A Review of Ransomware Detection Models for Cybersecurity Driven IIoT in Cloud Environments

Abrar Ali, Norah Hamed, Monir Abdullah
College of Computer Science and Information Technology, University of Bisha, Bisha 61922, Saudi Arabia

***Abstract*—Ransomware is currently one of the most severe cybersecurity threats and not only attacks legacy systems but cloud systems and Industrial Internet of Things (IIoT) systems as well. Security and privacy threats are heightened as these systems integrate more closely and thus are exposed to sophisticated and long-lasting attacks. This paper provides a comprehensive review of ransomware prevention and detection measures in cloud and IIoT environments with an emphasis on the usage of Machine Learning (ML) and Deep Learning (DL) models. Research studies published across IEEE, Elsevier, and Springer databases between 2020 and 2024 were analyzed. Our check reveals Ensemble methods and Random Forest (RF) are two of the ML methods most in use, with each at 18.00%, followed by Neural Networks (NNs) at 12.00%, with older models such as Support Vector Machines (SVMs) with 10.00%, Naïve Bayes (NBs) had 7.00%, and Decision Trees (DTs) still in use with utilization at 9.00% . Additionally, DL approaches (including Convolutional NN (NN), Long Short-Term Memory (LSTM), Bidirectional Long Short-Term Memory (BiLSTM), and Recurrent NN (RNN)) account for 20.00% of the techniques deployed, highlighting their growing prominence in IIoT security and ransomware research. Indicative of their integration into hybrid ML pipelines, Light Gradient Boosting Machine (LightGBM) and other ensemble boosting frameworks comprise 16.00%. Last but not least, other novel and specialized models including Extreme Gradient Boosting (XGBoos), Self-Organizing Maps (SOM), Gain Ratio, and Digital DNA account for 8.00% of the overall utilization observed throughout study. Among DL methods, Recurrent NNs (RNNs) are at the forefront with 40%, followed by CNNs with 30%, CNN–RNN hybrid models at 20%, and Autoencoders with 10%. Integration of cryptographic schemes, federated learning, blockchain-based audit mechanisms, and adaptive runtime mechanisms have further boosted the mechanisms of anomaly detection with detection rates of over 99% for polymorphic and zero-day ransomware.**

***Keywords*—Ransomware; Industrial Internet of Things; cloud computing; machine learning; deep learning; blockchain**

I. Introduction

It is any program engineered to disturb the usual operation of an operating system, literally through penetrating or exploiting holes in pre-existing software in a bid to impair a computer's operation through its resource, network, and data. Among the most common malware typologies are viruses, worms, spyware, Trojan horses, adware, and ransomware. Today, ransomware is also deemed the most prevalent malware for having a characteristic called cryptovirology, where it uses encryption methods to invade user data and computer files. Some of the latest significant ransomware attacks include those of Taiwan Semiconductor Company from WannaCry, SamSam Ransomware, WannaCry against the U.K. National Health Service, and the ransomware attack on Foxconn. The United States is the country most targeted in cybercrime, where government sector organizations are the highest victims, then the manufacturing, education, and healthcare industries [1].

A. Cloud Computing

Cloud computing offers a low-cost and scalable storage and data processing solution for vast amounts of data, and edge computing offers computing power and data storage where they are needed locally [2]. Artificial Intelligence (AI) and ML [3] enhance these systems.

This research offers a holistic evaluation of cryptographic methods applied in cloud computing to overcome data security issues. Among the most notable approaches reviewed is DNA cryptography, popular for high storage density and high security, though currently in a nascent developmental state; Elliptic Curve Cryptography (ECC), popular for security through a small key size, hence suitable for resource-limited spaces such as the IoT; and homomorphic encryption, allowing computations on encrypted data without decrypting it, hence maintaining data confidentiality in processing. Additionally, hybrid cryptography combines symmetric and asymmetric encryption for increased efficiency and security, while lightweight cryptography is specifically designed for use in devices with limited computational power, such as sensors and Radio Frequency Identification (RFID) devices. Comparative studies of these approaches have been carried out, basing analyses on performance, security aspects, and usability, with recommendations to merge methods such as ECC and homomorphic encryption with blockchain technology for increased robustness. Reliability and accuracy for these processes are determined based on application, with success rates of 85% to 98%, depending on applied algorithms [4].

B. Vulnerabilities and Technology Used

This study examines program protection for Autonomous Vehicular Cloud Computing (AVCC) platforms against timing side-channel attacks. A compiler-level obfuscation preprocessor is introduced by the researchers, adeptly rewriting the input program's control flow dynamically and in a randomized manner. It takes advantage of the Low Level Virtual Machine (LLVM) compiler for executing conditional branch transformations and extraneous code insertion for an increase in logical complexity and reverse engineering attempts deterrents. Independently of input language and platform, the system is centered on ARM-based embedded platforms and extends branch conversion opportunities. Experimental evaluations

validate higher runtime variability in various program versions, thereby enhancing protection against the timing analysis attacks. Having low overhead, the software solution is a quick and efficient method for protecting AVCC platforms [5].

Defines data storage and sharing security in cloud methods such as cryptography, access control, ML differential privacy, watermarking, and probabilistic methods. The essay compares techniques in detail, strength and weakness. Privacy and security are achieved by cryptography but are susceptible to exposure after encryption key hacking. Access control minimizes data leakages without any transformation cost but fails to detect malicious agents. Differential privacy is computationally expensive but preserves data utility and privacy. Probabilistic methods and watermarking are efficient in tracing leakers, and watermarking is good for tracing culprits and probabilistic methods are resistant to data alteration. The paper highlights the point that no single solution offers comprehensive security, in favor of composite solutions for offering comprehensive protection. Results show significant data security improvement, with performance relying on the approach and use [6].

Aims to provide a decentralized, privacy-preserving public auditing protocol that allows cloud data integrity while taking potential auditor or cloud server manipulation into account. The system employs the utilization of blockchain technology to provide secure, random challenges and audit results logging in a transparent manner to enable tamper-proof operations. Zero-knowledge proofs are utilized for the protection of user data privacy during auditing, while the Proof of Work mechanism prohibits the cloud server from preparing challenges in advance. With a decentralized system, the system avoids relying on fully trusted third parties. The outcomes validate the effectiveness of the system in data privacy protection and public, traceable auditing. Security analysis assures its resilience against guess attacks on challenge messages, and experimental tests on the ethereum test net confirm its practicability with high efficiency and minimal communication and computational overhead [7].

A blockchain-supported certificate-less public cloud data integrity audit scheme, proposed specifically for safe cloud storage while eliminating issues such as troublesome certificate administration and key escrow. It requires the administration of semi-trusted Third-Party Auditors (TPAs) through blockchain technology and preservation of user data privacy in the course of audit. A novel data structure in combination with a counting Bloom filter and Multi-Merkel hash tree is developed to enable efficient dynamic update of data. System robustness for audit correctness, privacy preservation, and preservation against substitution attack is experimentally tested. Experimental verification proves its efficiency with 99% detection likelihood for data tampering and low computational and communication overheads, rendering it plausible and practical [8].

The project develops Run-time Adaptations for Data protection (RADAR), a data protection system for dynamic cloud settings that adapts to dynamically emerging threats and configurations in real-time. Key methods utilized are Models@Runtime for runtime modeling of the system, pattern matching for identifying malicious configurations, adaptation rules for autonomous reconfigurations, and search algorithms (e.g., Best-First Search) for optimization of adaptation. Further functionalities such as Topology and Orchestration Specification for Cloud Applications (TOSCA) for system topology modeling, Eclipse Modeling Framework (EMF) for models at runtime, and encryption for data protection are included. The results establish the efficacy of RADAR in identifying and rectifying data protection threats such as General Data Protection Regulations (GDPR) compliance in low cost and low loss of functionality. High scalability and accuracy of the system were experimentally confirmed through numerous case studies, rendering the system applicable in complex real-world situations [9].

The study intends to deploy an intelligent behavior-based malware detection system in a cloud computing environment to detect known and unknown malware with high accuracy. Suspicious files are uploaded to the cloud, stored in VMs, and their unique behaviors and traits are tracked. The system employs modern methods, including rule-based detection, ML classifiers (J48, RF and K-Nearest Neighbors (KNN)), and the Cloud-Based Behavior Model (CBCM), to identify whether or not files contain malware. Beyond the state of the art, the evaluation reveals that low false positive rates (0.4% for ML and 6.6% for rule-based detection) and high detection rates (up to 99.8%) are achieved. The system is very accurate (99.7%) and scalable and can therefore be deployed in dynamic and complex environments [10].

This study focuses on advanced malware detection methodologies in cloud infrastructure. It aims at minimizing the threats of advanced malware, such as polymorphic and metamorphic variants, from evading simplistic signature-based detection schemes. It integrates ML algorithms, DL models, and behavioral detection for differentiating malicious from benign code. Principal methods involve both dynamic and static analyses for feature extraction, virtual machine introspection (VMI), and heuristic detection schemes. Test cases establish high detection rates with low false positives and thereby system scalability and performance in detecting known entities and unknown threats. It offers a comprehensive solution with high security for complex cloud infrastructure [11].

LSTM and BILSTM models are being studied for real-time malware detection in clouds using RNNs. To find malicious activity in VMs, it employs system monitoring of Central Processing Unit (CPU), memory, and disk utilization. A data set of 113 unique malware specimens collected in a real cloud infrastructure environment yielded 40,680 test instances. Both models achieved performance values above 99% in accuracy, precision, recall, and F1-score, with LSTMs requiring less training time. The results demonstrate how RNN-based methods can be used to identify sophisticated malware threats on cloud devices [12]. Table I summarizes the vulnerabilities and technologies used for prevention the ransomware in cloud computing.

TABLE I. VULNERABILITIES AND TECHNOLOGY USED FOR RANSOMWARE PREVENTION IN CLOUD COMPUTING

Ref	Vulnerabilities in Cloud Computing	Technology Used in Prevention	Year
[4]	Data security issues (data exposure, unauthorized access)	DNA Cryptography, ECC, homomorphic encryption, hybrid and lightweight cryptography	2024
[5]	Timing side-channel attacks in Autonomous Vehicular Cloud Computing	LLVM-based compiler obfuscation (branch transformation, junk code)	2022
[6]	Exposure of encryption keys, undetected malicious agents, data leakage	Cryptography, Access control, ML-based differential privacy, watermarking, probabilistic methods	2022
[7]	Manipulation by cloud servers/auditors, lack of trust in third parties	Blockchain-based decentralized auditing, Zero-knowledge proofs, Proof of Work	2020
[8]	Inconvenient certificate management, key escrow issues	Blockchain, Certificate-less auditing, Bloom filter, Multi-Merkel hash tree	2023
[9]	Real-time adaptation to emerging threats, dynamic configuration flaws	Models@Runtime, Pattern matching, Adaptation rules, TOSCA, EMF, encryption	2021
[10]	Detection of unknown and polymorphic malware	Behavior-based detection, CBCM model, ML classifiers (J48, RF, and KNN)	2021
[11]	Evasion by smart malware (polymorphic/metamorphic), low detection accuracy	ML/DL models (CNN and RNN), Dynamic & static analysis, Virtual Machine Introspection, Heuristic analysis	2024
[12]	Malware behaviors in cloud VMs, performance monitoring	RNNs (LSTM and BiLSTM) analyzing CPU, memory, disk usage	2021

II. RELATED WORKS

A. Industrial Internet of Things (IIoT)

IIoT is a fusion of IoT technology and industrial devices applied in industry [13]. presents a new cryptographic algorithm using the application of the Harris Hawks Optimization (HHO) approach, combined with feature selection, to enhance communication efficiency and security for communication between IIoT devices and cloud computing platforms [14]. This sector has attracted much attention in recent years with its ability to transform industry manufacturing using intelligent and efficient methods. The IIoT transformed industry settings through the linking of a wide range of devices in a network and facilitating the collection, analysis, and decision-making processes in real-time. Data-informed decisions have seen increased business efficiency in operation, decreased downtime, and enhanced productivity [15]. Traditional IIoT architecture, based mainly on cloud computing, however, is faced with inherent shortcomings in addressing the high volume and velocity of IIoT data, bandwidth limitations, and confidentiality-related data issues [16]. To overcome these issues, distributed edge-to-cloud computing has been introduced as a viable solution through the blending of edge computing and cloud computing in supporting IIoT endeavors.

B. Vulnerabilities and Technology Used

The title introduces a novel ransomware detection framework customized for IIoT networks. Principal Contributions Revolutionary FL Design: An asynchronous peer-to-peer FL structure does not entail the involvement of a cloud server. Enhanced Data Processing: CDAE obtains adversarial robustness against IID and non-IID data. Scalability and Privacy: Lowers bandwidth consumption and maintains data privacy throughout training and update processes. We tested the model on three data sets (X-IIoTID, ISOT, and NSL-KDD), and it showed the following features: Enhanced accuracy, recall, and F1 values compared to current ransomware detection models, including those for unknown variants (evasion attacks).Efficient working on IID and non-IID data distributions, maintaining adaptability in real-world heterogeneous settings. Adversarial robustness against attacks such as Fast Gradient Sign Method (FGSM) and brute-force (BF) attacks [17]. key issue of the protection of IIoT devices from every kind of cyberattack and introduces an AI-motivated professional system for detection. Key Contributions Classification of IIoT Attacks: Labels attacks as denial-of-service (DoS), data tampering, device hijacking, and physical tampering. Proposed Expert System: Combines rule-based reasoning, anomaly detection, and reinforcement learning. Utilize characteristics such as "duplication and retransmission rate" for detecting attacks more efficiently. Attack Types Addressed Man-in-the-Middle (MitM), Distributed DoS (DDoS), and Start-Stop attacks. Testing and Verification: Examined on real Programmable Logic Controllers (PLCs) and IIoT protocols such as Modbus, MQTT. Showed high precision (99.7%) and low latency in detecting attacks [18].

This research examines the convergence of ransomware attacks and IoT technologies and provides an in-depth examination of the evolution, classifications, and consequences of ransomware, especially in IoT settings. It categorizes ransomware into two kinds: Crypto-ransomware, where user data is encrypted and a ransom must be paid in exchange for a decryption key, and Locker ransomware, where the user's device is locked until a ransom is paid. It suggests not paying ransom as a way to discourage cybercriminals and promotes cybersecurity best practice, such as disabling of macros, privilege limitation for users, and advanced detection system implementation [19].

Provides a lightweight and efficient means of securing IoT applications via a publish-subscribe communication paradigm. Its primary issues it addresses are the limitations of resource-poor IoT devices, the lack of increased scalability, and the ineffectiveness in resource-poor devices of traditional security schemes such as Transport Layer Security (TLS). Proposed Solution: Architecture: Fog nodes assist in storage and computing. A broker facilitates communication and authentication in the publish-subscribe infrastructure. Encryption: Secret messages are maintained via Advanced Encryption Standard CCM (AES-CCM), and communication expense are reduced. Authentication: A safe key exchange utilizing ECC is utilized and is resource-light compared to

standard public-key schemes. Optimization: Comparatively, handshakes, message lengths, and memory consumption are minimized in this scheme with respect to TLS-dependent schemes. Paper Contributions: It demonstrated a resource-light encryption scheme tailored for resource-limited IoT devices. It ensured end-to-end security via significantly fewer communication, storage, and processing expenses [20].

Model Building: CNN models (1D, 2D, 3D) were developed with input layers, several convolutional layers, dropout layers (for overfitting prevention), and fully connected dense layers. Transfer learning was adopted to enhance classification efficiency for binary and multiclass classification. Paper Datasets: Four available datasets (BoT-IoT, MQTT-IoT-IDS2020, IoT-23, IoT Network Intrusion) were transformed to develop additional datasets, IoT-DS-1 and IoT-DS-2, with increased attack diversity. Characteristics were derived using tools such as CICF low meter, with particular consideration of flow-based traffic characteristics. The developed models performed well on each of the datasets. For instance, the CNN1D model performed up to 99.9% accuracy in certain instances. CNN1D and CNN2D were more accurate and efficient than CNN3D.paper Practical Utility: The generalizability of the developed model suggests potential use in real-world IoT network security situations [21].

Recommends up-to-date DL models for detecting anomalies in IoT networks with particular interest in RNNs models: RNN models use LSTM, BiLSTM, and Gated Recurrent Unit (GRU) architectures and layer normalization, dropout, and regularization to forestall overfitting. Hybrid CNN-RNN models use the CNN layers for extracting spatial features before inputting data into the RNN layers. The scientific paper resulting from the work had the following consequences: High detection rates on various datasets, CNN-BiLSTM having the highest overall detection rates for all cases. Good at identifying novel kinds of attacks through utilizing methods for reducing class imbalances. Lightweight binary classifiers showed promising evidence for real-time anomaly detection for IoT [22]. Considers utilizing Hierarchical Federated Learning (HFL) and Federated Learning (FL) for enhancing Intrusion Detection Systems (IDS) for IoT networks. NSL-KDD was the utilized dataset that contained imbalanced data for five normal and attack sample classes. 122 input features, two hidden layers, and output layer NNs were utilized. Findings of the experiment in the scientific paper were as follows: HFL outperformed FL at every point in accuracy, convergence rate, and non-iid data handling. HFL's hierarchical structure minimized communication overhead and optimized data inconsistency handling. Sting Accuracy: HFL had a 3-6% higher accuracy than FL in a majority of instances [23].

Recent studies have overwhelmingly explored the intersection of IoT and cyber threats, specifically ransomware. Existing literature suggests that the ubiquitous implementation of IoT devices has brought forward newfound vulnerabilities, making devices susceptible to exploitation via ransomware attacks. Scholarly research carried out by Nkenyereye et al. (2022) exhaustively studies the evolution of ransomware, describing the shift in tactics to exploit the inherent properties of IoT ecosystems, such as limited processing power, device heterogeneity, and lack of comprehensive security. The article divides ransomware targeting IoT devices into various kinds, such as crypto-ransomware and locker-ransomware, and studies popular infection vectors, including phishing, malicious codes, and remote exploitation. The article also covers the weaknesses of traditional mitigatory approaches—such as antivirus products and signature-based detection schemes—in adequately confronting threats specific to IoT devices. Valuable contributions of the present study include a review of prevailing mitigatory frameworks and a suggested set of future directions for improvement. Such suggested directions include detection schemes via AI, blockchain technology for communication via secured channels, and the enforcement of device-level tailored security policies specific to IoT devices. Such a study places stress on the need for adaptive and customized security products in response to the prevailing scenario of IoT ransomware [24]. Table II summarizes the vulnerabilities and technologies used for ransomware prevention in IIoT.

TABLE II. VULNERABILITIES AND TECHNOLOGY USED FOR RANSOMWARE PREVENTION IN IIOT

Ref	Vulnerabilities in IIoT	Technology Used in Prevention	Year
[3]	Scalability, security, and legacy system integration	Distributed Edge-to-Cloud computing platforms (e.g., ThingsBoard, Azure IoT)	2024
[13]	IoT ransomware attacks, file encryption, unauthorized modifications	L-IDS (TEE, decoy files, entropy, fuzzy hashing, GNB classifier)	2024
[14]	Secure and efficient communication between IIoT and cloud	Harris Hawks Optimization-based cryptographic algorithm	2024
[15]	Digital forensics issues due to device heterogeneity and decentralization	Blockchain with fuzzy hashing and smart contracts	2021
[16]	Latency, data consumption, and privacy issues	Edge computing (Device, Edge, and Cloud layers)	2020
[17]	Centralized detection model vulnerabilities, adversarial threats	Asynchronous Peer-to-Peer Federated Learning with CDAE	2021
[18]	DoS, data tampering, hijacking, and physical tampering in IIoT	AI-driven expert system (rule-based, anomaly detection, reinforcement learning)	2024
[20]	IoT resource limitations, inefficiency of TLS	Lightweight encryption (AES-CCM), ECC, fog nodes	2020
[21]	Anomaly detection challenges in diverse IoT networks	CNN-based DL models with flow-feature extraction	2021
[22]	Detection of novel attack types and class imbalance	Hybrid CNN-RNN models with LSTM, BiLSTM, GRU	2022
[23]	Non-IID data handling, communication overhead in IDS	HFL model	2021
[24]	Ransomware threats in IoT due to weak security and phishing	AI detection models, blockchain, device-specific security policies	2021

III. Ransomware Attack

Represent a novel and serious danger to international cybersecurity. Ransomware encrypts data or prevents users from accessing their own systems with the aim of extorting ransom payments, which have considerable financial and functional damage to individuals, businesses, and even governments. With the evolution of ransomware strategies, conventional detection techniques are unable to detect and remove such threats effectively and on time [25]. Ransomware not only targets traditional systems but also IoT systems. These systems are usually made up of many resource-constrained IoT devices with diverse requirements. In addition, in contrast to the majority of conventional computing systems, IoT devices mainly provide services and functionality, as opposed to holding sensitive information [13]. Fig. 1 show the ransomware attack process.

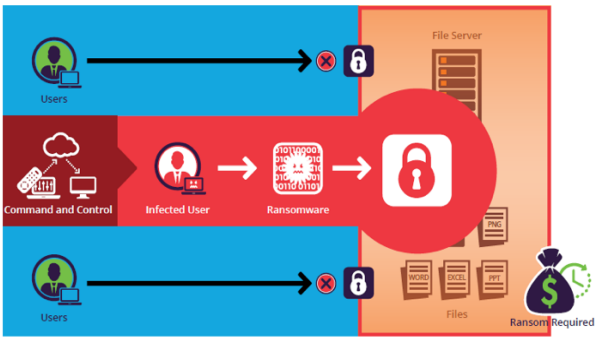

Fig. 1. Ransomware attacks process.

Ransomware is a type of malicious program that can render a computer or data attached to a computer inaccessible or encrypted. It can in some cases completely destroy the system, resulting in the loss of valuable and irretrievable data. Through such a measure of control, cybercriminals demand a heavy ransom from the victim in exchange for regaining access.

1) Crypto-ransomware: describes the amalgamation of ransomware attacks and IoT technology, with a holistic breakdown of the past, classifications, and consequences of ransomware, particularly in the scenario involving IoT.

This paper divides ransomware into two kinds: Crypto-ransomware: It encrypts user files and requests ransom for a decrypt key [19].

2) Locker ransomware: Locks out the user's device, disallowing usage until ransom is paid in return. It advises against ransom payments in a bid to discourage cybercriminals and encourages stringent cybersecurity practice, such as disabling of macros, restricting user permissions, and adopting advanced detection methods [19].

3) Doxware: Threatens to publish the victim's data unless a ransom is paid. The research categorizes ransomware into crypto-ransomware, locker ransomware, doxware, and mobile-based ransomware according to their unique attack patterns and impacts. The research also follows the evolution of ransomware from Crypto Locker (2013) to Ryuk (2020), showing how the tactics of ransomware have developed with encryption and anonymous payment methods. Detection and prevention are carried out through varied methodologies [26].

4) Mobile-based ransomware: This strategy focuses on mobile devices in particular, often through the use of screen locks or data encryption. Such methods based on ML have shown promise in identifying ransomware patterns, up to 97.3% accurate in identification rates by the use of RF, SVM, and NNs. Honey potting methods are also available for passive monitoring through luring ransomware into controlled sections for the sake of analysis. Statistical anomaly detection methods have also been utilized; they are, however, limited in countering more sophisticated, stealthy forms of ransomware [26]. Fig. 2. is an example of Ransomware attacks.

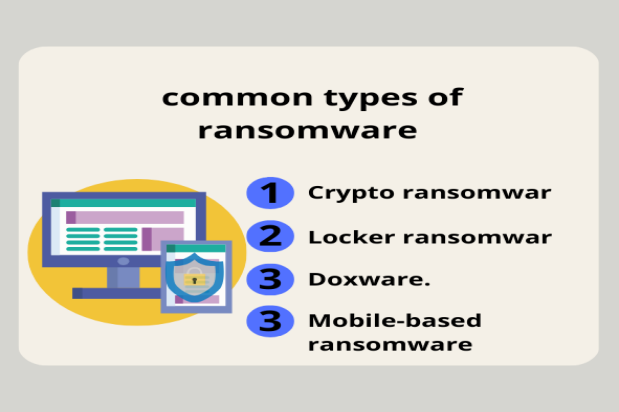

Fig. 2. Example of ransomware attacks.

IV. Ransomware Detection Models

The objective of this research is 1) exploration of the ransomware life cycle on the Windows operating system, 2) behavioral analysis of ransomware specimens in order to draw out various attributes of malicious code schemes, and 3) constructing and validating ML models of ransomware detection on diversified ransomware and non-ransomware specimens [1]. A stacked ensemble learning strategy utilizing six classifiers (Gaussian NB, KNN, DT, Logistic Regression (LR), Multi-Layer Perceptron, and SGD Classifier). A subsequent layer utilizing LightGBM to forecast the identified ransomware into related families [25]. A set of ML models comprising Self-Organizing Maps (SOM), RF classifier, and LSTM networks are utilized for behavior analysis. Implementation of LSTM networks enhances sequential behavior analysis, a key aspect for countering nascent ransomware approaches [26]. Brinkley et al. (2024) have suggested a ML-driven IDS for identifying zero-day ransomware attacks on the basis of as-yet unidentified data. A wide range of varied ML algorithms such as RF, SVM, and NNs were applied in the research and contrasted against a set of 2,850 samples taken from open-source cybersecurity databases and simulation labs. A comprehensive feature engineering mechanism was proposed in the study, with particular focus on system anomalies such as file access behavior, encryption activity, and network behavior. Key findings indicated the NN model had the highest accuracy (92.4%), and RF balanced a blend of accuracy and computational proficiency. A rigorous series of simulations in compliance with zero-day simulations

were carried out on the system and were found to have high generalizability towards hitherto unknown versions of ransomware. In spite of the growth of NN with increased resources and latency, the research proved the feasibility and usability of ML for real-time ransomware detection. It offers a strong framework for adaptive and dynamic cybersecurity protection, as a corrective measure against the inability of signature-based technologies to identify the newer ransomware threats [27]. This study uses XGBoost classifier and RF algorithms for detection and classification of ransomware attacks [28]. We reviewed ransomware's new prevention and detection breakthroughs and suggested directions and challenges for future studies. We actually examined a few well-known ransomware instances and also created our own experimental ransomware, AESthetic, to evade eight well-known antivirus products [29]. Static analysis for ransomware detection. Removal of disassembling procedure through direct feature extraction from raw byte using frequent pattern mining. The Gain Ratio method was implemented to use it on feature selection. RF classifier with in-depth investigation to the impact of both trees and seed amounts in the present study was implemented [30], [31]. Tried the classification algorithm's performance for NBs and RF. The algorithms' performance was assessed on the basis of Accuracy, Precision, Recall, and F-Measure [32]. We presented a comprehensive detail of malware analysis. Cyber Threat Hunting (CTH) methods are narrated on the basis of data analysis technique implemented. Ransomware building and research directions are introduced. Ransomware datasets implemented in the prior studies are cited along with their data sources [33]. AI-driven methods, such as ML and DL, to augment ransomware detection. Conventional ML Models: SVM, RF, NBs, DTs. DL models: CNNs, BiLSTMs, Auto-encoders. Ensemble Learning: A gathering of various classifiers for boosting detection rates. Real-Time Detection: AI models having runtime detection capabilities for ransomware [34]. Examined are the models:

- Blockchain-Based Data Backup and Recovery – Effective for safe, immutable backups but expensive to retain.
- Smart Contract-Enabled Ransomware Detection – Provides for automatic detection and response but is not scalable as it demands high computational requirements.
- Blockchain-Enhanced Secure Communication Channels – Blocks ransomware propagation through encrypted messaging but is not scalable as it faces scalability issues.
- Decentralized Malware Analysis Platforms – Effective for threat intelligence exchange but requires high computational infrastructure and facilities [35]. A combination of several methods, including behavioral analysis, heuristic detection, and DL models, performs better [36]. BSFR-SH is a strong blockchain-supported security framework efficient for ransomware detection, mitigation, and data recovery in intelligent healthcare systems [37]. Techniques developed on ML have been a success for ransomware pattern identification, and RF, SVM, and NNs are capable of identifying with up to 97.3% accuracy. Honeypotting methods also offer passive monitoring functionality through decoy attraction of ransomware in isolated areas for monitoring purposes. Statistical anomaly detection methods have also been applied [38]. Network traffic monitoring can also identify the attacker's IP address. Comparison of various methods utilized for detecting ransomware, such as signature-based, ML-based, and dynamic analysis, are also presented in the work [39] ML-based approaches proved to be an effective solution that provides real-time detection of ransomware. Several prevention techniques that involve firewalls, intrusion detection systems, and regular backup products. The proposed system in this study is an extension of these existing methods by analyzing encrypted file extensions to identify ransomware type and recommend decryption tools [40].Using Gradient Tree Boosting, the detection improves to 99.997% accuracy with an FPR of just 0.01%. Static analysis, when coupled with ML techniques, is able to detect ransomware before execution effectively with reduced system damage potential [41]. The research also compares common ML algorithms with the comment that while age-old techniques such as SVM and RF are still in the forefront, newer DL techniques such as LSTM networks and CNNs have shown high potential to extract features independently and enhance detection performance [42]. Table III summarizes the ransomware detection ML and DL models.

TABLE III. RANSOMWARE DETECTION MODELS (ML AND DL)

Ref	Vulnerabilities / Challenges	Technology Used in Prevention	Year
[1]	Ransomware lifecycle exploitation via Windows APIs	API-based detection with ML models	2021
[25]	Accurate classification of ransomware families	Dual-stage ML architecture using Ensemble + LightGBM	2024
[26]	Behavioral threats in network/system activities	SOM, RF, LSTM models	2023
[27]	Zero-Day Ransomware Threats, Evasion Techniques, System Behavior Manipulation, Model Generalization	ML Algorithms: RF, SVM, and NNs.	2024
[28]	Fast detection/classification of ransomware	XGBoost and RF classifiers	2023
[29]	Advanced ransomware evading antivirus detection	Experimental ransomware and prevention insights	2021
[30]	Slow detection due to disassembly and analysis	Static analysis with RF, Gain Ratio	2020
[31]	Understanding ransomware paths	DNA act-Ran using ML and Digital DNA Sequencing	2020
[32]	Healthcare ransomware attacks	NBs classifiers with 99.2% accuracy	2024
[33]	Detection techniques categorization	Cyber Threat Hunting and dataset review	2022
[34]	Limitations of traditional detection	AI-based models (ML, DL, Ensemble Learning)	2024

[35]	Inefficient backup, detection, and communication	Blockchain cybersecurity models (Smart Contracts)	2024
[36]	Inconsistent malware detection	Hybrid of signature, behavior, DL models	2020
[37]	Smart healthcare ransomware attacks	BSFR-SH: Blockchain framework	2022
[38]	Diverse ransomware types (crypto, locker, etc.)	ML models (RF, SVM, and NN), Honeypots, Anomaly detection	2023
[39]	Crypto ransomware via phishing and fake updates	Forensic detection, traffic analysis, ML	2020
[40]	Encrypted data attacks demanding ransom	AI/ML for detection and auto-decryption tool suggestions	2023
[41]	High false positive rate in static analysis	Gradient Tree Boosting with 99.997% accuracy	2020
[42]	Advanced RaaS, double extortion, evasion	ML taxonomy (SVM, RF, LSTM, CNN) with benchmark analysis	2024

V. Analysis and Discussions

Using specific inclusion and exclusion criteria, the research methodology identified and evaluated malware detection models in accordance with a systematic literature review (SLR) approach. This guaranteed the results' objectivity, transparency, and reproducibility.

The file under review emphasizes the increasing relevance of ML and DL methods in ransomware detection in cloud computing and industrial IoT settings Conventional detection measures are not effective against contemporary ransomware because of polymorphism obfuscation and zero day attacks AI based measures are increasingly employed for sound and dynamic detection. ML models such as RF, SVMs, NBs and DTs remain in favor due to simplicity interpretability and efficiency RF model is most conventional to handle high dimensional data Ensemble methods such as lightGBM and boosting are more accurate, but ml relies heavily on handcrafted features and can be beaten by evasive ransomware. Deep models such as CNNs, RNNs, LSTM, Bidirectional LSTM (BiLSTM) models are gaining popularity These automatically extract complex patterns and temporal features from unprocessed data Autoencoders find use in anomaly detection DL achieves high accuracy at high frequency often over 99 but is plagued with problems of interpretability scalability and computational cost. Compared to ML model is simple and effective while DL works outstandingly well in classifying advanced evasive ransomware Ensemble and hybrid approaches yield best results incorporating efficiency and accuracy The use of blockchain federated learning and anomaly detection mechanisms is validated through research for enhancing resilience. Fig. 3 shows the classification methods of ML Approaches.

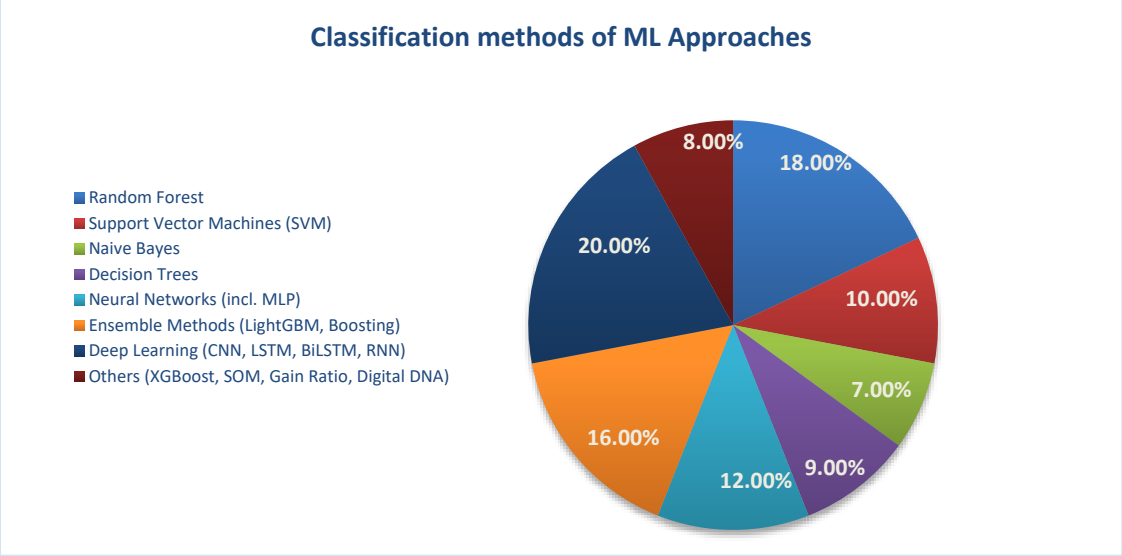

Fig. 3. Classification methods of ML approaches.

The most used methods are RFs and Ensemble Methods (18.00% each) due to their accuracy and robustness.

They are followed by NNs (12.00%), while classic models like SVM, NBs, and DTs still occupy an important role. hybrid approaches and neural solutions are gaining ubiquity, while traditional methods remain in common use for environments. Fig. 4 shows the classification methods of DL Approaches.

The most commonly used DL methods are RNNs, LSTM, BiLSTM, GRU at 40%, followed by CNNs at 30%. Hybrid CNN-RNN models take up 20%, which reflects the importance of architectural blends, and Autoencoders are utilized the least with 10%. In general, RNNs dominate due to their strength in sequence data handling, with CNNs and hybrids providing strong complementary techniques to ransomware detection. Fig. 5 shows the classification methods of ML approaches during past five years.

RF model was the leader in 2022 with nearly 100%, followed by the most commonly used method. After 2023, diversity picked up pace with XGBoost, Gradient Boosting, and SOM hitting about 30–35%.

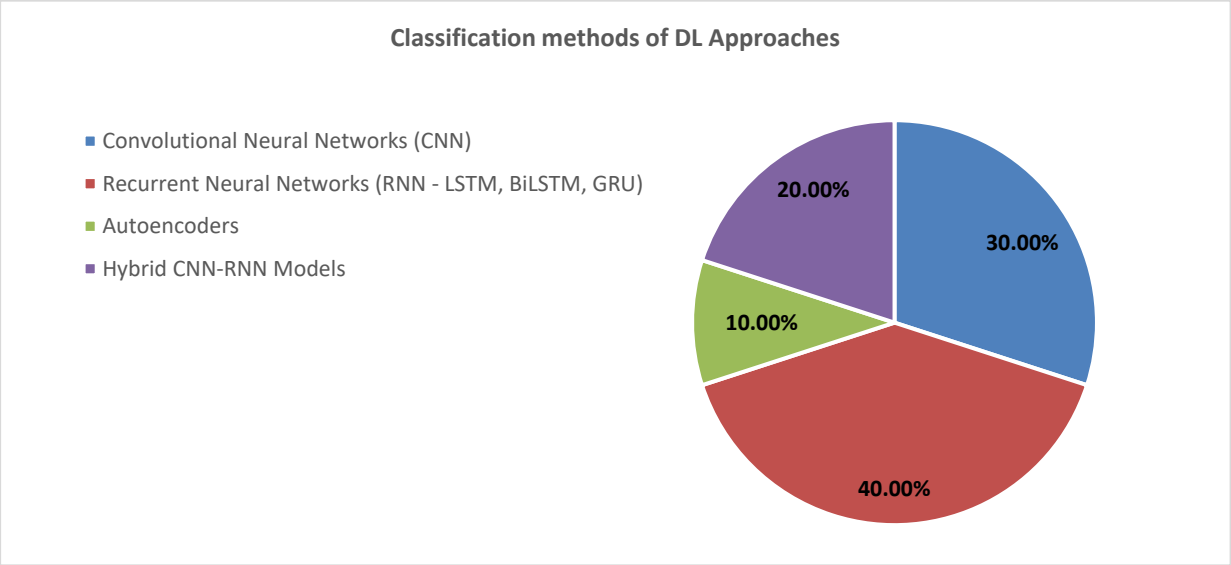

Fig. 4. Classification methods of DL approaches.

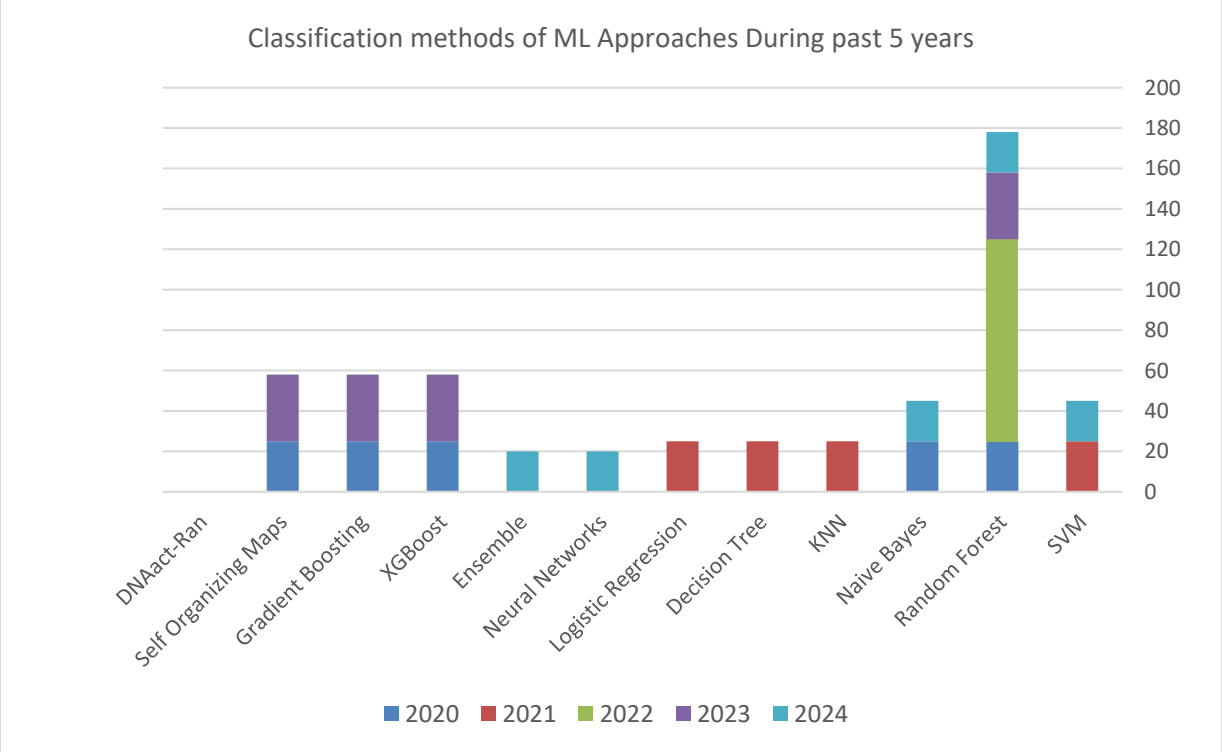

Fig. 5. Classification methods of ML approaches during past five years.

By 2024, NNs and Ensemble methods were popular (20%), which marked a shift towards complex and hybrid models.

- NSL-KDD has the maximum at 55%, the most sought-after dataset in all years.
- UNSW-NB15 leads with 28%, demonstrating its greater usage as a modern norm.
- Less frequently occurring data sets such as KDDCUP99 (6%), CIC-DoS2019 (5%), and CICIDS2017 (4%) are nonetheless useful for diversity.
- CICIDS2018 and ISCX2012 are used the least (1% each), reflecting minimal usage.

Overall, the findings reflect a continued overdependence on NSL-KDD and UNSW-NB15 with modest but useful contributions from newer datasets. Fig. 6 shows the different datasets for classification methods.

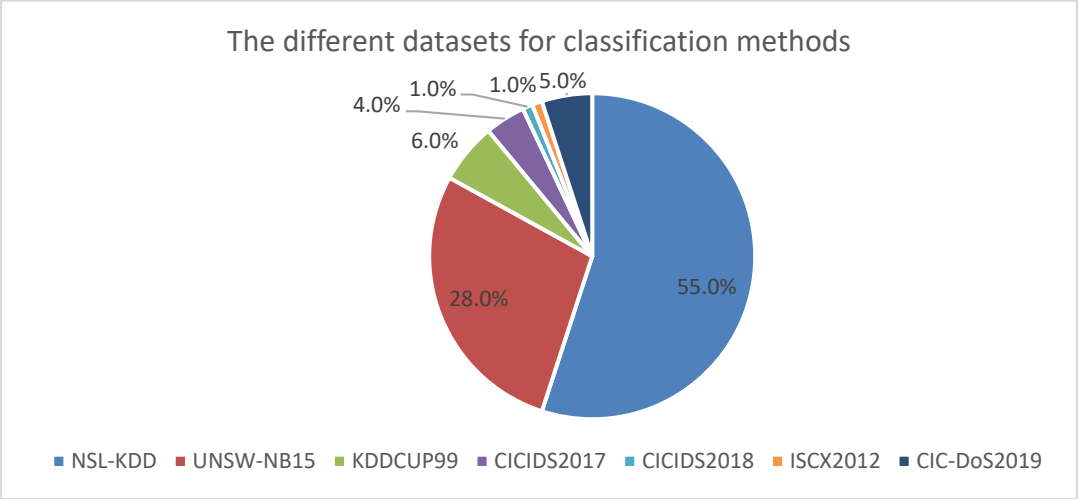

Fig. 6. The different datasets for classification methods.

VI. Conclusion

This work offers cybersecurity practitioners practical implications in addition to a comparative understanding of ransomware detection techniques. The results can help with the design of adaptive, hybrid security architectures that integrate blockchain, ML, and DL for practical protection systems. The findings from this research support that it is not one procedure that would suffice to offset the growing intricacy of cyber-attacks. Standard ML methods such as RF and Ensemble Techniques demonstrate good robustness and accuracy, while NNs provide greater adaptability. In contrast, DL approaches, specifically RNNs and CNNs, show improved accuracy in handling sophisticated and high-level threats, with hybrid CNN-RNN architectures further boosting detection. These results showcase the potential for constructing the future of resilient defense systems through an integration of hybrid and ensemble techniques, supported by blockchain-secured federated learning and adaptive anomaly detection. That type of integrated approach ensures a robust, scalable, and intelligent model for meeting current and future cyber threats.

Acknowledgment

The authors are thankful to the Deanship of Graduate Studies and Scientific Research at University of Bisha for supporting this work through the Fast-Track Research Support Program.

References

[1] Almousa, M., Basavaraju, S., and Anwar, M. (2021). Api-based ransomware detection using machine learning-based threat detection models. In *Proc. 18th Int.Conf. on Privacy, Security and Trust (PST), Dec. 2021*, pp. 1-7.

[2] Zhao, X. P., and Jiang, R. (2020). Distributed machine learning oriented data integrity verification scheme in cloud computing environment. *IEEE Access*, *8*, 26372-26384.

[3] Jamil, M. N., Schelén, O., Monrat, A. A., and Andersson, K. (2024). Enabling Industrial Internet of Things by Leveraging Distributed Edge-to-Cloud Computing: Challenges and Opportunities. *IEEE Access*.

[4] Sasikumar, K., and Nagarajan, S. (2024). Comprehensive review and analysis of cryptography techniques in cloud computing. *IEEE Access*.

[5] Hataba, M., Sherif, A., & Elkhouly, R. (2022). Enhanced obfuscation for software protection in autonomous vehicular cloud computing platforms. *IEEE Access*, *10*, 33943-33953.

[6] Gupta, I., Singh, A. K., Lee, C. N., and Buyya, R. (2022). Secure data storage and sharing techniques for data protection in cloud environments: A systematic review, analysis, and future directions. *IEEE Access*, *10*, 71247-71277.

[7] Miao, Y., Huang, Q., Xiao, M., and Li, H. (2020). Decentralized and privacy-preserving public auditing for cloud storage based on blockchain. *IEEE Access*, *8*, 139813-139826.

[8] Du, J., Dong, G., Ning, J., Xu, Z., and Yang, R. (2023). A Blockchain-Assisted Certificateless Public Cloud Data Integrity Auditing Scheme. *IEEE Access*, *11*, 123018-123029.

[9] Mann, Z. Á., Kunz, F., Laufer, J., Bellendorf, J., Metzger, A., and Pohl, K. (2021). RADAR: Data protection in cloud-based computer systems at run time. *IEEE Access*, *9*, 70816-70842.

[10] Aslan, Ö., Ozkan-Okay, M., and Gupta, D. (2021). Intelligent behavior-based malware detection system on cloud computing environment. *IEEE Access*, *9*, 83252-83271.

[11] Rao, S. M., and Jain, A. (2024). Advances in Malware Analysis and Detection in Cloud Computing Environments: A Review. *International Journal of Safety and Security Engineering*, *14*(1).

[12] Kimmel, J. C., Mcdole, A. D., Abdelsalam, M., Gupta, M., and Sandhu, R. (2021). Recurrent neural networks based online behavioural malware detection techniques for cloud infrastructure. *IEEE Access*, *9*, 68066-68080.

[13] Mofidi, F., Hounsinou, S. G., and Bloom, G. (2024, January). L-IDS: A multi-layered approach to ransomware detection in IoT. In *2024 IEEE 14th Annual Computing and Communication Workshop and Conference (CCWC)* (pp. 0387-0396). IEEE.

[14] Jawed, M. S., and Sajid, M. (2024, January). A Swarm Intelligence-based Faster and Secure Algorithm for Improved Industrial IoT-Cloud Computing Communication. In *2024 ASU International Conference in Emerging Technologies for Sustainability and Intelligent Systems (ICETSIS)* (pp. 1-5). IEEE.

[15] Mahrous, W. A., Farouk, M., and Darwish, S. M. (2021). An enhanced blockchain-based IoT digital forensics architecture using fuzzy hash. *IEEE Access*, *9*, 151327-151336.

[16] Qiu, T., Chi, J., Zhou, X., Ning, Z., Atiquzzaman, M., and Wu, D. O. (2020). Edge computing in industrial internet of things: Architecture, advances and challenges. *IEEE Communications Surveys & Tutorials*, *22*(4), 2462-2488.

[17] Al-Hawawreh, M., Sitnikova, E., and Aboutorab, N. (2021). Asynchronous peer-to-peer federated capability-based targeted ransomware detection model for industrial IoT. *IEEE Access*, *9*, 148738-148755.

[18] Karacayılmaz, G., and Artuner, H. (2024). A novel approach detection for IIoT attacks via artificial intelligence. *Cluster Computing*, *27*(8), 10467-10485.

[19] Inaam ul Haq, M., Li, Q., and Hou, J. (2022). Analyzing the research trends of IoT using topic modeling. *The Computer Journal*, *65*(10), 2589-2609.

[20] Diro, A., Reda, H., Chilamkurti, N., Mahmood, A., Zaman, N., and Nam, Y. (2020). Lightweight authenticated-encryption scheme for internet of things based on publish-subscribe communication. *IEEE Access*, *8*, 60539-60551.

[21] Ullah, I., and Mahmoud, Q. H. (2021). Design and development of a deep learning-based model for anomaly detection in IoT networks. *IEEE Access*, *9*, 103906-103926.

[22] Ullah, I., and Mahmoud, Q. H. (2022). Design and development of RNN anomaly detection model for IoT networks. *IEEE Access*, *10*, 62722-62750.

[23] Saadat, H., Aboumadi, A., Mohamed, A., Erbad, A., and Guizani, M. (2021, June). Hierarchical federated learning for collaborative IDS in IoT applications. In *2021 10th Mediterranean Conference on Embedded Computing (MECO)* (pp. 1-6). IEEE.

[24] Humayun, M., Jhanjhi, N. Z., Alsayat, A., and Ponnusamy, V. (2021). Internet of things and ransomware: Evolution, mitigation and prevention. *Egyptian Informatics Journal*, *22*(1), 105-117.

[25] Yan, P., Khoei, T. T., Hyder, R. S., and Hyder, R. S. (2024, October). A Dual-Stage Ensemble Approach to Detect and Classify Ransomware Attacks. In *2024 IEEE 15th Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON)* (pp. 781-786). IEEE.

[26] Khurana, S. (2023, December). Ransomware Threat Detection and Mitigation using Machine Learning Models. In *2023 IEEE International Conference on ICT in Business Industry & Government (ICTBIG)* (pp. 1-6). IEEE.

[27] Brinkley, Y., Thompson, D., and Simmons, N. (2024). Machine learning-based intrusion detection for zero-day ransomware in unseen data.

[28] Kunku, K., Zaman, A. N. K., and Roy, K. (2023, December). Ransomware detection and classification using machine learning. In *2023 IEEE Symposium Series on Computational Intelligence (SSCI)* (pp. 862-866). IEEE.

[29] Beaman, C., Barkworth, A., Akande, T. D., Hakak, S., and Khan, M. K. (2021). Ransomware: Recent advances, analysis, challenges and future research directions. *Computers & security*, *111*, 102490.

[30] Khammas, B. M. (2020). Ransomware detection using random forest technique. *ICT Express*, *6*(4), 325-331.

[31] Dutta, R., and Karmakar, S. (2024, June). Ransomware Detection in Healthcare Organizations using Supervised Learning Models: Naive Bayes Classifier. In *2024 15th International Conference on Computing Communication and Networking Technologies (ICCCNT)* (pp. 1-5). IEEE.

[32] Khan, F., Ncube, C., Ramasamy, L. K., Kadry, S., and Nam, Y. (2020). A digital DNA sequencing engine for ransomware detection using machine learning. *IEEE Access*, *8*, 119710-119719.

[33] Aldauiji, F., Batarfi, O., and Bayousef, M. (2022). Utilizing cyber threat hunting techniques to find ransomware attacks: A survey of the state of the art. *IEEE Access*, *10*, 61695-61706.

[34] Ferdous, J., Islam, R., Mahboubi, A., and Islam, M. Z. (2024). AI-based ransomware detection: A comprehensive review. *IEEE Access*.

[35] Fajri, A. I., Irawan, M. I., and Mahananto, F. (2024, August). A Systematic Literature Review on Blockchain-based Cybersecurity Models for Ransomware Mitigation. In *2024 IEEE International Symposium on Consumer Technology (ISCT)* (pp. 799-804). IEEE.

[36] Aslan, Ö. A., and Samet, R. (2020). A comprehensive review on malware detection approaches. *IEEE access*, *8*, 6249-6271.

[37] Wazid, M., Das, A. K., and Shetty, S. (2022). BSFR-SH: Blockchain-enabled security framework against ransomware attacks for smart healthcare. *IEEE Transactions on Consumer Electronics*, *69*(1), 18-28.

[38] Pandey, P., Jain, P., Gupta, A., Gupta, V. K., Jindal, H., and Gupta, A. (2023, November). Categorization, Detection, and Prevention of Ransomware Attack: A Review. In *2023 Seventh International Conference on Image Information Processing (ICIIP)* (pp. 552-557). IEEE.

[39] Ilker, K. A. R. A., and Aydos, M. (2020, October). Cyber fraud: Detection and analysis of the crypto-ransomware. In *2020 11th IEEE Annual Ubiquitous Computing, Electronics and Mobile Communication Conference (UEMCON)* (pp. 0764-0769). IEEE.

[40] Jayanthi, M. M., and Vijayakumar, K. (2023, May). Detection and decryption of ransomware. In *2023 2nd International Conference on Applied Artificial Intelligence and Computing (ICAAIC)* (pp. 1264-1267). IEEE.

[41] Usharani, S., and Sandhya, S. G. (2020, July). Detection of ransomware in static analysis by using Gradient Tree Boosting Algorithm. In *2020 International Conference on System, Computation, Automation and Networking (ICSCAN)* (pp. 1-5). IEEE.

[42] Ispahany, J., Islam, M. R., Islam, M. Z., and Khan, M. A. (2024). Ransomware detection using machine learning: A review, research limitations and future directions. *IEEE Access*.