Journal of Basrah Researches (Sciences) **52**(1), 135 (2026)
DOI: https://DOI.org/10.56714/bjrs.52.1.11

Network Traffic-Based Ransomware Detection Using Anomaly Detection Algorithms: A Comprehensive Systematic Review

Qusay J. Shaheen *, **Esraa Saleh Alomari**

Department of Computer, College of Education for Pure Sciences, Wasit University, 52001 Al-Kut, Wasit, Iraq.

A R T I C L E I N F O

Received 14 February 2026
Revised 17 March 2026
Accepted 19 March 2026
Published 30 June 2026

K e y w o r d s :

Ransomware Detection, Anomaly Detection, Cybersecurity, Network Traffic Analysis, Hybrid Algorithms, Proactive Defense.

Citation: Q. J. Shaheen, E. S. Alomari., J. Basrah Res. (Sci.) **52**(1), 135 (2026). DOI:https://DOI.org/10.56714/bjrs.52.1.11

A B S T R A C T

The present study offers an exhaustive systematic review of various ransomware detection techniques, with a specific focus on network traffic analysis and anomaly detection algorithms. In accordance with the PRISMA protocol, this study analyzes fifteen research papers published between 2021 and 2025. The research papers are collected from prominent scientific database sources, including IEEE Xplore, Scopus, ScienceDirect, and Google Scholar. The corpus of research articles can be broadly classified into four main categories of ransomware detection techniques: supervised machine learning approaches, unsupervised anomaly detection techniques, deep learning approaches, and hybrid approaches for ransomware detection.A comparative analysis of the research articles reveals that the deep learning approaches have been able to achieve higher detection accuracies of more than 99%, while the unsupervised anomaly detection approaches have been able to demonstrate higher adaptability in the detection of ransomware. However, the area of ransomware detection has several research gaps that need to be addressed: the lack of standardized data sets for the experiments, the processing of encrypted network traffic, and the occurrence of false positives in the detection process. The research demonstrates the need to incorporate hybrid and behavioral detection techniques to strengthen the robustness of cybersecurity systems against new ransomware attacks.

1. Introduction

Ransomware has undergone a dramatic evolution since its debut in the late eighties, moving from just limited threats to an integrated criminal sector driven by huge profit motives. In its technical essence, this software relies on the mechanism of blocking the service from users through forced encryption of information or disabling devices, which puts victims before the only option is to succumb to ransom requests to recover their information assets.The attackers have developed their methods by using advanced encryption techniques and "jamming" tactics to hide their activities, which has weakened the efficiency of traditional anomaly detection systems. "File-free" threats have also emerged that run inside memory without leaving a trace on the hard drive, which has further

*Corresponding author email: qusayjoudah6@gmail.com

ISSN: 1817-2695 (Print); 2411-524X (Online)
Online at: https://jou.jobrs.edu.iq

complicated monitoring operations.According to the report (Cybersecurity Ventures, 2025), Global losses are expected to jump from 57 billion dollars in 2025 to about 275 billion dollars a year by 2031, with an annual growth rate of 30% [1]. However, the Sophos 2025 report points to strategic shifts; data encryption operations have decreased from 70% to 50%, while pure extortion attacks have doubled (Exly). Economically, the average recovery costs decreased by 44%, and the actual ransom payments decreased from two million dollars to one million dollars as an average.[2].The second quarter of 2025 witnessed a significant decrease in the rate of attacks by 43% compared to the first quarter [3]. (See Fig. 1) .The scene was characterized by a state of "fragmentation"; emerging groups accounted for 41.7% of the total activity. Qilin with 12.6% and Akira with 10.5% topped the scene, while Play Group recorded a growth of 15.5%. In contrast, the activity of Lynx decreased by 50% and Incransom by 15.9%. This sharp contrast and the ongoing dynamics confirm the urgent need for organizations to adopt flexible defense strategies based on threat intelligence (Intelligence-driven) to counter this volatile intelligence environment [4]. (See Fig. 2).

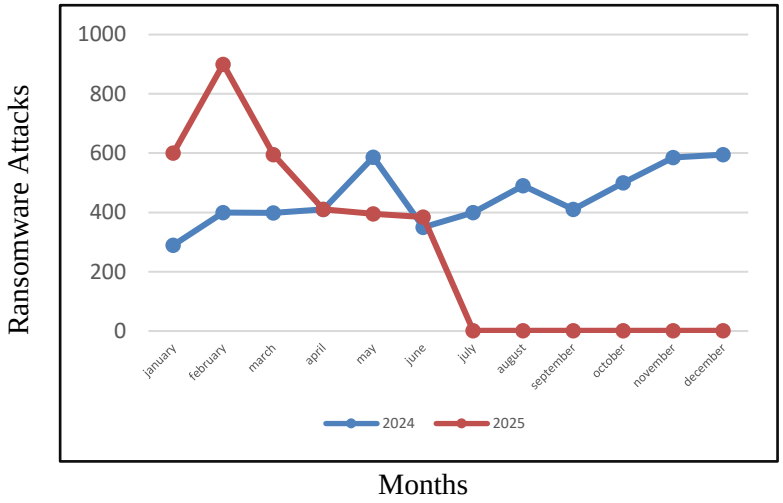

Fig. 1. Ransomware Attacks by Month 2024 – Q2/2025

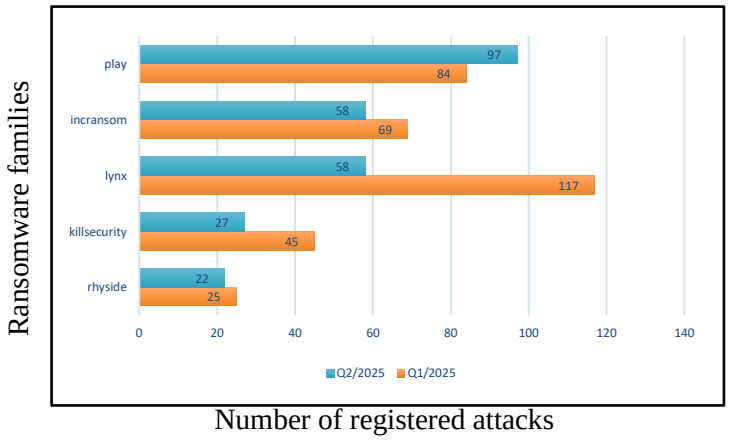

Fig. 2. Ransomware Attacks Comparison Across Group: Q1/2025 - Q2/2025.

This paper aims to carry out a systematic study and critical analysis of existing research works related to ransomware detection techniques, with a specific emphasis on techniques based on analyzing network communication and applying anomaly detection algorithms. This study aims to examine the potential use of behavioral patterns, as identified by analyzing communication patterns such as data packets, data transfers, and data request and response communication, in order to identify and differentiate malicious ransomware attacks from legitimate communication patterns. The proposed

techniques have the potential to identify ransomware attacks without access to the source code of the malicious software and to identify new ransomware attacks by analyzing unusual communication patterns. The rest of this paper is structured as follows: In Section 2, the methodology used in this systematic study is presented. In Section 3, the basic concepts in network security and ransomware are discussed. In Section 4, the lifecycle of a ransomware attack is presented. In Section 5, the evolution of ransomware extortion techniques is discussed. In Section 6, the impact of ransomware attacks is evaluated. In Section 7, existing work in this area is discussed and critically reviewed. In Section 8, this study is concluded and future directions are presented.

2. Methodology

It is proposed that the framework of Systematic Literature Review (SLR) be followed in order to ensure the systematic evaluation of the existing literature on ransomware detection techniques, with special emphasis on the techniques based on network traffic analysis and anomaly detection algorithms. The Preferred Reporting Items for Systematic Reviews and Meta-Analysis (PRISMA) criteria have been followed in order to ensure transparency in the process of literature selection for the proposed systematic literature review. The entire process of literature search was carried out using the scholarly databases like *IEEE Xplore*, *Scopus*, *ScienceDirect* . with *Google Scholar* used as a secondary source of literature search in order to ensure the extraction of relevant literature on the proposed topic of ransomware detection techniques based on network traffic analysis and anomaly detection algorithms. The search terms used were "*Ransomware Detection*," "*Network Traffic Analysis*," "*Network Flow*," "*Machine Learning*," "*Deep Learning*," "*Anomaly Detection*," with the use of logical operators like AND, OR in order to ensure a precise search. The time frame for the literature search was set from the year 2021-2025 in order to ensure the extraction of the recent trends in the development of ransomware detection techniques. The search resulted in the extraction of 126 articles, out of which 118 articles were retained after the removal of duplicates. The titles and abstracts of the articles were thoroughly searched in order to ensure the selection of articles relevant to the proposed topic of ransomware detection techniques, out of which 15 articles were selected for the proposed systematic literature review in order to ensure the extraction of relevant information on the techniques used in the process of ransomware detection, along with the advantages and disadvantages, in order to ensure the comprehensive evaluation of the existing trends in the development of ransomware detection techniques.

The study is guided by the following research questions:
RQ1: What machine learning and anomaly detection techniques are used for ransomware detection?
RQ2: What datasets and evaluation metrics are commonly used in ransomware detection studies?
RQ3: What are the strengths and limitations of existing approaches?

The study selection process followed the PRISMA guidelines to ensure transparency in identifying, screening, and selecting relevant studies. The flow of article selection is illustrated in Fig. 3.

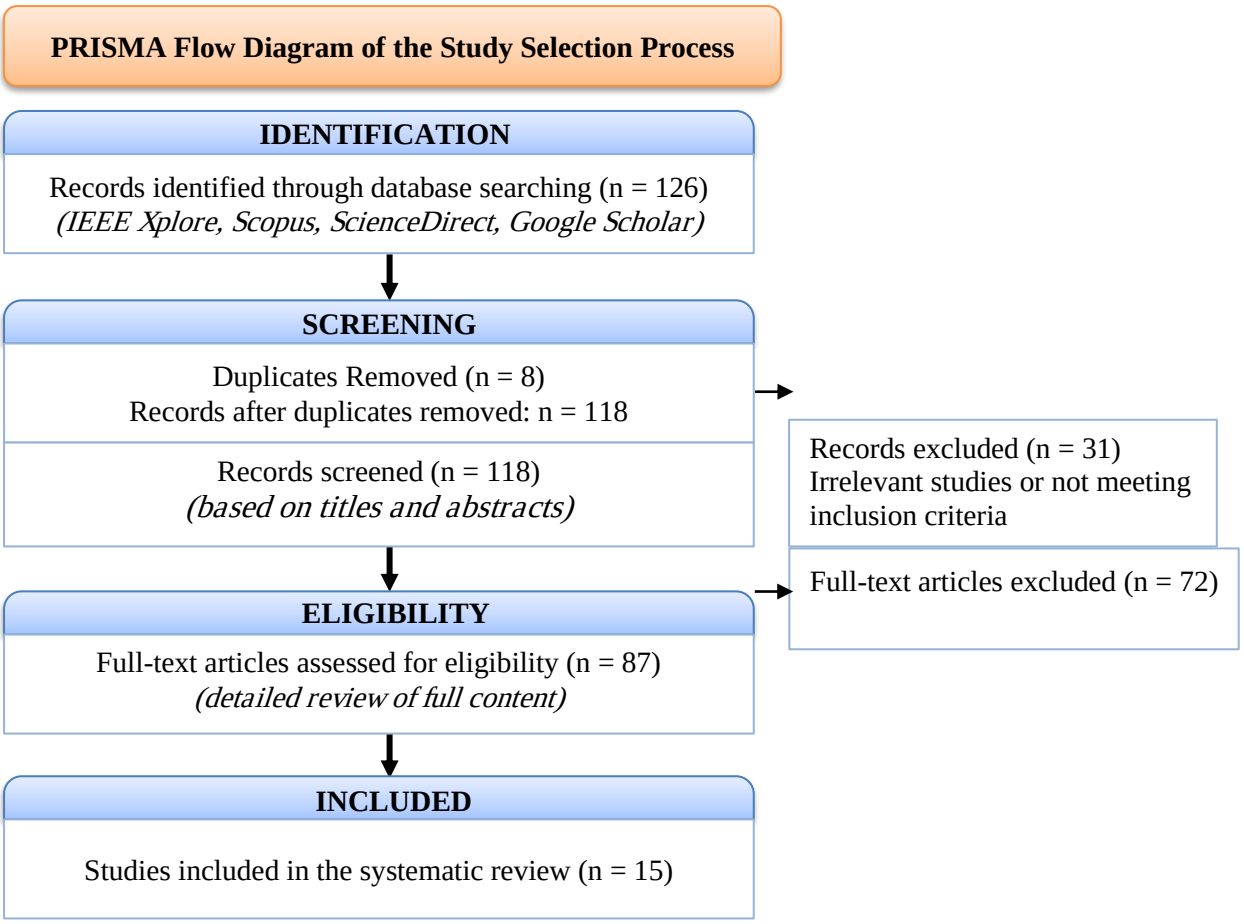

Fig. 3. PRISMA flow diagram illustrating the study selection process used to identify relevant studies for the systematic review.

3. Network Security

Network security is defined as an integrated system of policies, controls and technologies concerned with maintaining network structures and services from any unauthorized modification, disruption or disclosure of information, to ensure the continuity of operation efficiently and reliably in critical conditions without harm to users or workers[5],[6],[7]. Networks were created primarily to enable the sharing of high-cost computing resources, which led to the need for a security framework that focuses on data networks and their physical and software components connected to the internet, and secures them through the appropriate layers of protection [8],[9] .

3.1. alware

Malware are programs that are developed with the aim of weakening or penetrating the security of the system [10]. encompasses many applications designed to harm, exploit, or perpetrate illegal activities on computer systems and networks.[11],[12]. This category include viruses, worms, trojans, ransomware, spyware, and adware, each engineered for objectives such as data exfiltration, system infiltration, espionage, obtrusive advertising, or detrimental resource exploitation [13],[14]. Computers can be infected with malware through several means such as phishing emails, infected websites, software weaknesses, and the installation of additional applications [15]. Infected systems have the ability to mine bitcoins, encrypt data for ransom, build backdoors, and log keystrokes for passwords. Malicious software nowadays uses super clever ways to avoid detection [16] , takes use of flaws in the system that have not been patched yet, and it mimics legitimate software. To protect

oneself against this, one must use current security software, update their system regularly, educate themselves, and follow all cybersecurity standards[17].

3.1.1. Ransomware Definition

A ransomware assault severely limits access to your data unless a ransom is paid. Ransomware is a category of malware or phishing attacks that compromise or encrypt files and directories on a computer, server, or device [18],[19]. When devices or files are secured or encrypted, the offenders may solicit a ransom from the company or the device owner in return for the decryption key. Nonetheless, even promptly following payment, the offenders may fail to furnish the decryption key to the proprietor of the business or gadget, thereby irreparably obstructing access[20].

Taxonomy of Common Ransomware Types

The ransomware attack mainly manifests itself in three forms.[21].

1. Crypto ransomware: . It is malicious software that encrypts the victim's files so that they become unreadable only with the decryption key. After infection it searches for valuable files (documents, photos, databases) and encrypts them at once, then the attacker demands that the victim pay a ransom-often in cryptocurrencies-in exchange for providing him with the recovery key[22],[23].
2. Leakware: This pattern, also known as "doxware," is based on the theft and dissemination of sensitive data as an additional extortion tool besides encryption, where the attacker threatens his victim to publish or sell leaked copies in case of non-payment [24],[25] .This tactic increases psychological and economic pressure on individuals and organizations as a result of risks to reputation and loss of customer trust[26].
3. Locker ransomware: This type completely restricts the victim's access to the system via a lock screen or by disabling device functionalities; it generally does not encrypt files but rather curtails device usage until the ransom is paid[27],[28].
4. Ransomware as a service (RaaS): This type of ransomware involves ransomware developers designing and creating software tools and integrated management platforms that are leased or given to third-party executors for the purpose of carrying out extortion attacks. This business style allows even attackers with limited experience to carry out effective attacks, while package providers share resources and risks and usually receive a percentage of ransom payments[29],[30]. Examples such as Stampado, Jigsaw, Karmen, Cerber, and Atom [31]. embody this economic model of cybercrime, where structured networks for the distribution of ransom tools show how this activity has turned into a stand-alone criminal market [32].
5. Scareware: Ransomware of the 'horror' type poses a growing threat by threatening to release sensitive and personal data - such as customer account data, health records, and trade secrets — to the public instead of just blocking the victim from accessing their files [33],[34].may employ pop-up adverts to deceive users into believing that specific software is mandatory for download, hence utilizing coercive tactics to install malware[35]. Fig. 4. The main classification of ransomware shows depending on the attack mechanism and functional behavior.

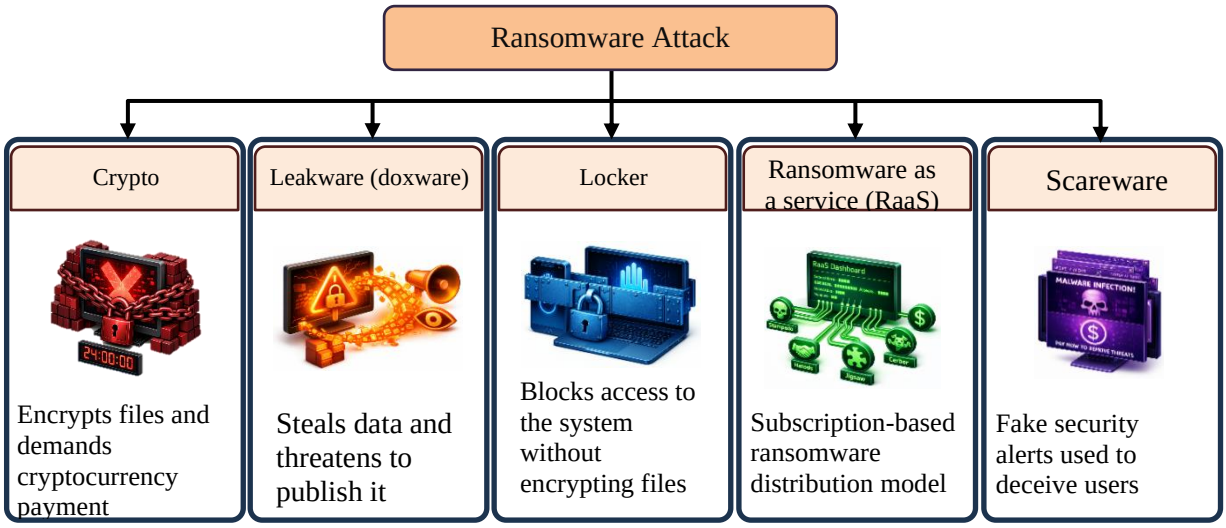

Fig. 4. Taxonomy of common ransomware types based on attack mechanisms.

4. Ransomware attack life cycle

Ransomware programs often exploit asymmetric encryption techniques to carry out their attacks against Target Systems. In general, the course of a ransomware attack can be divided into four stages depending on the reference study [33]. Based on the basics of the current literature, in this study we show the ransomware attack workflow divided into four characteristic stages, as visually shown in Fig. 5 .

1. Logistics and surveillance : At this step, the attacker gathers information about the target to ascertain its vulnerabilities and possible exploitation routes. The collected data may encompass IP addresses, network architecture, and the types and versions of operating systems. Simultaneously, ransomware can utilize multiple methods to infiltrate target computers or systems. Ransomware frequently employs many infection vectors to clandestinely and indiscriminately infiltrate its attack targets [36],[37]. These vectors vary in their complexity and efficacy. (1) Security vulnerabilities: Attackers exploit various security vulnerabilities - such as weak passwords and combinations that trigger remote code execution-to penetrate the victim's internal network and initiate subsequent attacks [38]. (2) Phishing/spam email: Attackers hide the ransomware payload within email attachments (such as documents or photos) or embed malicious links within the body of a phishing message in order to convince the target to click. When the victim interacts with the attachment or link, the malware inserts on the device and begins to perform a series of operations—such as exploiting vulnerabilities, moving sideways within the network, spreading the load to other systems—infecting the entire network [39]. (3) Mobile media: Attackers rely on removable storage media—such as USB and flash drives—and create shortcuts or icons that look like the letters of the drives of those media to deceive the user and push him to click, which leads to the execution of the malicious payload on the device[40]. (4) Software supply chain: Adversaries exploit the mutual trust between the user and the source of the software through mechanisms such as updates and distribution programs within the supply chain, with the aim of injecting ransomware into the victim's environment[41]. (5) Remote desktop: Attackers use brute force attacks to crack weak passwords on a remote desktop service (RDP), and then exploit the acquired credentials to gain access to the victim's server and plant a ransomware[42]. In addition to the previous strategies, ransomware also penetrates systems via other methods such as Exploit kits (EK) — frameworks that exploit vulnerabilities of browsers, extensions and software to automatically deliver the malicious payload to the victims ' devices[43].

2. Attack directive : Once an attacker has exploited a vulnerability, they will use it to launch attacks on the network and will also allocate resources accordingly. Threatening ledgers, dynamic link libraries (DLLs), and other ways to evade software surveillance are some of the ways ransomware is spread. Afterwards, it uses file-sharing protocols to spread laterally or through other ways, increasing the infection's scope and ensuring its persistence in the infected system [44]. In order to gain access, the right attack tools are used.In order to evade detection and increase the attack's success rate, ransomware typically explores the target environment and uses stealth approaches to covertly execute and configure the assault [45],[46].
3. Devastation:In this step, ransomware will execute harmful binary code (e.g., a program) on the compromised system. Subsequently, the malicious malware will seek for and encrypt valuable data files, including databases, pictures, and Microsoft Word documents. Ransomware may use system and network security flaws to infiltrate further systems, including IoT or industrial control systems.[33].
4. Extortion demand: Following a successful assault on the victim, ransomware perpetrators generally need a ransom to be remitted within a designated period, typically 24 or 48 hours [47]. Neglecting to remit the ransom frequently culminates in irreversible data loss or machine malfunction. Should the victim acquiesce to the assailant's demands and remit the ransom, the assailant will furnish the decryption key necessary for the recovery of the victim's data. Nonetheless, even post-payment, there is no assurance that the keys supplied by the perpetrator would effectively decrypt the files. Consequently, victims are atdanger of file loss and concurrent financial detriment [48].

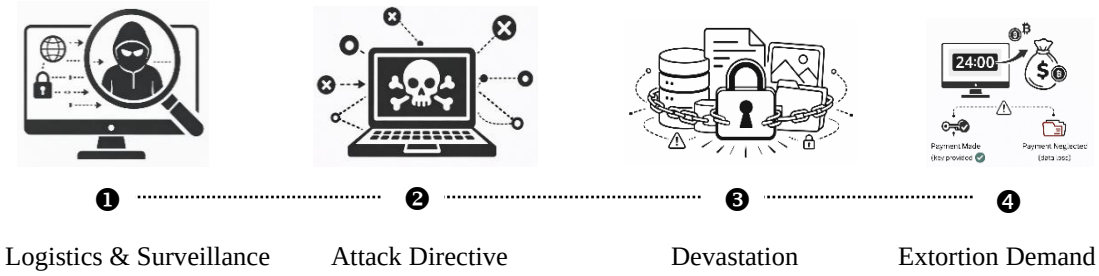

Fig. 5. Lifecycle of a typical ransomware attack in network environments .

5. The evolution of extortion tactics in ransomware attacks

1. Single extortion : The attacker encrypts the victim's files and demands a ransom in exchange for the decryption key — this is the traditional and historically the first pattern in ransomware attacks.[49]
2. Double extortion : Besides encryption, the attacker copies sensitive data from the victim's network and threatens to publish or sell it if the ransom is not paid, which doubles the pressure on the victim.[50]
3. Triple extortion : A third attack is added to the previous mechanic (for example: a DDoS attack that stops the victim's services or directly targets the victim's clients/partners), to increase stress and economic/reputational damage [51] , [52] .

4. Quadruple extortion : The highest evolutionary level-combines encryption, leaks, external attacks (such as DDoS) and additional actions such as: supply chain targeting, threat of disclosure to regulators or the media, or direct attacks on multiple suppliers/customers [53],[54].The goal is to create multidimensional pressure (operational, organizational, informational, financial) [55]. Fig. 6 It shows the evolution of extortion tactics in ransomware attacks: from single extortion to double, triple, and quadruple forms.

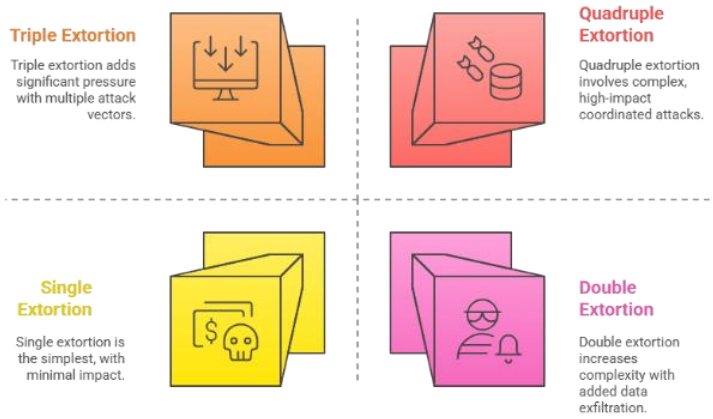

Fig. 6 . The evolution of extortion methods in ransomware attacks.

6. Impact of ransomware attack

In recent years, ransomware attacks have evolved from isolated technical incidents to integrated systematic threats, combining advanced hacking methods with organized extortion networks that affect the operational, financial, legal, reputational and social structures of enterprises. The effects of these attacks are not limited to disrupting operations, but extend to high response and recovery costs, loss of revenue, expenses for hiring external technical experts, as well as side effects on investor confidence and stock prices of affected companies — as highlighted by the Colonial Pipeline accident that accompanied a temporary decline in stock values and increased market volatility [56],[57] . In addition to direct material losses, ransomware attacks generate reputational damage that can erode customer and partner trust and damage long-term business relationships, expanding the scope of potential losses and requiring comprehensive response strategies that go beyond narrow technical solutions [58]. Based on the findings, the most common operational cause for ransomware attacks to succeed is inexperience (40.2%), followed by undiagnosed security flaws (40.1%), and finally, a lack of staff or operational capabilities (39.4%) [59].Fig. 7 illustrates the distribution of operational factors contributing to the success of ransomware attacks.

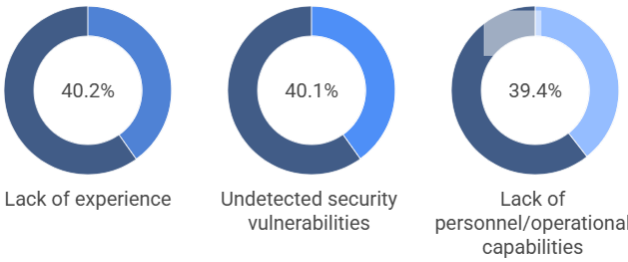

Fig. 7. ransomware attack success factors .

7. Related Works

Ransomware is an important threat to cybersecurity, as it is capable of hiding its malicious activities within legitimate processes, thus making it difficult to detect by traditional signature-based

detection mechanisms. Traditional static analysis is effective in detecting known ransomware samples; however, it is not effective in detecting unknown or obfuscated variants[60]. Dynamic analysis of malware in a sandbox environment is also effective; however, it is computationally expensive to perform dynamic analysis on a large scale within large network environments[61]. To overcome the limitations of traditional ransomware detection mechanisms, recent research has focused on network traffic-based detection mechanisms. Instead of analyzing the executable files of malware, network traffic-based mechanisms analyze the communication patterns of the malware-infected devices, abnormal packet flows, abnormal data transfer patterns, and abnormal connections to the command-and-control centers. Machine learning and anomaly detection mechanisms have been found to be effective in the context of network traffic-based mechanisms[62]. Machine learning and anomaly detection mechanisms derive their effectiveness from their ability to learn the normal behavioral patterns of network traffic, enabling them to detect unusual deviations and provide early detection of malicious activity, including unknown variants of ransomware. However, the effectiveness of these mechanisms does not negate the existence of fundamental technical challenges that continue to hinder the development of a comprehensive and reliable detection system in real-world network environments[63][64]. The challenges include the difficulty of analyzing the network traffic of the malware, the lack of benchmark datasets, the need to achieve high accuracy at the lowest computational cost, and the fact that the effectiveness of the proposed models has been validated within the laboratory environments[65][66]. For the purpose of structured analysis of the existing literature, the literature reviewed in the paper has been grouped according to the techniques used by the authors to detect the ransomware attacks. The classification of the techniques is useful to compare the different methodological approaches to the problem of ransomware attacks.

7.1. Supervised-Based Ransomware Detection Techniques

Supervised learning techniques are trained on pre-labeled network data that includes samples representing both natural and harmful traffic[67]. This study presents a number of supervision-based detection systems that follow standard methodologies established in the literature.

Ahmed and his partner Al-Dabbagh (2021).[68] presented a ransomware detection system based on network traffic analysis using machine learning algorithms, applying several feature selection techniques to CICAndMal2017 data. The research showed the superiority of the Decision Tree and XGBoost algorithms with an accuracy exceeding 99% in the classification of ransomware samples, highlighting the effectiveness of network features in detecting attacks early.

Berrueta et al. (2022).[69] presented a crypto-ransomware detection model based on features extracted from the traffic of file-sharing protocols even when they are encrypted, via machine learning models capable of distinguishing between malicious and normal behavior of users. The system demonstrated a detection capability of up to 99.8% with a very low error rate, and proved its effectiveness even with ransomware samples not present in the training data.

Venturini et al. (2025).[70] presented an extensive analysis of the Differential Area Analysis method used to detect files encrypted with ransomware, and demonstrated its circumventability via three attacks based on reducing the randomness of file headers. The authors proposed three new antagonists (2F, 3F, 4F) whose ability to restore detection accuracy and raise the resistance of the system to various circumvention methods was proved by experiments.

Manmeet mahinderjit Singh and colleagues (2025).[71] suggest developing a framework based on network behavior analysis to extract 84 discriminating features used in the classification of ransomware families on Android devices using machine learning models. The study showed that the Random Forest model achieved the best performance with an accuracy of 95.21% after applying feature selection and cluster techniques, highlighting the effectiveness of traffic analysis in accurately detecting ransomware families.

Table 1. provides a comparative summary of the work published during the period 2021-2025 on supervision-based ransomware detection solutions, highlighting their characteristics, results and limitation .

Table 1. Comparative summary of supervised learning-based ransomware detection approaches.

Author	Detection Method	Dataset	Performance	Strengths	Limitations
Omar Shamil Ahmed; et al / 2021[68]	DT, RF, XGBoost, SVM, KNN, NB	CICAndMal2017	Highest accuracy DT = 99.37%, / F1 = 99.35%	It is based on network features only, which reduces complexity and is easy to apply in real environments.	It is based on Android data only, which limits generalization to other systems.
Eduardo Berrueta; et al / 2022 [69]	RF, J48, Bayes Net, KNN, SVM	Encrypted vs. benign files (Entropy & Structure)	accuracy of KNN = 99.9% / F1 =99.87%	Effective even with fully encrypted files because the features depend on the file structure, not the content.	It does not deal with network traffic or system behavior, it just depends on the properties of the files.
Marco Venturini; et al / 2025 [70]	DAA method (non-ML) + 2F/3F/4F filters	Pre- and post-encryption files	Accuracy = 98.24% / F1 = 97.10%	A fast and light methodology that does not rely on machine learning.	They are based on comparing files before/after encryption, which is not always possible in reality.
Manmeet Mahinderjit Singh; et al / 2025 [71]	DT, RF, KNN, SVM, Bagging	Android Traffic Dataset (392k samples)	accuracy of RF = 95.21% / F1=95.27 %	Using 84 network features and then reducing them to 10 greatly improved performance.	It is intended only for Android network traffic data, which limits generalization.

As shown in Table 1, supervised machine learning techniques demonstrate high effectiveness in ransomware detection. Algorithms such as Decision Tree, Random Forest, and XGBoost frequently achieve detection accuracies exceeding 95% when distinguishing ransomware traffic from benign network behavior. These approaches benefit from their ability to process high-dimensional network features and provide efficient classification performance. However, their effectiveness strongly depends on the availability of labeled datasets, which may limit their applicability in real-world environments. Furthermore, several studies rely on specific datasets, such as Android traffic or file-based encryption data, which may reduce the generalization capability of the proposed models across heterogeneous network environments.

7.2. Unsupervised-Based Ransomware Detection Techniques

This category focuses on anomaly detection techniques that seek to detect unusual patterns in network traffic without the need for pre-titled data; it assumes the predominance of normal behavior, and any deviation from it is an indicator of the possible presence of malicious activity.[72] This study presents a set of unsupervised systems that employ statistical models, cluster algorithms and probabilistic representations to build a baseline of normal behavior and highlight function deviations**.**

Sheldon Chadler et al. (2024).[73] presented an advanced approach to ransomware detection based on multivariate anomalous profiling (MVAP), in which system behavior is analyzed across several dimensions including file system, network traffic, sequence of operations, and resource consumption. The results showed the achievement of high detection accuracy with low rates of false positives and negatives, which confirms the effectiveness of the proposed approach in dealing with sophisticated ransomware attacks and its applicability in practical environments.
Table 2. presents a comparative summary of the published literature on anomaly Detection techniques, highlighting the methodological foundations of these studies, the approved performance measurement indicators, as well as the practical determinants facing their application in real-world environments.

Table 2. summary of work related to non-supervisory (Unsupervised) ransomware detection technologies.

Author	Detection Method	Dataset	Performance	Strengths	Limitations
Sheldon Chadler et al. (2024).[73]	(Multi-Vector Anomaly Profiling - MVAP)	Multi-Vector Behavioral Datasets (File, Network, Process, Resource)	accuracy = 97.1% / F1= 97.1%	High accuracy and speed of response in detecting complex and unknown attacks thanks to its comprehensive and multifaceted analysis	Intensive consumption of system resources and its excessive sensitivity to threshold settings, which may limit its scalability.

The unsupervised anomaly detection approaches do not require labelled data; hence, they provide a significant advantage for the detection of unknown types of ransomware. The approaches discussed in Table 2 show promising performance for the detection of abnormal encryption patterns and multi-vector anomalies. These approaches are more effective for the detection of unknown types of attacks because they focus more on the behavior of the system. Nevertheless, the performance of the unsupervised approaches may also lead to an increased number of false positives because normal changes in system behavior may sometimes be treated as attacks. In addition, the performance of some anomaly detection systems may require careful tuning and may also lead to increased computational overhead.

7.3. Deep Learning -Based Ransomware Detection Techniques

This category represents the latest maturity, as it relies on deep learning capabilities to extract complex patterns directly from raw data without the need for manual feature engineering.[74]. It employs deep neural networks such as Convolutional Neural Networks (CNN), recurrent Neural Networks (RNN/LSTM) and transformers to analyze traffic sequences and learn the temporal and spatial relationships inherent in them.
Presented by Hussein et al. (2024).[75] an innovative methodology based on deep learning algorithms aimed at monitoring ransomware and accurately identifying its software families. The study focused in particular on the challenges associated with software that employs obfuscation techniques, as the results showed the high efficiency of the proposed framework in dealing with these complex threats.
Davidian et al. (2024).[76] an approach to detecting unknown ransomware (Zero-day) is based on monitoring the behavior of software through sequences (API calls). The study concluded the effectiveness of the use of convolutional neural networks (CNN) and long-term memory (LSTM) in identifying malicious patterns with high accuracy when integrating the outputs of operations within the input features.

Developed by Alzahrani et al. (2025) [77]. a "RansomFormer" model that employs deep learning techniques to integrate features of raw bytes with information of software application interfaces (APIs). The results have shown the effectiveness of this cross-Modal approach in improving the detection accuracy of complex ransomware compared to relying on one type of feature.
Proposed by Wang et al. (2025) [78] an approach based on adversarial training using generative competitive networks (GANs) to enhance the durability of long-term memory classifiers (LSTM). The study proved that generating hostile samples and retraining the model on them significantly increases the efficiency of the defense system in countering ransomware that tries to evade detection.
By Rahman et al. (2025).[79] a new strategy for employing large language models (LLMs) in cybersecurity by integrating non-textual data to fine-tune the BERT model. The results showed that this approach enhances the ability to explore hidden semantic relationships in ransomware data, which significantly improved detection rates compared to existing solutions.
Table 3. presents a comparative analysis of the relevant research literature, highlighting the structural architectures of the models and the training methodologies adopted (including self-learning techniques). The table also deals with the key performance measurement indicators, as well as operational determinants and computational costs of the resources required for the application.

Table 3. Comparative analysis of deep learning-based ransomware detection studies.

Author	Detection Method	Dataset	Performance	Strengths	Limitations
Hussein ; et al /2024 [75]	CNN , MLP , LSTM	CIC-MalMem-2022 (OMM-2022 +Self-Created Dataset	Accuracy = 99.99% (CNN, MLP, LSTM)	Camouflage resistance: high detection ability of software that uses obfuscation techniques.	Data dependency : it requires huge amounts of finely sorted data for each family to train the model effectively.
Davidian ; et al /2024 [76]	CNN , LSTM	A data set based on the API Call Sequences (system call sequences)	accuracy of LSTM = 99.27% / F1=99.09%	Early detection: focuses on monitoring the attack in the first seconds of execution.	It requires the software to run in an isolated environment (Sandbox), which may not be effective against software that detects the Phantom environment and hides its behavior.
Alzahrani ; et al /2025 [77]	RansomFormer (Cross-Modal Transformer)	Hybrid data combines PE Bytes (raw data) and API features (dynamic behavior).	Accuracy = 99.50% / F1 = 99.50%	The use of Transformers allows detecting complex and long-term relationships between features.	Transformer architectures are usually heavy and require large memory for inference (Inference).

Wang; et al /2025 [78]	RNN , GRU , LSTM , LSTM-ED	Ransomware samples generated and modified to be hostile (Adversarial Samples).	Accuracy of LSTM-ED / F1 = 99.52%	The system is specially trained to resist dodging and dodging attacks thanks to hostile training.	The process of hostile training takes much more time than traditional training.
Rahman; et al /2025 [79]	LSTM, BERT (Propose)	UGRansome	Accuracy BERT (Proposed) / F1 = 99.21%	A superior ability to understand hidden semantic relationships in non-textual data.	Converting digital attributes (Non-text) into a text format that BERT understands may lead to the loss of some fine details.

Deep learning ransomware detection methods use CNN, LSTM, and Transformer models to automatically detect ransomware attacks through learning complex patterns from system-level data. As shown in Table 3, deep learning ransomware detection methods can achieve high detection accuracy, as several studies have reported an accuracy of more than 99%. However, the main advantage of deep learning models is their ability to automatically detect complex features in large data sets, which improves their potential to detect complex ransomware attacks. However, it is also important to note that deep learning models require large data sets to achieve high detection accuracy, which might limit their use in real-time ransomware detection systems. In addition, it is also important to note that deep learning models might lack generality due to their use of specific data sets to train their models.

7.4. Hybrid-Ransomware Detection Techniques

Continuing with the previous discussions on the detection approaches based on supervised learning, unsupervised anomaly detection, and deep learning paradigms, the hybrid approach has been proposed as an integration of the above approaches by exploiting the benefits and avoiding the shortcomings of the above approaches. The integration of classification approaches with anomaly-based detection approaches has provided the system with the capability of effective generalization as well as the ability to detect zero-day attacks in the network traffic, even in the presence of encryption and concept drift [80]. This approach has been popularized in the literature as well as in the industry for its flexibility and high adaptability.

Presented by Woo et al. (2024) [81]. a framework based on the integration of deep learning (CNN) with machine learning (RF) to analyze network flows to detect ransomware. Based on the findings, this strategy offers a strong alternative to conventional signature-based approaches for reliably and accurately detecting complex attacks.

Li et al. (2024) [82] proposed an innovative technique called Semantic Flow mapping, which relies on graph Theory to model system interactions and detect atypical programming practices. The study proved the effectiveness of this approach when combined with neural networks in tracking complex cyber attacks in real-time, while ensuring efficient operational performance without overloading system resources.

Itasoy et al. (2024) [83] suggest a ransomware detector that employs a hybrid of Isolation Forest and XGBoost for file system access monitoring. The authors tested the ransomware detector using actual Windows file system logs containing over 50,000 events from various ransomware attacks. Results: precision >95%, F1 ≈96%, false positives 2-3.9%, detection time <2.4 seconds. The proposed approach is system-level but requires a controlled environment, thus necessitating a more flexible network-level approach.

Muhammad S (2025) [84] suggests an AI-based hybrid approach to protect digital banking from ransomware attacks. This approach uses a CNN-based deep learning technique along with an unsupervised Autoencoder to detect ransomware. This technique uses multi-source behavioral data from a synthetic 1M event dataset. This approach has 94.3% accuracy, 94.2% F1, 95.6% recall, and 1.8s latency. The disadvantages are related to the use of synthetic data and increased computational requirements. This approach is highly relevant as it uses network traffic features along with anomaly detection.

Deleon J et al. (2025) [85] presented a proactive approach based on lightweight Neural networks to analyze the dynamic interactions of the system and monitor threats in real time. The study also demonstrated the effectiveness of this particular architectural model in penetrating and countering the camouflage approaches used by ransomware attacks and obtaining high detection rates with fewer false positives compared to other methodologies.

Table 4. presents a comparative analysis of the published research literature within this scope.

Table 4. Related works on hybrid-ransomware detection technologies.

Author	Detection Method	Dataset	Performance	Strengths	Limitations
Woo; et al / 2024 [81]	CNN + RF	(Network Traffic Patterns)	Accuracy = 94.6% / F1= 92.9%	High ability to adapt to new variables as soon as they appear.	Focusing on traffic (Network Traffic) may make the model less effective against ransomware that runs locally (Offline Encryption) without an immediate connection to the server.
Li; et al / (2024) [82]	Graph + Clustering + Neural Networks	Host-based (Behavioral)	Accuracy / F1 = 98.7%	The use of graph theory (Graphs) allows understanding the full context of processes instead of looking at them as isolated events	The effectiveness of this technique depends on the accuracy of determining the 'baseline', as distinguishing between legitimate shifts and abnormal activities remains a challenge that increases the rate of false alarms.
Itasoy et al., 2024 [83]	Isolation Forest + XGBoost	File System Logs	Accuracy = 95–97% / F1 = 96%	Fast detection suitable for real-time use	Host-based approach, not network-focused

Muhammad S / 2025 [84]	CNN + Autoencoder	A synthetic test dataset simulating digital banking environments.	Accuracy = 94.3% / F1=94.2%	The use of Autoencoders helps in detecting previously unknown anomalies (Zero-day).	The model is trained and tested on synthetic Dataset generated data, which may not accurately reflect the chaos and complexity of data in real banking environments.
Deleon J; et al / 2025 [85]	(Contextual Signature Extraction) + (Lightweight Neural Networks)	Dynamic system interactions for families such as LockBit and BlackCat.	Average accuracy = 94.5% / F1= Not reported	The most important advantage is the detection before the encryption starts, which protects the data from elementary damage.	Relying on predictive profiling can sometimes lead to blocking legitimate programs that perform intensive operations if their behavior resembles ransomware.

For instance, hybrid detection approaches are designed in a manner that tries to exploit the benefits of using multiple, diverse ransomware detection approaches, including machine learning-based classifiers as well as anomaly-based approaches. As indicated in Table 4, hybrid approaches are observed to offer effective trade-offs in terms of achieving high accuracy in ransomware detection while still managing to detect new forms of attack patterns. Hybrid approaches are perceived as promising in the development of effective zero-day ransomware detection systems, owing to the integration of pattern as well as behavioral anomaly-based approaches. However, there is the tendency for hybrid approaches to be associated with increased complexity, which may require optimization in order to ensure effective usage in ransomware detection systems.

A systematic synthesis of the reviewed literature suggests that network behavioral monitoring is a promising and robust concept for the early detection of ransomware attacks, especially in addressing the challenges associated with the application of traditional static analysis in the presence of anti-obfuscation techniques. Nevertheless, the application of these approaches in real-world network scenarios is considered challenging. One of the major challenges associated with the application of these approaches is the presence of false positives in the analysis of the encrypted network traffic, which might impact the reliability of the security alerts.

7.5. Research Gaps

Despite the major contributions made in the field of ransomware detection using these approaches, there exist major issues that need to be addressed. For instance, most of these approaches have shown their contribution to the field of ransomware detection using certain data sets, which may affect the ability of these models to generalize in a wide variety of networks. In addition, the increase in the number of networks using encrypted communication channels makes the process of analyzing such traffic a challenge, which affects the process of ransomware detection. Furthermore, despite the high accuracy shown by most of these models in the process of ransomware detection, the rate of false positives is still a major concern in the field of anomaly-based approaches, as these models have a high possibility of being classified as ransomware. In order to overcome the challenges that exist in

the field of ransomware detection, there is a need to develop effective models that can handle these challenges, while maintaining high accuracy in the process of ransomware detection.
These identified gaps highlight the need for more advanced detection strategies, which motivates future research in ransomware detection systems.

8. Conclusion

The study presented a comprehensive systematic review of ransomware detection techniques, especially with regard to network traffic analysis and anomaly detection techniques. The study reviewed fifteen recent studies published between 2021 and 2025. The studies were classified according to their respective ransomware detection techniques, which were divided into four categories: supervised learning, unsupervised anomaly detection, deep learning, and hybrid approaches. Based on the findings of the reviewed studies, it is evident that ransomware detection techniques, especially machine learning and deep learning techniques, have high detection rates, with accuracy ranging between 95% and 99%. Another advantage of using network traffic is that it is more effective compared to analyzing malicious files, especially because it can detect unknown ransomware variants. Despite these positive findings, there were challenges affecting ransomware detection, such as the lack of a standardized dataset, complexity in analyzing encrypted network traffic, false positives, and a lack of validation of the reviewed approaches. Based on the study's findings, there is a clear understanding of the importance of developing more effective ransomware detection techniques. Therefore, it is recommended that future studies focus on developing hybrid approaches, especially those that combine machine learning, anomaly detection, and deep learning techniques. Future studies should focus on developing more effective approaches, especially those that can effectively detect ransomware in large-scale networks, thus helping to develop more effective approaches to mitigate ransomware attack threats.

References

[1] S. Morgan, "Global ransomware damage costs predicted to hit $57B annually in 2025," Cybersecurity Ventures, Sausalito, CA, USA, 2025.
[2] Sophos Ltd., "The State of Ransomware 2025: Findings from an independent survey of 3,400 IT and cybersecurity leaders across 17 countries," Abingdon, U.K., 2025.
[3] NCC Group and Fox-IT, "Cyber Threat Intelligence Report: Review of Q2 2025," NCC Group, U.K., Tech. Rep., 2025.
[4] Brandefense, "Ransomware Trends Report Q2 2025 with Comparison Q1 2025," Brandefense, Tech. Rep., 2025.
[5] J. Mongay Batalla, "Featured Papers on Network Security and Privacy," Feb. 01, 2024, *Multidisciplinary Digital Publishing Institute (MDPI)*. DOI: 10.3390/jsan13010011.
[6] "Network Security Concepts, Dangers, and Defense Best Practical," *Computer Engineering and Intelligent Systems*, Mar. 2023, DOI: 10.7176/ceis/14-2-03.
[7] A. Alexei and A. Alexei, "THE DIFFERENCE BETWEEN CYBER SECURITY VS INFORMATION SECURITY," *Journal of Engineering Science*, vol. 29, no. 4, pp. 72–83, Jan. 2023, DOI: 10.52326/jes.utm.2022.29(4).08.
[8] F. Ojo, B. Ojo, F. Fidelis, and S. Lawrence, "AN OVERVIEW OF NETWORK SECURITY AND MANAGEMENT," 2024. [Online]. Available: https://www.researchgate.net/publication/381480940
[9] P. Rajesh Kanna and P. Santhi, "Exploring the landscape of network security: a comparative analysis of attack detection strategies," *J. Ambient Intell. Humaniz. Comput.*, vol. 15, no. 8, pp. 3211–3228, Aug. 2024, DOI: 10.1007/s12652-024-04794-y.
[10] J. Ferdous, R. Islam, A. Mahboubi, and M. Z. Islam, "A Review of State-of-the-Art Malware Attack Trends and Defense Mechanisms," *IEEE Access*, vol. 11, pp. 121118–121141, 2023, DOI: 10.1109/ACCESS.2023.3328351.
[11] R. Hasan *et al.*, "Enhancing malware detection with feature selection and scaling techniques using machine learning models," *Sci. Rep.*, vol. 15, no. 1, Dec. 2025, DOI: 10.1038/s41598-025-93447-x.

[12] S. Berrios, D. Leiva, B. Olivares, H. Allende-Cid, and P. Hermosilla, "Systematic review: Malware detection and classification in cybersecurity," *Applied Sciences*, vol. 15, no. 14, p. 7747, 2025.
[13] S. F. Ali, M. R. Abdulrazzaq, and M. T. Gaata, "Learning Techniques-Based Malware Detection: A Comprehensive Review," Jan. 10, 2025, *Mesopotamian Academic Press*. DOI: 10.58496/MJCS/2025/018.
[14] M. Maghanaki, S. Keramati, F. F. Chen, and M. Shahin, "Generation of a Multi-Class IoT Malware Dataset for Cybersecurity," *Electronics (Switzerland)*, vol. 14, no. 21, Nov. 2025, DOI: 10.3390/electronics14214196.
[15] S. R. Kadari, G. Radhika, M. Shekar, R. V. V. S. Ravi Shankar, and C. Madhu, "A Study on the Key Applications of Malware," *International Journal of Advanced Research in Science, Communication and Technology*, pp. 481-485, Aug. 2024, DOI: 10.48175/IJARSCT-19359.
[16] A. Z. Chahoki, H. R. Shahriari, and M. Roveri, "CryptojackingTrap: An Evasion Resilient Nature-Inspired Algorithm to Detect Cryptojacking Malware," *IEEE Transactions on Information Forensics and Security*, vol. 19, pp. 7465–7477, 2024, DOI: 10.1109/TIFS.2024.3353072.
[17] 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," Mar. 01, 2023, *MDPI*. DOI: 10.3390/electronics12061333.
[18] A. Warikoo, "Perspective Chapter: Ransomware," in *Malware - Detection and Defense*, IntechOpen, 2023. DOI: 10.5772/intechopen.108433.
[19] L. Albshaier, S. Almarri, and M. M. H. Rahman, "Earlier Decision on Detection of Ransomware Identification: A Comprehensive Systematic Literature Review," Aug. 01, 2024, *Multidisciplinary Digital Publishing Institute (MDPI)*. DOI: 10.3390/info15080484.
[20] J. A. Gómez Hernández, P. García Teodoro, R. Magán Carrión, and R. Rodríguez Gómez, "Crypto-Ransomware: A Revision of the State of the Art, Advances and Challenges," Nov. 01, 2023, *Multidisciplinary Digital Publishing Institute (MDPI)*. DOI: 10.3390/electronics12214494.
[21] S. H. Kok, A. Abdullah, N. Z. Jhanjhi, and M. Supramaniam, "Prevention of crypto-ransomware using a pre-encryption detection algorithm," *Computers*, vol. 8, no. 4, Dec. 2019, DOI: 10.3390/computers8040079.
[22] A. Alqahtani and F. T. Sheldon, "Temporal Data Correlation Providing Enhanced Dynamic Crypto-Ransomware Pre-Encryption Boundary Delineation," *Sensors*, vol. 23, no. 9, May 2023, DOI: 10.3390/s23094355.
[23] X. Fang, E. Song, C. Ning, H. Huseynov, and T. Saadawi, "Crypto-Ransomware Detection Through a Honeyfile-Based Approach with R-Locker," 2025, DOI: 10.3390/math.
[24] S. Razaulla *et al.*, "The Age of Ransomware: A Survey on the Evolution, Taxonomy, and Research Directions," *IEEE Access*, vol. 11, pp. 40698–40723, 2023, DOI: 10.1109/ACCESS.2023.3268535.
[25] T. McIntosh *et al.*, "Ransomware Reloaded: Re-examining Its Trend, Research and Mitigation in the Era of Data Exfiltration," *ACM Comput. Surv.*, vol. 57, no. 1, Oct. 2024, DOI: 10.1145/3691340.
[26] J. Y. Marion, "Ransomware: Extortion Is My Business," *Commun. ACM*, vol. 68, no. 5, pp. 36–47, May 2025, DOI: 10.1145/3697829.
[27] K. Drabent, R. Janowski, and J. Mongay Batalla, "How to Circumvent and Beat the Ransomware in Android Operating System—A Case Study of Locker.CB!tr," *Electronics (Switzerland)*, vol. 13, no. 11, Jun. 2024, DOI: 10.3390/electronics13112212.
[28] A. Albin Ahmed, A. Shaahid, F. Alnasser, S. Alfaddagh, S. Binagag, and D. Alqahtani, "Android Ransomware Detection Using Supervised Machine Learning Techniques Based on Traffic Analysis," *Sensors*, vol. 24, no. 1, Jan. 2024, DOI: 10.3390/s24010189.
[29] E. Kritika, "A comprehensive literature review on ransomware detection using deep learning," Dec. 01, 2025, *KeAi Communications Co.* DOI: 10.1016/j.csa.2024.100078.
[30] P. H. Meland, Y. F. F. Bayoumy, and G. Sindre, "The Ransomware-as-a-Service economy within the darknet," *Comput. Secur.*, vol. 92, p. 101762, 2020.

[31] D.-I. GRIGORIȚĂ, E. DIMA, I.-A. BUICĂ, and E. SIMION, "Ransomware in the Automotive Industry," *Romanian Cyber Security Journal*, vol. 7, no. 1, pp. 3–22, Jun. 2025, DOI: 10.54851/v7i1y202501.
[32] K. Oosthoek, J. Cable, and G. Smaragdakis, "A Tale of Two Markets: Investigating the Ransomware Payments Economy," May 2022, [Online]. Available: http://arxiv.org/abs/2205.05028
[33] M. Cen, F. Jiang, X. Qin, Q. Jiang, and R. Doss, "Ransomware early detection: A survey," Feb. 01, 2024, *Elsevier B.V.* DOI: 10.1016/j.comnet.2023.110138.
[34] A. Alraizza and A. Algarni, "Ransomware Detection Using Machine Learning: A Survey," Sep. 01, 2023, *Multidisciplinary Digital Publishing Institute (MDPI)*. DOI: 10.3390/bdcc7030143.
[35] J. Li, G. Yang, and Y. Shao, "Ransomware Detection Model Based on Adaptive Graph Neural Network Learning †," *Applied Sciences (Switzerland)*, vol. 14, no. 11, Jun. 2024, DOI: 10.3390/app14114579.
[36] B. A. S. Al-rimy, M. A. Maarof, and S. Z. M. Shaid, "Ransomware threat success factors, taxonomy, and countermeasures: A survey and research directions," May 01, 2018, *Elsevier Ltd*. DOI: 10.1016/j.cose.2018.01.001.
[37] F. Oelmaier, U. Knebelsberger, and A. Naefe, "Taktik, Tools und Vorgehen der Angreifer," 2023, pp. 61–105. DOI: 10.1007/978-3-658-41614-0_5.
[38] Y. Lee, J. Lee, D. Ryu, H. Park, and D. Shin, "Clop Ransomware in Action: A Comprehensive Analysis of Its Multi-Stage Tactics," *Electronics (Basel).*, vol. 13, no. 18, p. 3689, Sep. 2024, DOI: 10.3390/electronics13183689.
[39] H. Alshaikh, H. Ahmed, and N. Ramadan, "Crypto-Ransomware Detection and Prevention Techniques and Tools A Survey," *International Journal of Computing and Digital Systems*, vol. 14, no. 1, pp. 10299–10308, Oct. 2023, DOI: 10.12785/ijcds/1401102.
[40] R. R. Simón *et al.*, "Empirical Analysis and Practical Assessment of Ransomware Attacks to Data in Motion," in *2024 IEEE International Conference on Cyber Security and Resilience (CSR)*, IEEE, Sep. 2024, pp. 216–221. DOI: 10.1109/CSR61664.2024.10679487.
[41] H. Siadati *et al.*, "DevPhish: Exploring Social Engineering in Software Supply Chain Attacks on Developers," Sep. 2024, [Online]. Available: http://arxiv.org/abs/2402.18401
[42] Surendra Vitla, "Unsecured Remote Desktop Protocol (RDP) Access: A Gateway for Ransomware Attacks and Corporate Extortion," *Journal of Computer Science and Technology Studies*, vol. 6, no. 2, pp. 150–165, May 2024, DOI: 10.32996/jcsts.2024.6.2.17.
[43] K. Gangwar, S. Mohanty, and A. K. Mohapatra, "Analysis and Detection of Ransomware Through Its Delivery Methods," 2018, pp. 353–362. DOI: 10.1007/978-981-10-8527-7_29.
[44]K. Begovic, A. Al-Ali, and Q. Malluhi, "Cryptographic ransomware encryption detection: Survey," *Comput. Secur.*, vol. 132, p. 103349, 2023.
[45] Y. J. Seng *et al.*, "In-Depth Analysis and Countermeasures for Ransomware Attacks: Case Studies and Recommendations," Sep. 02, 2024. DOI: 10.20944/preprints202408.2261.v1.
[46] C. B. Basha *et al.*, "Understanding and Mitigating Ransomware Threats: Trends, Techniques, and Countermeasures in the Digital Age," in *2023 International Conference for Technological Engineering and its Applications in Sustainable Development (ICTEASD)*, IEEE, Nov. 2023, pp. 383–387. DOI: 10.1109/ICTEASD57136.2023.10585140.
[47] F. Bureau of Investigation, I. Security Agency, M.-S. Information Sharing, and A. Center, "#StopRansomware: Medusa Ransomware."
[48] U. - United Nations Office on Drugs, "Ransomware policy paper UNITED NATIONS Vienna, 2023 UNITED NATIONS OFFICE ON DRUGS AND CRIME."
[49] M. Aggarwal, "Ransomware Attack: An Evolving Targeted Threat," in *2023 14th International Conference on Computing Communication and Networking Technologies, ICCCNT 2023*, Institute of Electrical and Electronics Engineers Inc., 2023. DOI: 10.1109/ICCCNT56998.2023.10308249.
[50] M. Said BOUFLIH, "Specificity of Ransomware Investigation (Analytical Study in Light of the European Cybercrime Programmed 2022) Introduction," 2025. [Online]. Available: http://revue.umc.edu.dz/index.php/h

[51] J. Y. Marion, “Ransomware: Extortion Is My Business,” *Commun. ACM*, vol. 68, no. 5, pp. 36–47, May 2025, DOI: 10.1145/3697829.
[52] “Ransomware in the EU: Assessment of the Threat Landscape and Cybersecurity Governance,” 2024.
[53] M. Mundt and H. Baier, “Threat-Based Simulation of Data Exfiltration Toward Mitigating Multiple Ransomware Extortions,” *Digital Threats: Research and Practice*, vol. 4, no. 4, Oct. 2023, DOI: 10.1145/3568993.
[54] J. O. Buabeng and R. Essah, "Decoding Ransomware: A Thematic Analysis of Trends and Countermeasures," *International Journal of Latest Technology in Engineering Management & Applied Science*, vol. 14, no. 8, pp. 420-423, Sep. 2025, DOI: 10.51583/IJLTEMAS.2025.1408000051.

[55] C. Beaman, A. Barkworth, T. D. Akande, S. Hakak, and M. K. Khan, “Ransomware: Recent advances, analysis, challenges and future research directions,” *Comput. Secur.*, vol. 111, Dec. 2021, DOI: 10.1016/j.cose.2021.102490.
[56] N. Vidović, V. M. Cvetković, H. Beriša, and S. Milašinović, “Understanding Ransomware Through the Lens of Disaster Risk: Implications for Cybersecurity and Economic Stability,” Apr. 27, 2025. DOI: 10.20944/preprints202504.1950.v1.
[57] I. Security Agency, “TLP:CLEAR #StopRansomware Guide CHANGE RECORD,” 2020.
[58]S. Corbet and J. W. Goodell, “The reputational contagion effects of ransomware attacks.” [Online]. Available: https://ssrn.com/abstract=4674924
[59] Sophos Ltd, “THE STATE OF RANSOMWARE 2025,” Abingdon, Oxfordshire, UK, Jan. 2025. [Online]. Available: www.sophos.com
[60]S. Alzahrani, Y. Xiao, S. Asiri, J. Zheng, and T. Li, “A Survey of Ransomware Detection Methods,” 2025, *Institute of Electrical and Electronics Engineers Inc.* DOI: 10.1109/ACCESS.2025.3556187.
[61] M. M. Andronache, A. Vulpe, and C. Burileanu, “Integrated Analysis of Malicious Software: Insights from Static and Dynamic Perspectives,” *Journal of Cybersecurity and Privacy*, vol. 5, no. 4, Dec. 2025, DOI: 10.3390/jcp5040098.
[62] M. Kohli and I. Chhabra, “A comprehensive survey on techniques, challenges, evaluation metrics and applications of deep learning models for anomaly detection,” Jul. 01, 2025, *Springer Nature*. DOI: 10.1007/s42452-025-07312-7.
[63] R. Almuhanna and S. Dardouri, “A deep learning/machine learning approach for anomaly based network intrusion detection,” *Front. Artif. Intell.*, vol. 8, 2025, DOI: 10.3389/frai.2025.1625891.
[64] Z. He, D. Davila, S. Bi, T. Wang, and T. Hou, “Machine Learning for Cybersecurity: A Survey of Applications, Adversarial Challenges, and Future Research Directions,” *Electronics (Switzerland)*, vol. 14, no. 23, Dec. 2025, DOI: 10.3390/electronics14234563.
[65] J. Ferdous, R. Islam, A. Mahboubi, and M. Z. Islam, “A novel technique for ransomware detection using image based dynamic features and transfer learning to address dataset limitations,” *Sci. Rep.*, vol. 15, no. 1, Dec. 2025, DOI: 10.1038/s41598-025-17647-1.
[66] I. H. Ji, J. H. Lee, M. J. Kang, W. J. Park, S. H. Jeon, and J. T. Seo, “Artificial Intelligence-Based Anomaly Detection Technology over Encrypted Traffic: A Systematic Literature Review,” Feb. 01, 2024, *Multidisciplinary Digital Publishing Institute (MDPI)*. DOI: 10.3390/s24030898.
[67] K. K. Verma, B. M. Singh, and A. Dixit, “A review of supervised and unsupervised machine learning techniques for suspicious behavior recognition in intelligent surveillance system,” *International Journal of Information Technology (Singapore)*, vol. 14, no. 1, pp. 397–410, Feb. 2022, DOI: 10.1007/s41870-019-00364-0.
[68] O. Ahmed and O. Al-Dabbagh, “Ransomware Detection System Based on Machine Learning,” *JOURNAL OF EDUCATION AND SCIENCE*, vol. 30, no. 5, pp. 86–102, Dec. 2021, DOI: 10.33899/edusj.2021.130760.1173.
[69] E. Berrueta, D. Morato, E. Magaña, and M. Izal, “Crypto-ransomware detection using machine learning models in file-sharing network scenarios with encrypted traffic,” *Expert Syst. Appl.*, vol. 209, Dec. 2022, DOI: 10.1016/j.eswa.2022.118299.

[70] M. Venturini, F. Freda, E. Miotto, M. Conti, and A. Giaretta, "Differential Area Analysis for Ransomware: Attacks, Countermeasures, and Limitations," *IEEE Trans. Dependable Secure Comput.*, vol. 22, no. 4, pp. 3449–3464, 2025, DOI: 10.1109/TDSC.2025.3532324.
[71] M. M. Singh, K. Selvaraj, and Z. Wei, "Enhanced detection of android ransomware families using machine learning and network traffic analysis," *Bulletin of Electrical Engineering and Informatics*, vol. 14, no. 4, pp. 2987–2996, Aug. 2025, DOI: 10.11591/eei.v14i4.9485.
[72] N. Christakis and D. Drikakis, "Reducing Uncertainty and Increasing Confidence in Unsupervised Learning," *Mathematics*, vol. 11, no. 14, Jul. 2023, DOI: 10.3390/math11143063.
[73] S. Chadler, S. Davis, T. Delacroix, and W. Carrington, "Ransomware Detection Using Multi-Vector Anomaly Profiling for Maximum Security," Nov. 15, 2024. DOI: 10.21203/rs.3.rs-5452210/v1.
[74] A. Redhu, P. Choudhary, K. Srinivasan, and T. K. Das, "Deep learning-powered malware detection in cyberspace: a contemporary review," 2024, *Frontiers Media SA*. DOI: 10.3389/fphy.2024.1349463.
[75]A. Hussain, A. Saadia, M. Alhussein, A. Gul, and K. Aurangzeb, "Enhancing ransomware defense: deep learning-based detection and family-wise classification of evolving threats," *PeerJ Comput. Sci.*, vol. 10, pp. 1–44, 2024, DOI: 10.7717/peerj-cs.2546.
[76] M. Davidian, M. Kiperberg, and N. Vanetik, "Early Ransomware Detection with Deep Learning Models," *Future Internet*, vol. 16, no. 8, Aug. 2024, DOI: 10.3390/fi16080291.
[77] S. Alzahrani, Y. Xiao, S. Asiri, N. Alasmari, and T. Li, "RansomFormer: A Cross-Modal Transformer Architecture for Ransomware Detection via the Fusion of Byte and API Features," *Electronics (Switzerland)*, vol. 14, no. 7, Apr. 2025, DOI: 10.3390/electronics14071245.
[78] P. Wang, H. C. Lin, J. H. Chen, W. H. Lin, and H. C. Li, "Improving Cyber Defense Against Ransomware: A Generative Adversarial Networks-Based Adversarial Training Approach for Long Short-Term Memory Network Classifier," *Electronics (Switzerland)*, vol. 14, no. 4, Feb. 2025, DOI: 10.3390/electronics14040810.
[79] M. Abdur Rahman, G. A. Francia Iii, H. Shahriar, G. Francia III, E. El-Sheikh, and S. Iqbal Ahamed, "A Novel Approach to Fine-tune BERT using Non-Text Features for Enhanced Ransomware Detection", DOI: 10.13140/RG.2.2.35576.15365.
[80] A. Lumazine *et al.*, "Ransomware Detection in Network Traffic Using a Hybrid CNN and Isolation Forest Approach," Oct. 15, 2024. DOI: 10.22541/au.172901014.44599790/v1.
[81] L. Woo, S. Tan, T. Tan, and G. Lao, "A Hybrid Approach to Ransomware Detection Using Convolutional Neural Networks and Random Forests on Network Traffic Patterns."
[82] E. Li, H. He, C. Huang, J. Zhang, H. Cheng, and Y. Ge, "Anomaly-Driven Crypto-Locking Behavior Analysis for Ransomware Detection through Semantic Flow Mapping," Dec. 12, 2024. DOI: 10.36227/techrxiv.173398043.39428308/v1.
[83] E. Itasoy, V. Rosenberg, N. Stavrakis, A. Dietrich, and C. Montanari, "Ransomware Detection on Windows Using File System Activity Monitoring and a Hybrid Isolation Forest-XGBoost Model," Oct. 16, 2024. DOI: 10.21203/rs.3.rs-5257558/v1.
[84] S. Muhammad, "AI-Driven Ransomware Defense Framework for Digital Banking International Journal of Innovative Research in Science Engineering and Technology (IJIRSET) AI-Driven Ransomware Defense Framework for Digital Banking," *Article in International Journal of Innovative Research in Science Engineering and Technology*, 2025, DOI: 10.15680/IJIRSET.2025.1406012.
[85] J. Deleon, C. Hatherleigh, A. Cumberbatch, J. Ashworth, and L. Heathcote, "Predictive Profiling Framework for Ransomware Detection Using Contextual Signature Extraction," 2024.

Journal of Basrah Researches (Sciences) **52**(1), 135 (2026)
DOI: https://DOI.org/10.56714/bjrs.52.1.11

الكشف عن برامج الفدية المستندة إلى حركة مرور الشبكة باستخدام خوارزميات الكشف عن الشذوذ: مراجعة منهجية شاملة

قصي جودة شاهين*، إسراء صالح العلماري

قسم علوم الحاسبات، كلية التربية للعلوم الصرفة، جامعة واسط.

معلومات البحث

الاستلام 14 شباط 2026
المراجعة 17 اذار 2026
القبول 19 اذار 2026
النشر 30 حزيران 2026

الكلمات المفتاحية

الكشف عن الفدية ، الكشف عن الشذوذ ، الامن السيبراني ، تحليل حركة مرور الشبكة ، الخوارزميات الهجينة ، الدفاع الاستباقي.

الملخص

تقدم هذه الدراسة مراجعة منهجية شاملة لمختلف تقنيات الكشف عن برامج الفدية، مع التركيز بشكل خاص على تحليل حركة مرور الشبكة وخوارزميات الكشف عن الحالات الشاذة. ووفقًا لبروتوكولPRISMA ، تحلل هذه الدراسة ستة عشر ورقة بحثية نُشرت بين عامي 2021 و2025. وقد تم جمع هذه الأوراق البحثية من مصادر قواعد البيانات العلمية البارزة، بما في ذلك IEEE Xplore و Scopus و ScienceDirectو Google Scholar. يمكن تصنيف مجموعة المقالات البحثية بشكل عام إلى أربع فئات رئيسية لتقنيات الكشف عن برامج الفدية: مناهج التعلم الآلي الخاضع للإشراف، وتقنيات الكشف عن الحالات الشاذة غير الخاضعة للإشراف، ومناهج التعلم العميق، والمناهج الهجينة للكشف عن برامج الفدية. يكشف التحليل المقارن للمقالات البحثية أن مناهج التعلم العميق تمكنت من تحقيق دقة كشف أعلى تزيد عن 99٪، في حين تمكنت مناهج الكشف عن الحالات الشاذة غير الخاضعة للإشراف من إظهار قدرة أكبر على التكيف في الكشف عن برامج الفدية. ومع ذلك، فإن مجال الكشف عن برامج الفدية يعاني من عدة ثغرات بحثية يجب معالجتها: عدم وجود مجموعات بيانات موحدة للتجارب، ومعالجة حركة مرور الشبكة المشفرة، وظهور نتائج إيجابية خاطئة في عملية الكشف. يوضح البحث الحاجة إلى دمج تقنيات الكشف الهجينة والسلوكية لتعزيز متانة أنظمة الأمن السيبراني ضد هجمات برامج الفدية الجديدة.

Citation: Q. J. Shaheen, E. S. Alomari., J. Basrah Res. (Sci.) **52**(1), 135 (2026). DOI:https://DOI.org/10.56714/bjrs.52.1.11

***Corresponding author email:** qusayjoudah6@gmail.com

ISSN: 1817-2695 (Print); 2411-524X (Online)
Online at: https://jou.jobrs.edu.iq