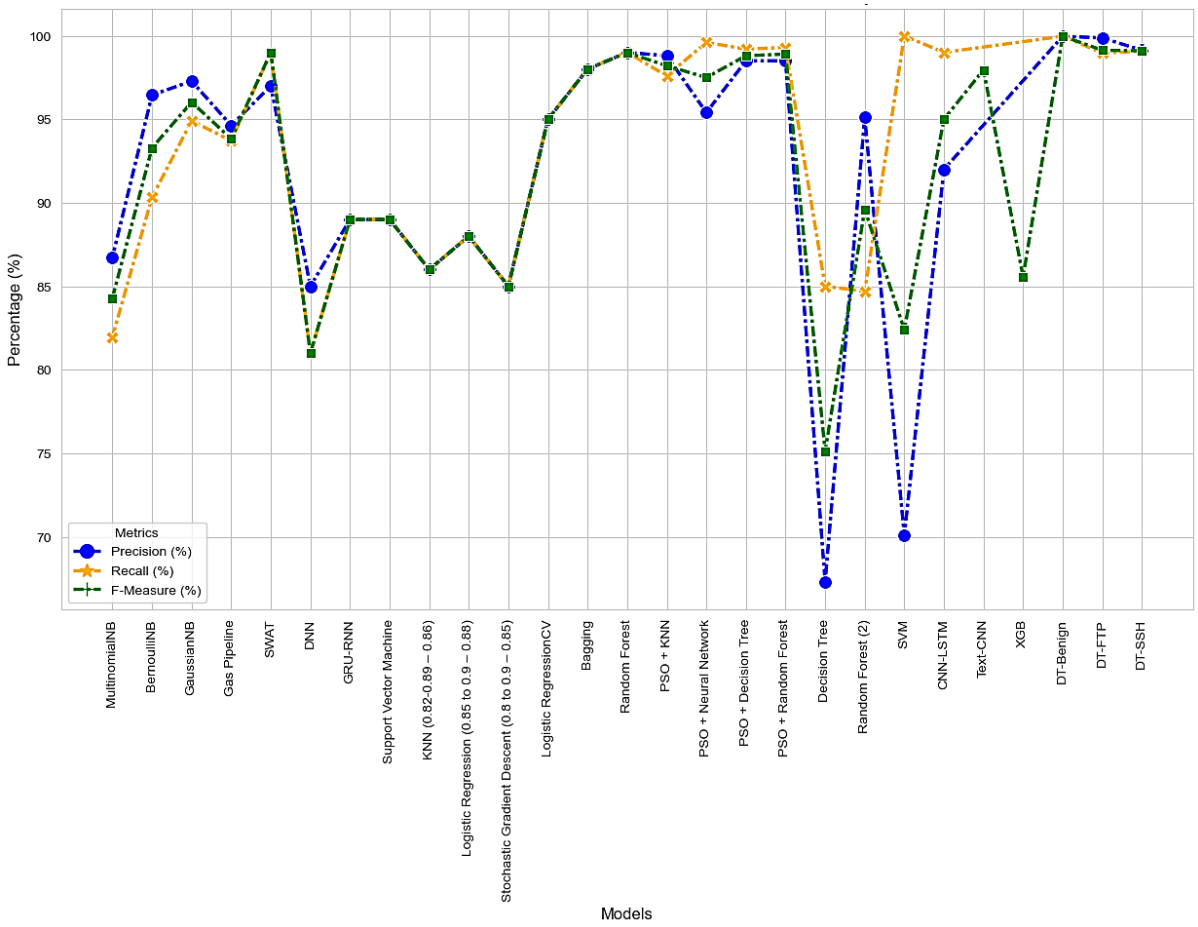

Figure 6. Accuracy, Precision And Recall Performance Analysis

In **Table 8** and **Table 9**, various models are evaluated based on their performance measures including accuracy, precision, recall, and F-measure percentages. Here is a comprehensive analysis focusing on the most used models, the best-performing models, and a recommendation for further application:

Most Used Models

- Random Forest: Random Forest appears multiple times in the table with high accuracy percentages ranging from 95.00% to 99.53% . It is a popular ensemble learning method known for its robustness and accuracy in classification tasks.
- GaussianNB: Gaussian Naive Bayes is another frequently used model with accuracy percentages ranging from 96.71% to 95.33% . It is a simple yet effective probabilistic classifier based on Bayes' theorem with the assumption of independence between features.

Best-Performing Models

- PSO + Random Forest and PSO + Neural Network: The combination of Particle Swarm Optimization (PSO) with Random Forest and Neural Network models achieved high accuracy, precision, recall, and F-measure, with values ranging from 95.40% to 99.60%. This demonstrates the superior performance of these hybrid models in classification tasks.
- SWAT: The SWAT model stands out with an impressive accuracy of 99.67% and high precision, recall, and F-measure percentages . This model showcases exceptional performance in the evaluated metrics.

Discussion

The findings highlight the efficacy of several machine learning (ML) techniques in detecting cryptographic attacks, emphasizing the importance of effective model selection. Decision Tree (C4.5) and Random Forest gave optimal performance scoring 99.9% across precision, recall and f-1 score, making them highly reliable for threat identification. Other supervised learning approaches such as Naïve Bayes, K-Nearest Neighbors (KNN), and Support Vector Machines (SVM) are discovered suitable for phishing and intrusion detection. The comparative analysis of detection time and classification accuracy showed that while Naïve Bayesian classifiers offer good accuracy, their detection time is relatively high, making them less ideal for real-time applications. C4.5 and ensemble methods like Particle Swarm Optimization (PSO) with Random Forest provided a balance between speed and accuracy.

Strategies for Implementing Machine Learning in Cryptographic Systems

The deployment of machine learning (ML) models in cryptographic attack detection requires a structured approach that ensures efficiency, adaptability, and real-time threat mitigation. ML models must be optimized for real-time attack detection. This involves ensuring algorithm efficiency and reducing model complexity. **Table 10** highlight the techniques used in the reviewed articles with optimal performance.

Table 10. ML Implementation Strategies

Model	Implementation
The Random Forest (RF) [45]	RF model, optimized for performance, is implemented as an ensemble learning approach that aggregates predictions from multiple decision trees. Utilization of Bootstrap aggregation enhanced efficiency, increasing diversity in decision-making and reducing model variance. The model employs feature randomness, selecting random subsets at each split to prevent dominance by correlated attributes and improve generalization across attack scenarios. Gini impurity was used for feature selection, optimizing the model's ability to distinguish normal from attack-related activities. This ensured accurate detection of complex cryptographic attacks while maintaining robustness against noise and overfitting.
PSO + Neural Network [46]	Weighted PSO improves feature selection by prioritizing the most relevant attributes, which enhances classification accuracy. The refined features are subsequently input into a Multilayer Perceptron (MLP) neural network, ensuring that the model processes the most relevant data for identifying intrusions effectively. Once feature selection is complete, the Neural Network (NN) model is designed and trained to classify network traffic effectively. The MLP architecture consists of an input layer, multiple hidden layers (typically 60), and an output layer. The ReLU activation function is applied to introduce non-linearity, enhancing the network's ability to detect complex attack patterns. Training is performed using backpropagation with adaptive weight updates, ensuring fast and stable learning. Hyperparameters like batch size, learning rate ($\alpha = 0.0001$), and maximum iterations (Max-Iter = 200) are cautiously adjusted to ensure model accuracy. To prevent overfitting, dropout regularization is applied, allowing the model to generalize well to new data.
DT-Benign [34]	In implementing Decision Tree (DT) model, the dataset is properly preprocessed by handling missing values, removing redundant attributes and normalizing numerical features for consistency. The dataset is split for training and testing (7:3) and the model is trained using entropy as the splitting criterion. The training process involves tuning hyperparameters such as tree depth and minimum samples per split to prevent overfitting while maintaining high classification accuracy. The deployed model analyzes key attributes such as packet length mean, destination port, and flow rate to assess whether a network request is indicative of anomalous behaviour. To strengthen its reliability, continuous monitoring and periodic retraining are implemented, allowing the model to adapt to emerging attack techniques. Logging and alerting mechanisms are essential for ensure timely action against potential threats.

Recommendation

Based on the analysis of Findings, it is recommended to consider the following for further application:

- Ensemble Methods: Given the success of Random Forest and Bagging models in achieving high accuracy percentages, further exploration of ensemble methods could be beneficial. Techniques like boosting and stacking could be investigated to potentially enhance classification performance.
- Hybrid Models: Models combining optimization algorithms like PSO with powerful classifiers such as Random Forest show promise in achieving superior results. Exploring hybrid models that leverage the strengths of different algorithms could lead to improved performance in various domains.
- Model Selection: Depending on the specific requirements of the classification task, it is essential to carefully select the appropriate model. Consider factors such as interpretability, computational efficiency, and the nature of the dataset when choosing a model for application

The analysis of **Table 9** highlights the effectiveness of certain models in achieving high performance in classification tasks. By leveraging the strengths of top-performing models and exploring innovative approaches, researchers and practitioners can enhance the accuracy and reliability of classification systems in various domains.

The research project applied the application of varioius machine learning models for combating a spectrum of cyber threats, as evidenced by the detailed analyses the tailored selection of models for specific cyber threat scenarios, emphasizing the significance of employing appropriate learning methods and classifier algorithms. Notably, supervised techniques like Random Forests and KNN are adept at detecting phishing attacks, while unsupervised methods such as SOM and DBN excel in identifying botnet attacks and false data injections. The recommendation of Decision Tree methodology for DDoS flooding attacks and the effectiveness of DNNs and CNNs for vulnerability detection underscore the versatility and efficacy of machine learning in cybersecurity.

Table 9 provides a comparative analysis of performance measures across various machine learning models, shedding light on the trade-offs between detection time and correct classification percentage. Models like Naive Bayesian exhibit commendable accuracy albeit with longer detection times, making them suitable for scenarios prioritizing precision over speed. Conversely, the C4.5 decision tree algorithm stands out for its rapid detection time and high accuracy rate, ideal for real-time detection systems. The Random Forest and Decision Tree models emerge as top performers in terms of correct classification rate, emphasizing their reliability in precise threat identification.

General Interpretation of Results

The research project's findings contribute valuable knowledge to the realm of cybersecurity, offering practical guidance for bolstering cryptographic attack detection and vulnerability analysis through the strategic application of machine learning and deep learning techniques. It provides insights into the strengths and weaknesses of each model, contributing to enhanced cryptographic attack detection and vulnerability analysis.

Limitations of Evidence

This research has certain limitations, including its reliance on a simulated environment, which may not fully reflect real-world conditions. Additionally, assumptions regarding DDoS attack characteristics and network behavior could impact the accuracy of findings. Another concern is the potential for false positives and false negatives, which may affect the model’s reliability in practical deployment scenarios [60]. These limitations and gaps requires further examination to improve the accuracy and practicality of DDoS attack detection [61]. In addition, the dataset utilized by various models are not aggregately quantified to output equal measures of performance thereby limiting the baseline of the results

4. Conclusion

The research project's comprehensive exploration of machine learning models for cybersecurity applications underscores the critical role of tailored model selection in addressing diverse cyber threats effectively. By leveraging supervised and unsupervised learning methods, organizations can enhance their threat detection capabilities across a spectrum of attack vectors. The performance analysis provides valuable insights that help in making informed decisions about using machine learning models. It highlights the need to balance detection time and classification accuracy. Notably, the Random Forest and Decision Tree models achieved the highest correct classification rate of

99.9%, proving their reliability in accurately identifying threats. This outcome value reinforces the notion that these models are not only highly accurate but also excel in swiftly detecting cyber threats. Therefore, organizations seeking optimal precision in threat identification can confidently rely on Random Forest and Decision Tree models for robust cybersecurity defense strategies.

By leveraging the performance outcomes of specific models, organizations can make informed decisions to fortify their cybersecurity posture and proactively combat evolving cyber threats with enhanced accuracy and efficiency. Utilizing an algorithm that can blend cryptographic algorithm and machine learning to detect ransomware will aid optimal protection of cryptographic systems [33].

References:

[1] M. A. Yalçınkaya and E. U. Küçüksille, "Artificial Intelligence and Dynamic Analysis-Based Web Application Vulnerability Scanner," *ISeCure*, vol. 16, no. 1, pp. 55–77, 2024, doi: 10.22042/isecure.2023.367746.847.

[2] M. A. Ferrag, M. Babaghayou, and M. A. Yazici, "Cyber security for fog-based smart grid SCADA systems: Solutions and challenges," *J. Inf. Secur. Appl.*, vol. 52, 2020, doi: 10.1016/j.jisa.2020.102500.

[3] M. Basnet and M. H. Ali, "Exploring cybersecurity issues in 5G enabled electric vehicle charging station with deep learning," *IET Gener. Transm. Distrib.*, vol. 15, no. 24, pp. 3435–3449, 2021, doi: 10.1049/gtd2.12275.

[4] B. A. Alabsi, M. Anbar, and S. D. A. Rihan, "CNN-CNN: Dual Convolutional Neural Network Approach for Feature Selection and Attack Detection on Internet of Things Networks," *Sensors*, vol. 23, no. 14, 2023, doi: 10.3390/s23146507.

[5] M. Sherafatian and F. Arjmand, "Decision tree-based classifiers for lung cancer diagnosis and subtyping using TCGA miRNA expression data," *Oncol. Lett.*, vol. 18, no. 2, pp. 2125–2131, 2019, doi: 10.3892/ol.2019.10462.

[6] J.-S. Coron, "What is cryptography?," *IEEE Secur. Priv. Mag.*, vol. 4, no. 1, pp. 70–73, Jan. 2006, doi: 10.1109/MSP.2006.29.

[7] P. Mathews, A. Gaikwad, … M. U.-… M. L., and undefined 2024, "Introduction to Modern Cryptography and Machine Learning," *igi-global.com*, Accessed: May 07, 2024.

[8] "Hash Functions," in *Applied Cryptanalysis*, Wiley, 2007, pp. 193–264. doi: 10.1002/9780470148778.ch5.

[9] Y. Li and Q. Liu, "A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments," *Energy Reports*, vol. 7, pp. 8176–8186, Nov. 2021, doi: 10.1016/j.egyr.2021.08.126.

[10] V. Vasani, A. K. Bairwa, S. Joshi, A. Pljonkin, M. Kaur, and M. Amoon, "Comprehensive Analysis of Advanced Techniques and Vital Tools for Detecting Malware Intrusion," *Electronics*, vol. 12, no. 20, p. 4299, Oct. 2023, doi: 10.3390/electronics12204299.

[11] A. Sarkar, S. R. Chatterjee, and M. Chakraborty, "Role of Cryptography in Network Security," 2021, pp. 103–143. doi: 10.1007/978-981-15-9317-8_5.

[12] Ö. Aslan, S. S. Aktuğ, M. Ozkan-Okay, A. A. Yilmaz, and E. Akin, "A Comprehensive Review of Cyber Security Vulnerabilities, Threats, Attacks, and Solutions," *Electronics*, vol. 12, no. 6, p. 1333, Mar. 2023, doi: 10.3390/electronics12061333.

[13] Q. Covert, D. Steinhagen, M. Francis, and K. Streff, "Towards a Triad for Data Privacy," 2020. doi: 10.24251/HICSS.2020.535.

[14] M. Tarawneh, "Cryptography: Recent Advances and Research Perspectives," in *Cryptography - Recent Advances and Research Perspectives [Working Title]*, IntechOpen, 2023. doi: 10.5772/intechopen.111847.

[15] Z. Alkhalil, C. Hewage, L. Nawaf, and I. Khan, "Phishing Attacks: A Recent Comprehensive Study and a New Anatomy," *Front. Comput. Sci.*, vol. 3, Mar. 2021, doi: 10.3389/fcomp.2021.563060.

[16] E. Gyamfi and A. Jurcut, "Intrusion Detection in Internet of Things Systems: A Review on Design Approaches Leveraging Multi-Access Edge Computing, Machine Learning, and Datasets," *Sensors*, vol. 22, no. 10, p. 3744, May 2022, doi: 10.3390/s22103744.

[17] A. D. Dwivedi, "BRISK: Dynamic Encryption Based Cipher for Long Term Security," *Sensors*, vol. 21, no. 17, p. 5744, Aug. 2021, doi: 10.3390/s21175744.

[18] K. Tsantikidou and N. Sklavos, "Threats, Attacks, and Cryptography Frameworks of Cybersecurity in Critical Infrastructures," *Cryptography*, vol. 8, no. 1, p. 7, Feb. 2024, doi: 10.3390/cryptography8010007.

[19] J. Ding, A. Qammar, Z. Zhang, A. Karim, and H. Ning, "Cyber Threats to Smart Grids: Review, Taxonomy, Potential Solutions, and Future Directions," *Energies*, vol. 15, no. 18, 2022, doi: 10.3390/en15186799.

[20] L. Vigoya, D. Fernandez, V. Carneiro, and F. J. Nóvoa, "IoT dataset validation using machine learning techniques for traffic anomaly detection," *Electron.*, vol. 10, no. 22, 2021, doi: 10.3390/electronics10222857.

[21] P. M. Johnson, W. Barbour, J. V Camp, and H. Baroud, "Using machine learning to examine freight network spatial vulnerabilities to disasters: A new take on partial dependence plots," *Transp. Res. Interdiscip. Perspect.*, vol. 14, 2022, doi: 10.1016/j.trip.2022.100617.

[22] A. Aziz and S. Mirzaliev, "Optimizing Intrusion Detection Mechanisms for IoT Network Security," *J. Cybersecurity Inf. Manag.*, vol. 13, no. 1, pp. 60–68, 2024, doi: 10.54216/JCIM.130106.

[23] J. Yang, C. Fu, F. Deng, M. Wen, X. Guo, and C. Wan, "Toward Interpretable Graph Tensor Convolution Neural Network for Code Semantics Embedding," *ACM Trans. Softw. Eng. Methodol.*, vol. 32, no. 5, 2023, doi: 10.1145/3582574.

[24] "Cryptographic Attack Detection and Vulnerability... - Google Scholar." Accessed: May 07, 2024.

[25] "Cryptographic Attack Detection and Vulnerability... - Google Scholar." Accessed: May 07, 2024.

[26] X. Zheng, "Computer Deep Learning Network Security Vulnerability Detection Based on Virtual Reality Technology," *Adv. Multimed.*, vol. 2022, 2022, doi: 10.1155/2022/6039690.

[27] A. Salam *et al.*, "Securing Smart Manufacturing by Integrating Anomaly Detection with Zero-Knowledge Proofs," *IEEE Access*, vol. 12, pp. 36346–36360, 2024, doi: 10.1109/ACCESS.2024.3373697.

[28] R. Zhang, S. Hussain, H. Chen, M. Javaheripi, and F. Koushanfar, "Systemization of Knowledge: Robust Deep Learning using Hardware-software co-design in Centralized and Federated Settings," *ACM Trans. Des. Autom. Electron. Syst.*, vol. 28, no. 6, 2023, doi: 10.1145/3616868.

[29] A. Yazhari Kermani, A. Abdollahi, and M. Rashidinejad, "Cyber-secure energy and flexibility scheduling of interconnected local energy networks with introducing an XGBoost-assisted false data detection and correction method," *Int. J. Electr. Power Energy Syst.*, vol. 155, 2024, doi: 10.1016/j.ijepes.2023.109683.

[30] H. Mohajan and H. K. Mohajan, "Munich Personal RePEc Archive Two Criteria for Good Measurements in Research: Validity and Reliability Two Criteria for Good Measurements in Research: Validity and Reliability," 2017.

[31] M. Amir-Behghadami and A. Janati, "Population, Intervention, Comparison, Outcomes and Study (PICOS) design as a framework to formulate eligibility criteria in systematic reviews," *Emerg. Med. J.*, vol. 37, no. 6, pp. 387–387, Jun. 2020, doi: 10.1136/emermed-2020-209567.

[32] M. J. Page *et al.*, "The PRISMA 2020 statement: an updated guideline for reporting systematic reviews," *BMJ*, p. n71, Mar. 2021, doi: 10.1136/bmj.n71.

[33] N. Niture, "Machine Learning and Cryptographic Algorithms – Analysis and Design in Ransomware and Vulnerabilities Detection," Oct. 2020, doi: 10.36227/techrxiv.13146866.v1.

[34] M. F. Kamarudin Shah, M. Md-Arshad, A. Abdul Samad, and F. A. Ghaleb, "Comparing FTP and SSH Password Brute Force Attack Detection using k-Nearest Neighbour (k-NN) and Decision Tree in Cloud Computing," *Int. J. Innov. Comput.*, vol. 13, no. 1, pp. 29–35, May 2023, doi: 10.11113/ijic.v13n1.386.

[35] Y. Ahmed, A. T. Asyhari, and M. Rahman, "A Cyber Kill Chain Approach for Detecting Advanced Persistent Threats," *Comput. Mater. Contin.*, vol. 67, no. 2, pp. 2497–2513, 2021, doi: 10.32604/cmc.2021.014223.

[36] A. Ali Hamza and R. Jumma surayh Al-Janabi, "Detecting Brute Force Attacks Using Machine Learning," *BIO Web Conf.*, vol. 97, p. 00045, Apr. 2024, doi: 10.1051/bioconf/20249700045.

[37] A. F. Otoom, W. Eleisah, and E. E. Abdallah, "Deep Learning for Accurate Detection of Brute Force attacks on IoT Networks," *Procedia Comput. Sci.*, vol. 220, pp. 291–298, 2023, doi: 10.1016/j.procs.2023.03.038.

[38] N. Alotibi and M. Alshammari, "Deep Learning-based Intrusion Detection: A Novel Approach for Identifying Brute-Force Attacks on FTP and SSH Protocol," *Int. J. Adv. Comput. Sci. Appl.*, vol. 14, no. 6, 2023, doi: 10.14569/IJACSA.2023.0140612.

[39] N. Omer, A. H. Samak, A. I. Taloba, and R. M. A. El-Aziz, "Cybersecurity Threats Detection Using Optimized Machine Learning Frameworks," *Comput. Syst. Sci. Eng.*, vol. 48, no. 1, pp. 77–95, 2024, doi: 10.32604/csse.2023.039265.

[40] A. A. Jabbar and W. S. Bhaya, "Security of private cloud using machine learning and cryptography," *Bull. Electr. Eng. Informatics*, vol. 12, no. 1, pp. 561–569, Feb. 2023, doi: 10.11591/eei.v12i1.4383.

[41] S. Shilpashree, S. C. Lingareddy, N. G. Bhat, and G. Sunil Kumar, "Decision tree: A machine learning for intrusion detection," *Int. J. Innov. Technol. Explor. Eng.*, vol. 8, no. 6 Special Issue 4, pp. 1126–1130, 2019, doi: 10.35940/ijitee.F1234.0486S419.

[42] A. Al-Abassi, H. Karimipour, A. Dehghantanha, and R. M. Parizi, "An ensemble deep learning-based cyber-attack detection in industrial control system," *IEEE Access*, vol. 8, pp. 83965–83973, 2020, doi: 10.1109/ACCESS.2020.2992249.

[43] T. A. Tang, L. Mhamdi, D. McLernon, S. A. R. Zaidi, M. Ghogho, and F. E. Moussa, "DeepIDS: Deep learning approach for intrusion detection in software defined networking," *Electron.*, vol. 9, no. 9, pp. 1–18, 2020, doi: 10.3390/electronics9091533.

[44] P. S. Saini, S. Behal, and S. Bhatia, "Detection of DDoS Attacks using Machine Learning Algorithms," in *2020 7th International Conference on Computing for Sustainable Global Development (INDIACom)*, IEEE, Mar. 2020, pp. 16–21. doi: 10.23919/INDIACom49435.2020.9083716.

[45] S. Hossain, D. Sarma, and R. J. Chakma, "Machine learning-based phishing attack detection," *Int. J. Adv. Comput. Sci. Appl.*, vol. 11, no. 9, pp. 378–388, 2020, doi: 10.14569/IJACSA.2020.0110945.

[46] S. Khan, K. Kifayat, A. Kashif Bashir, A. Gurtov, and M. Hassan, "Intelligent intrusion detection system in smart grid using computational intelligence and machine learning," *Trans. Emerg. Telecommun. Technol.*, vol. 32, no. 6, 2021, doi: 10.1002/ett.4062.

[47] M. Kang, "Machine Learning: Anomaly Detection," in *Prognostics and Health Management of Electronics*, Wiley, 2018, pp. 131–162. doi: 10.1002/9781119515326.ch6.

[48] R. Zagrouba, R. A.-I. J. of Communication, and undefined 2021, "Machine learning based attacks detection and countermeasures in IoT," *core.ac.uk*, vol. 13, no. 2, 2021, Accessed: May 07, 2024.

[49] K. Kumari and M. Mrunalini, "Detecting Denial of Service attacks using machine learning algorithms," *J. Big Data*, vol. 9, no. 1, Dec. 2022, doi: 10.1186/S40537-022-00616-0.

[50] T. Gaber, A. El-Ghamry, and A. E. Hassanien, "Injection attack detection using machine learning for smart IoT applications," *Phys. Commun.*, vol. 52, 2022, doi: 10.1016/j.phycom.2022.101685.

[51] T. Muhammad and H. Ghafory, "SQL Injection Attack Detection Using Machine Learning Algorithm," *Mesopotamian J. CyberSecurity*, vol. 2022, pp. 5–17, 2022, doi: 10.58496/MJCS/2022/002.

[52] F. Subhan, X. Wu, L. Bo, X. Sun, and M. Rahman, "A deep learning-based approach for software vulnerability detection using code metrics," *IET Softw.*, vol. 16, no. 5, pp. 516–526, 2022, doi: 10.1049/sfw2.12066.

[53] J. H. An, Z. Wang, and I. Joe, "A CNN-based automatic vulnerability detection," *Eurasip J. Wirel. Commun. Netw.*, vol. 2023, no. 1, 2023, doi: 10.1186/s13638-023-02255-2.

[54] S. Ruiz-Villafranca, J. Roldán-Gómez, J. Carrillo-Mondéjar, J. M. C. Gómez, and J. M. Villalón, "A MEC-IIoT intelligent threat detector based on machine learning boosted tree algorithms," *Comput. Networks*, vol. 233, 2023, doi: 10.1016/j.comnet.2023.109868.

[55] W. B. Demilie and F. G. Deriba, "Detection and prevention of SQLI attacks and developing compressive framework using machine learning and hybrid techniques," *J. Big Data*, vol. 9, no. 1, 2022, doi: 10.1186/s40537-022-00678-0.

[56] M. K. Baklizi *et al.*, "Web Attack Intrusion Detection System Using Machine Learning Techniques," *Int. J. online Biomed. Eng.*, vol. 20, no. 3, pp. 24–38, 2024, doi: 10.3991/ijoe.v20i03.45249.

[57] M. Zekri, S. El Kafhali, … N. A.-2017 3rd international, and undefined 2017, "DDoS attack detection using machine learning techniques in cloud computing environments," *ieeexplore.ieee.org*, 2018, doi: 10.1109/CloudTech.2017.8284731.

[58] H. Karimipour, A. Dehghantanha, R. M. Parizi, K.-K. R. Choo, and H. Leung, "A Deep and Scalable Unsupervised Machine Learning System for Cyber-Attack Detection in Large-Scale Smart Grids," *IEEE Access*, vol. 7, pp. 80778–80788, 2019, doi: 10.1109/ACCESS.2019.2920326.

[59] S. Reddy and G. K. Shyam, "A machine learning based attack detection and mitigation using a secure SaaS framework," *J. King Saud Univ. - Comput. Inf. Sci.*, vol. 34, no. 7, pp. 4047–4061, Jul. 2020, doi: 10.1016/j.jksuci.2020.10.005.

[60] S. Hariprasad, T. Deepa, and N. Bharathiraja, "Detection of DDoS Attack in IoT Networks Using Sample Selected RNN-ELM," *Intell. Autom. Soft Comput.*, vol. 34, no. 3, pp. 1425–1440, 2022, doi: 10.32604/iasc.2022.022856.

[61] A. Amjad, T. Alyas, U. Farooq, and M. A. Tariq, "Detection and Mitigation of DDoS Attack in Cloud Computing Using Machine Learning Algorithm," *EAI Endorsed Trans. Scalable Inf. Syst.*, vol. 6, no. 23, pp. 1–8, 2019, doi: 10.4108/eai.29-7-2019.159834.