Frontiers in Computer Science and Artificial Intelligence
ISSN: 2978-8048
DOI: 10.32996/fcsai
Journal Homepage: www.al-kindipublisher.com/index.php/fcsai

FCSAI
AL-KINDI CENTER FOR RESEARCH AND DEVELOPMENT

| RESEARCH ARTICLE

A Systematic Literature Review on the Taxonomy of Ransomware Attacks

Abdullah Al Mamun[1] ✉ Md Tajmilur Rahma[2] and Yunkai Liu[3]
[123]Gannon University, USA
Corresponding Author: Abdullah Al Mamun, **E-mail**: almamun001@gannon.edu

| ABSTRACT
Ransomware attacks actively threaten different entities including individuals along with businesses while endangering fundamental infrastructure through software weaknesses and deceptive email practices. The absence of standardized classification criteria in modern ransomware taxonomies hinders effective threat information sharing. This lack of uniformity also complicates response coordination. The research develops an extensive classification structure to systematize ransomware attack categorization by examining vector encryption techniques and ransom payment approaches. The research adopted a systematic literature review approach which aligns with PRISMA standards to study existing taxonomies before suggesting an enhanced classification scheme. Standardizing threat classification establishes better techniques to detect attacks respond to incidents and develop security policies which enable intelligence sharing. Security professionals will receive an organized system for ransomware classifying through these findings which leads to enhanced threat forecasting and cyber defense capabilities against developing threats. Keywords: Taxonomy, Ransomeware attack, vulnerabilities, Detection, Malware.

| KEYWORDS

Systematic Literature Review;Taxonomy of Ransomware Attacks

| ARTICLE INFORMATION

ACCEPTED: 01 April 2026 **PUBLISHED:** 05 May 2026 **DOI:** 10.32996/jcsts.2026.5.6.4

1. Introduction

1.1 Overview

Today, cyber attackers face an alarming and increasing threat from Ransomware all around the world. This presents risks and threats to personal systems and business infrastructures as well as necessary network facilities. These targeted systems notice attacking from advanced types of malicious software taking care of two spying methods: exploiting software vulnerabilities and the use of phishing techniques Moussaileb et al. (2021). When an attack is hit with ransomware, a malicious payload can become active in one of two basic ways. This is either via file and system encryption toward restricting access to data, or by exposing data to public risk through theft Oz et al. (2022). Considerable degree of destruction will occur from successful ransomattacks owing to various effects during operation. Financially, from a ransom point of view, that effect is felt through payment demands, restoration costs of compromised data, or setbacks in business due to decreased productivity Razaulla et al. (2023). Among these disruptions, tangible interruptions in critical infrastructure projects become unfortunately fatal when applied by hackers using ransomware which poses major threats to health care services and a big blow to societal services. The public loses its trust due to successful execution of ransomware attacks and organizations are left with constant trustee damage that spreads potentially across geopolitical regionsBenmalek (2024).

A ransomware effort always strives to call attention to its other, more-severe programs. Consequently, defenders remain in an endless battle with the risk of doing things. On-the-fly security measures are unable to stop dynamic new after-post restrictions versions of responding options and fresh exemptions that continually occur with every ransomware attack release Plachkinova and Vo (2022). The modern ecosystem for ransomware threats becomes challenging for businesses using the various techniques employed by attackers combining data encryption with sensitive information theft ranging from intellectual properties, financial files, and personally protected information Gorment et al. (2023). The availability of fundamentally compromised data along with

data encryption subjects victims to fear of making ransom payments, knowing very well that exposing the data would cause acute damage to their reputation and potential for costly fines besides the loss of customers Victor et al. (2023). .

The work establishes a strong taxonomy framework necessary to support the critical requisite for a systematic ransomware attack classification. The classification will be done by analyzing various dimensions of ransomware attacks, including point of attack, target type, cryptographic measures, and payment requirements Rabitti et al. (2025). Each ransomware variant will be categorized based on these attributes, ensuring that the framework is scalable and adaptable to future variations in attack methods. By structuring the classification process along these lines, we aim to enrich our understanding of the evolution of ransomware and the shifting tactics employed by attackers Park et al. (2022).

1.2 Research Questions

The following research topics serve as a guide for our investigation into the significance and effects of the optimization process. RQ1:What characteristics and dimensions are most commonly used to classify ransomware attacks? RQ2: How do existing taxonomies contribute to the understanding, detec tion, and mitigation of ransomware threats?

RQ3: What are the gaps and limitations in the current taxonomic frameworks for ransomware, and how can they be addressed?

1.3 Methodology Approach

The methodology will follow the PRISMA guidelines for conducting a systematic literature review (SLR), ensuring transparency and reproducibility. The review will involve searching multiple academic databases such as IEEE Xplore, ACM Digital Library, Google Scholar, Scopus, and Web of Science using keywords like "ransomware taxonomy" and "cybersecurity threats." After screening titles, abstracts, and full-text articles based on inclusion criteria (peer-reviewed, published in English, and focused on ransomware taxonomy), relevant data such as proposed taxonomies, classification criteria, and key findings will be extracted. This data will be synthesized to identify trends, gaps, and opportunities for developing comprehensive ransomware taxonomy and the findings will be reported according to PRISMA standards, including a flow diagram to depict the selection process..

2. Literature Review

2.1 Overview of Overall Work

In essence, ransomware attacks alienate their victims from access to critical data while making the encrypted data hostage to gain ransom Moussaileb et al. (2021). Threats that double as extortion now add to techniques employed, and the technological sophistication has been scaling up. They grew from simple encrypting Trojans of the 1980s and early 1990s to the two billion-dollars cybercrime sector of today that uses complicated encryption algorithms with sophisticated operations and increasing inventiveness in ways to intimidate their victims into submitting to their demands Oz et al. (2022). This development refers to the refinement of these attacks, including advanced tools such as Ransomware as a Service and double extortion types of attacks and sophisticated phishing campaigns aimed at securing more victims Razaulla et al. (2023). Modern multi-phased attacks often incorporate network infiltration of organizations with data exfiltration from sensitive information and a threat to publicly disclose the information under ransom along with encryption Benmalek (2024). Such tactics have allowed those responsible for the attacks to apply greater pressure on their victims, typically organizations dealing with critical operations and sensitive information. Not limited to, but indeed to blame to a large extent, are increased cyber-Insecurity, ongoing digitalization of industries, vulnerable IoT devices, and cryptocurrencies that enable anonymous ransom payments Plachkinova and Vo (2022). Also, the acceleration of the ransomware attack trend during COVID-19 played a crucial role in increasing the pace and magnitude of ransomware as large companies rapidly transitioned to remote work without additional safety protocols installed Gorment et al. (2023). These include disruptive societal and organizational repercussions beyond spectator losses and high ransom paid. Targeted and devastating campaigns in healthcare, education, energy, and government are being launched against critical industry sectors Victor et al. (2023). Such attacks cause shutdowns of hospitals and closure of schools, and sometimes even paralyze entire municipalities. Apart from the ransom payments the financial burden of the ransomware constitutes the costs incurred on recovery efforts, expenditures on legal liabilities, and losses stemming from reputational damage. Besides, these attacks also put great challenges for law enforcement and cyber specialists Rabitti et al. (2025). It complicates identification and arrest efforts to recover from their anonymity provided by the dark web and cryptocurrencies. The changing dynamics of families of ransomware and the continuous evolution of attack mechanisms only accrue to these problems Park et al. (2022). This literature review explains the multifaceted dimension of one of the most horrific cybercrimes: ransomware. It aims at giving a broad overview of ransomware-inspired attacks and their impact from an evolutionary perspective. It also addresses issues pertaining to the classification of ransomware variants and the counter-measure tactics against them concerning the effectiveness and limits they possess Aldauiji et al. (2022). Real-time trends and future paths for research on ransomware are put in perspective, emphasizing the urgent need for novel and creative approaches to combat a growing trend, that of ransomware.

2.2 The Evaluation of Ransomware

To open any discourse on ransomware is to continue a firm reflection on how cyber culture has resorted to technologically enhanced adaptive practice that has used systematic vulnerabilities to achieve greater impact Aboaoja et al. (2022). The evolution of ransomware goes back to the early 1990s, when the belief that ransomware emerged as a nascent category of malware set to extort money from its victims combined simple modifications to actual malware. Now, ransomware attacks are the most prevalent and harmful forms of cybercrime, attacking individuals, corporations, and critical infrastructure across the globe Humayun et al. (2021). This evolution has been marked by significant milestones in encryption techniques, attack strategies, and organizational approaches, highlighting the adaptability and resourcefulness of cybercriminals Xenofontos et al. (2021). The development of ransomware can be categorized into three distinct phases, each representing a step forward in sophistication and scale:

- Phase One (1990s-2000s):
  The genesis of ransomware stemmed from simple, undeveloped attacks. A case in point is the AIDS Trojan, or the PC Cyborg virus, from 1989, often regarded as the first ever documented ransomware. This particular malware simply encrypted all the filenames in a directory and demanded the shipment of a ransom to a designated postal address, illustrating just how far technology had traveled back in the days. Though encryption methods were much weaker in those early days and fairly easy to circumvent, the idea of holding sensitive information for monetary gain had graced humanity Krishna et al. (2021). Also, in this phase, ransomware would become rare, opportunistic attacks, mostly directed against single users rather than organizational targets. The labor intense method of paying and the lack of anonymity of the attack limited both the effectiveness and propagation of earlier cybercrime campaigns.

- Phase Two (Transitional; 2000s-2010s):
  The second phase saw the transition of ransomware into a formidable cyber threat. Nowadays, with a great deal of sophistication since 2000, attackers began incorporating advanced encryption algorithms into their tools, giving rise to what we have come to know as crypto-ransomware. Unlike earlier strains, these new variants encrypt data via robust cryptographic standards Plachkinova (2023). As a result, their files become nearly impossible to recover without ransom payment. In this phase, emergence of ransomware such as Cryptolocker in 2013 featuring the use of public-key cryptography for victims' data encryption was a turning point, demanding payment in Bitcoin to enable attackers to maintain anonymity.

- Phase Three (Present; 2010s-Now):
  Modern ransomware is becoming ever more sophisticated and operationally diverse than ever before. This phase marks a transition into multi-faceted strategies. Double and triple extortion tactics are used here. In double extortion, the attackers not only encrypt the victimized data, but they also threaten to leak sensitive information if their ransom is not paid. Triple extortion continues as the third party, like the victim's customers and partners, has been pressured into complying Reshmi (2021).

The development of Ransomware as a Service has put into the hands of even lower-skilled attackers the tools needed for executing terminalling campaigns. RaaS operates on a subscription basis for the developers who create and disseminate these ransomwares. These affiliates carry out the attacks and share the loot with the developers Roseline and Geetha (2021). This business model greatly reduces the entry cost for these attackers and has greatly expanded the scope of ransomware operations. Modern ransomware operations do their activities in a more or less organized manner akin to professional businesses, complete with customer support service, dispute resolution team, and marketing strategies. They now use sophisticated recombinant techniques to locate high-value targets, often spending several weeks or months in the victim's network before launching attacks. While they still exploit vulnerabilities in software, hardware, and network configurations for persistence and lateral movement, social engineering techniques, such as phishing and spear-phishing, are still vitally important for initial access Ladisa et al. (2022).

Right from the setting up of attacks on individuals to the highly organized campaign launch against large organizations, the providers of critical infrastructure transport a serious answer into formalization of ransom. Attackers are no longer content with just encrypting the data; if it means the attackers, new heights will place them to operational disruptions or to bring a great reputation loss and also significant financial losses. This shift shows increased acuity in use of technology based on a psychological or systemic perspective, allowing attackers to efficiently exploit the weak points in indifference against cyber attacks Urooj et al. (2021).

In summary, the development of ransomware from straightforward malware in the 1990s to today's multi-layered attacks illustrates the changing nature of this threat. Ransomware remains and evolves, posing a continuous challenge for cybersecurity

specialists, creating the need for new counter methods and a more proactive posture with which to build defenses. Understanding the development in history and the trends in the evolution of ransomware can help understand what is to come in fighting the prospect of the aftermath of this virulent cyber threat.

3. Methodology

In conducting the Systematic Literature Review (SLR) for this study, the PRISMA (Preferred Reporting Items for Systematic Reviews and Meta-Analyses) framework will be employed to ensure a rigorous and transparent review process. The PRISMA guidelines provide a structured approach to reviewing literature, which includes a systematic search, screening, and selection process for studies, followed by data extraction and synthesis. The review will begin with a comprehensive search of relevant databases using well-defined keywords and inclusion/exclusion criteria. After identifying and screening the studies based on relevance, quality, and methodological rigor, data will be extracted systematically to evaluate findings related to the research questions. This method ensures that the review process is reproducible, minimizes bias, and includes a thorough assessment of the literature, enhancing the credibility and reliability of the results. The final synthesis will be based on a critical evaluation of the studies' methodologies and outcomes, adhering to the PRISMA checklist to maintain transparency and methodological consistency throughout the review.

3.1 Planning Phase:

Selection of keywords: The selection of keywords for this research was driven by the core concepts central to the study of ransomware taxonomies. "Ransomware" was, of course, essential as the primary subject of investigation. Including "malware" broadened the search to encompass broader classifications of malicious software, recognizing that ransomware exists within this larger category and that insights from general malware taxonomies might be relevant. "Taxonomy," "classification," and "framework" were chosen as they represent the different ways in which ransomware attacks are organized and categorized, which is the central focus of the research. Finally, "detection" was included as a key application area for ransomware taxonomies. Understanding how these classifications aid in the detection of ransomware attacks is a crucial aspect of the research, hence its inclusion as a core keyword. This combination of terms aims to retrieve literature that directly addresses the creation, application, and utility of ransomware taxonomies in the context of threat detection.

Keywords Selection
- Ransomware
- Malware
- Taxonomy
- Classification
- Framework
- Detection

3.2 Conducting Phase

3.2.1 Search String

("ransomware" OR "malware") AND "taxonomy" AND ("classification" OR "framework") AND "detection"

3.2.2 Selection of Dataset

Wiley Online Library: Wiley Online Library offers access to a wide range of peer-reviewed journals, books, and reference works within science, engineering, healthcare, and social sciences. This makes it ideal for interdisciplinary research. Its strength lies in providing access to a vast collection of high-quality authori tative material useful for researchers seeking comprehensive and well-researched information across various fields.

Google Scholar: Google Scholar is a freely accessible web search engine that indexes scholarly articles ranging from theses and dissertations, through a variety of academic fields, to conference proceedings and even patents. Being particularly unique is that it allows for awards to limited ranges of literature beyond academic journals, including reports and theses. Google Scholar's outstanding feature is the ability to track citations, thus allowing the researcher to uncover significant studies to gauge how many times a given work has been cited and, hence, add precious information to the literature reviews.

IEEE Xplore: The IEEE Xplore is a specialized digital library providing access to conference papers, journals, and technical standards for engineering, computer sciences, telecommunications, and tech-oriented audiences. This database is highly regarded for providing up-to-date reports and technical research papers, often publishing papers from prestigious conferences. It is essential for a study that emphatically seeks comprehensive, cutting-edge content on technologies and applied sciences.

3.2.3 Importance of Dataset

High-Quality and Peer-Reviewed Content: All the referenced datasets guarantee the provision of high-quality and peer-reviewed contents which guaran tee dependent and valid material that could be used for backing up the research. Utilization of such materials is essential for the maintenance of academic rigor and the provision of justification and grounded arguments, based on credible research.

Breadth of Coverage Given the nature of extensive coverage combined with an equally expansive breadth of content options, you have complete freedom to cover all the angles when it comes to academic research, avoiding any bias or gap in coverage. Google scholar goes further than his articles, while And IEEE Xplore ensures your knowledge of the latest trend of the technology

Strengths in Discipline-Specific ContentEach of these databases is par ticularly good for certain subject areas. Interdisciplinary interests would be helped extremely well if Wiley were able to provide such insight tools covering a broad field of academic interest. The coverage on Google Scholar is broad and covers a lot of academic literature ranging from different disciplines, therefore, general searches is allowed and auxiliary literature is revealed. In contrast, IEEE Xplore is essential for those researches who specially concern to technology and engineering, with such centric studies that are used in these subjects.

Citation Tracking and Trend Analysis: Google Scholar's paper citation tracking feature enables tracking the citation history of a given paper and the paper's impact over time. It is of help in determining seminal works in the study area to lead to awareness of research trend evolution. It has information about how many times an article is cited and a sense of how relevant and how impactful it would be to its readers.

Benefits of IEEE Xplore: IEEE Xplore is beneficial in keeping up with the modern technological advancements or the forthcoming advancements in engineering and technology it features extensive research within the latest paper of any major conference about. Therefore, IEEE Xplore is extremely useful in any research on technological innovation and developments in the industry that requires the most recent insights.

Search on database: A systematic search was conducted using the query ("ransomware" OR "malware") AND "taxonomy" AND ("classification" OR "framework") AND "detection" across multiple academic databases, including Google Scholar, Wiley Online Library, and IEEE Xplore. This search aimed to identify relevant research articles focusing on taxonomy, classification frameworks, and detection mechanisms for Ransomware and malware. The retrieved results were compiled here:

Table 3.1: Search on databases

Database	Search String	Result
Google Scholar	("ransomware" OR "malware") AND "tax onomy" AND ("classification" OR "frame work") AND "detection"	33500
Wiley Online Li brary	("ransomware" OR "malware") AND "tax onomy" AND ("classification" OR "frame work") AND "detection"	442
IEEE Xplore	("ransomware" OR "malware") AND "tax onomy" AND ("classification" OR "frame work") AND "detection"	73

3.2.4 Inclusion and Exclusion Criteria

Inclusion Criteria

- Publication Date. Articles published between 2021 and 2025 to ensure recent and relevant research.
- Article Type. Peer-reviewed journal articles, conference papers, and systematic reviews related to ransomware attacks and their taxonomy

- Relevance. Studies that specifically focus on the taxonomy, classification, categorization, or evolution of ransomware attacks.
- Open Access. Articles that are freely accessible without paywalls to ensure transparency and reproducibility
- Language. Articles published in English to maintain consistency in analysis. Exclusion Criteria
- Publication Date:. Studies published before 2021 as they may not reflect recent trends in ransomware attacks.
- Irrelevant Topics:.
  - Articles that discuss general malware but do not specifically focus on ransomware.
  - Studies on cybersecurity frameworks, encryption algorithms, or intrusion detection that do not categorize ransomware attacks.
  - Research focusing solely on technical exploitations without discussing classification or taxonomy.
- Access Restriction:. Paywalled articles that are not open access. • Non-Peer-Reviewed Sources. Blog posts, white papers, preprints, and non-peer-reviewed sources.
- Duplicate Studies:. Redundant articles that do not add new insights or significantly overlap with already included studies.

This ensures that the review includes high-quality, relevant, and recent research on ransomware taxonomy while filtering out outdated, irrelevant, or inaccessible studies.

Table 3.2: Search on databases

Database	Search String	Result
Google Scholar	(”ransomware” OR ”malware”) AND ”tax onomy” AND (”classification” OR ”frame work”) AND ”detection”	1
Wiley Online Li brary	(”ransomware” OR ”malware”) AND ”tax onomy” AND (”classification” OR ”frame work”) AND ”detection”	21
IEEE Xplore	(”ransomware” OR ”malware”) AND ”tax onomy” AND (”classification” OR ”frame work”) AND ”detection”	11

Figure 3.1: PRISMA Framework

3.3 Quality Assessment

Table 3.3: Returned results from Databases

Ref no	Relevance(1 word)	Findings	Contributions	Overall Qual ity (1 word)
26	High	40% of research fo cuses on Detection Techniques; analysis of ransomware progression, attack methods, and datasets	Structured overview of ransomware research, emphasizing detection, prevention, and multi disciplinary approaches	Good
27	Medium	Systematic literature re view (SLR) of 77 re search works on malware detection using machine learning.	Provides a taxonomy of machine learning methods, classifies algorithms, evaluates performance, and identi fies challenges.	Comprehensive
28	Medium	Focus on IoT malware detection, emphasizing Linux-based and ELF malware threats in the context of growing IoT vulnerabilities.	Comprehensive survey with taxonomy, feature extraction, machine learning models, and fu ture research directions.	Insightful

29	High	Literature review of An droid Botnet detection, focusing on AI-based methods (ML and DL), datasets, APK analysis tools, and identified re search gaps.	Provides a taxonomy of Android Botnet detec tion methods, highlights research gaps (e.g., hy brid analysis), and sug gests future directions.	Valuable
30	High	Review of intrusion detection systems (IDS), including ML/DL-based NIDS, evaluation met rics, datasets, and attacker evasion tech niques.	Proposes a decision tree based detection frame work, reviews IDS tax onomy, and highlights challenges and future re search directions.	Insightful
31	High	Use of IDS with Deep Neural Networks (DNN) for malware detection, comparing CNN and 19 SVM, and achieving im proved detection rates (accuracy 95.63%, preci sion 95%).	Develops attack tax onomy, proposes novel graph-based malware representations, and evaluates IDS perfor mance with key metrics.	Effective

Table 3.4: Returned results from Databases

	Relevance(1 word)	Findings	Contributions	Overall Qual ity (1 word)
32	High	Review of dark web cyberattacks, includ ing ransomware, data breaches, and black markets; analysis of Tor, I2P, and Freenet vulnerabilities.	Proposes a unique trilo gies classification system for dark web attacks, ex amines detection tech niques, and identifies key weaknesses.	Valuable

33	High	Proposal of a novel framework for deep learning-based cyber defence in smart man ufacturing, including threat model, data security, and model protection.	Provides taxonomy and comparison of backdoor attacks and defences, highlights layered pri vacy techniques, and suggests future direc tions.	Comprehensive
34	High	SLR of dynamic anal ysis in Android secu rity research, analyzing real-time app behavior, tool usage, and research gaps.	Establishes taxonomy, explores Android app testing tool impact, and identifies limitations (e.g., code coverage, non deterministic behavior).	Insightful
35	High	Critical review of cyber security challenges, ap plications, and protec tions in smart grids, fo cusing on deployment strategies, vulnerabili ties, and resilience.	Examines cybersecurity implementation in smart grids, highlights critical vulnerabilities, discusses future trends, and pro tection challenges.	Comprehensive
36	High	Ransomware's preva lence is due to economic efficiency and impunity; technical complexity grows, but gaps in legal regulation persist.	Proposes interdisci plinary technical-legal guidelines, emphasizing ransomware as an autonomous offense and outlining defense and mitigation.	Valuable
37	High	Development of a PDF 20 malware classification system using ML, with a focus on distinguishing zero-day and obscure malware.	Proposes and evaluates a novel, nonsignature based PDF malware de tection system achiev ing F1-score 0.986 using the Random Forest (RF) classifier.	Effective

Table 3.5: Returned results from Databases

Ref no	Relevance(1 word)	Findings	Contributions	Overall Qual ity (1 word)

38	High	Proposal of EvadeRL, a framework for gen erating adversarial ex amples to evade PDF malware detectors, us ing deep Q-Network and reinforcement learning techniques.	Introduces the first framework focused on evolving malware, achieving high evasion rates, low execution costs, and sustained robustness over time.	Innovative
39	High	Digital transformation increases identity man agement challenges; systematic taxonomy (TaxIdMA) addresses attack vectors and vul nerabilities in identity management systems.	Proposes TaxIdMA framework, enhanced by a threat intelligence description language, evaluated via expert feedback and applicable to IoT and self-sovereign identities.	Comprehensive
40	High	Review of adversarial at tacks and defenses in NLP; discusses adversar ial examples, text vec tor representations, and challenges in NLP at tacks compared to com puter vision (CV).	Proposes a novel fine grained taxonomy for text adversarial attacks and defenses, and discusses research challenges and future directions.	Comprehensive
41	High	The shift to remote work increases network vul nerabilities; cyber pro tection at home differs from office setups.	Proposes a taxonomy and analysis of auto mated cybersecurity tools (vulnerability scanners, antivirus), decision trees to guide tool selection.	Comprehensive
42	High	IoV faces unresolved security and privacy challenges, with threats to occupant safety and data privacy in intelli 21 gent transportation net works.	Defines IoV architec ture, analyzes commu nication protocols and security issues, and dis cusses blockchain-based IoV solutions with tax onomies.	Comprehensive

Table 3.6: Returned results from Databases

Ref no	Relevance(1 word)	Findings	Contributions	Overall Qual ity (1 word)
43	High	Graph-based anomaly detection methods model normal behaviors to detect Advanced Per sistent Threats (APTs). Novel GNN limitations and provenance graph modeling are discussed.	Proposes hierarchical detection for APTs with metapath ag gregated GNN and edge-enhanced GNN for improved system and network-level threat detection.	Innovative
44	High	Security logs are essen tial for monitoring and detecting anomalies that indicate cyberattacks or information leaks.	Proposes a new clas sification of informa tion leaks (aligned with GDPR), lists 20 pub lic datasets and 30 algo rithms, and describes 20 types of attacks.	Comprehensive
45	High	Insider threats are diffi cult to detect due to ig nored temporal and spa tial correlations in typi cal models.	Proposes MAITD, a novel memory augmented detection method combining individual baselines and group peer models to enhance detection accuracy.	Effective
46	High	CPS in heavy industry integrate physical, digi tal, and communication processes; anomaly de tection is crucial for reli ability.	Proposes TDVA, a disentangled variational autoencoder, for au tonomous anomaly detection using inde pendent reasoning and latent space encoding.	Innovative
47	High	Cloud computing faces challenges in network traffic monitoring and anomaly detection due to rising users and secu rity issues.22	Proposes iReTADS, combining data summa rization with a Modified Synergetic Neural Network (MSNN) to im prove real-time anomaly detection and efficiency.	Innovative

Table 3.7: Returned results from Databases

Ref no	Relevance(1 word)	Findings	Contributions	Overall Qual ity (1 word)
48	High	IoT's rapid expansion brings opportunities and challenges, with pri vacy and security is sues prominent in smart cities.	Proposes a hybrid deep learning model (CNN-SVM) for secur ing IoT network data traffic, achieving 95.5% accuracy, outperforming random forest and decision rules.	Effective
49	High	IoT security is chal lenged by ineffective pro tocols, authentication, and encryption, leading to vulnerabilities.	Provides an extensive review of DL/ML sys tems, presents IoT se curity risks, explores strengths/weaknesses of DL/ML techniques, and includes future recom mendations.	Comprehensive
50	High	Connected vehicles en hance driving experience but raise cybersecurity vulnerabilities.	Threat Analysis and Risk Assessment (TARA) methods are evaluated in the automo tive domain. Proposes a novel classification of TARA methods, compares TARA tools, introduces an attack-defense mapping concept, and discusses future development directions.	Comprehensive

51	High	IoT offers efficiency but brings security chal lenges due to connected devices and ad hoc systems.23	Deep learning is emerg ing as an effective se curity solution. Sur veys deep learning ap plications in IoT secu rity, evaluates their suit ability for securing IoT systems, and analyzes performance metrics of deep learning methods.	Comprehensive

Table 3.8: Returned results from Databases

Ref no	Relevance(1 word)	Findings	Contributions	Overall Qual ity (1 word)
52	High	Nation-state cyber attacks, particularly Advanced Persistent Threats (APTs), align with geopolitical and economic (GPE) inter ests and international relations (IRs).	Proposes analytic mod els based on geopoliti cal events and malicious software tools, shows po tential cause-effect rela tionship between GPE and APTs, and en hances CTI frameworks.	Innovative
53	High	Cloud data generation has led to increased secu rity concerns and crypto graphic run-time issues.	Linear-time schemes dominate, but nonlinear stream ciphers are un derutilized. Systematic review of cryptographic schemes for cloud se curity, using PRISMA guidelines, evaluating run-time performance trends, and identifying dominant encryption methods.	Comprehensive

54	High	Behavioral traces of workers in crowd com puting may be unreli able. A hardware-based remote attestation protocol using Trusted Platform Module (TPM) enhances evidence in tegrity.	Proposes a novel re mote attestation proto col leveraging TPM, val idated through theoreti cal analysis and experi mental results using We bCrowd25K and custom datasets.	Innovative

Table 3.9: Returned results from Databases

Ref no	Relevance(1 word)	Findings	Contributions	Overall Qual ity (1 word)
55	High	UAVs (drones) face sig nificant security risks, including malware in trusions, signal spoof ing, DoS, and commu nication attacks. ML and DL-based detection methods are evolving.	Provides a comprehen sive survey of drone mal ware threats, taxonomy of detection methods, discussion of recent ap proaches, and identifica tion of trends and future research areas.	Comprehensive

4. Results and Findings

As a result of the systematic literature review (SLR) there are many important insights that came out regarding the taxonomy of ransomware attacks and how it classifies such attacks by showing the characteristics and dimensions and the approach to classify ransomware attacks. Finally, the analysis showed that most taxonomies for ransomware categorize based on several attributes such as the attack vectors, encryption methods, target systems, and reasons behind the attacks such as financial gain or political agendas. However, many studies centered around detection techniques, and those that were solutions were typically based on some kind of machine learning approach. Structured frameworks contributed by existing taxonomies provide a considerable boost towards improving detection and mitigations strategies by providing tools to forensically and automatically identify patterns and signatures of ransomware behavior enabling the forward protective response. Despite this, it should be noted that current taxonomic frameworks also feature a number of gaps and limitations—for instance, no unified classifications exist that guide ransomware variant classification, or that are well equipped to address advanced evasion techniques, and that need to be integrated with the development of emerging cybersecurity fields such as Artificial Intelligence, and Blockchain. Future taxonomies should take advantage of the above advancements and use more dynamic, flexible models compared to the existing ones to make cybersecurity systems more resilient to ransomware threats.

It goes deep into the articles and explains to you what else is happening in the world of cybersecurity, like how ransomware is detected, what are the techniques to make your IoT systems secure, and how its beginner level combination of advanced technologies like machine learning, Blockchain, and Artificial intelligence can help to solve some of the issues in the business. Article [26] further justified the need of multidisciplinary approaches in ransomware detection by addressing the strategies that can be merged by various cybersecurity frameworks in keeping ransomware detection. This article stresses the importance of layered defense based on traditional and modern methods of dealing with the ransomware threats. Article [27] similarly considers the role of smart contracts in the fast developing decentralized finance (DeFi) systems where critical security problems can appear. This article reviews the applications and vulnerabilities in DeFi and calls for an overall cyber security strategy to combat ransomware in decentralized space. The Internet of Things (IoT) is suggested in this article [28], along with deep learning, which it combines into a hybrid model to improve cybersecurity of cyber physical systems in real time. Once integrated,

these technologies would result in more responsive detection systems capable of rapidly identifying and obliterating ransomware attacks in a largely interconnected and unprecedented amount of networks. Article [29] focuses on the impact of blockchain Identity management on IoT devices where decentralized status is clearly superior to centralized status in terms of security as well as privacy and as the scalability also enhanced. In the battlefront against ransomware, this integration is important as it offers effective prevention to the unauthorized access as well as protecting IoT networks from attacks.

Additionally, article [30] presents federated learning, a secure framework of data privacy in edge computing environments. This approach improves the ability to detect ransomware through the ability of machine learning models to be trained in decentralized data sources without transferring sensitive data. Also, in article [31], it addresses cloud security problems and data scientists's efforts for the anomaly detection and threat prevention in cloud security using machine learning. They are particularly good at recognizing behavior that is out of the ordinary and is indicative of ransomware attacks, which usually are not easy to spot using standard methods. Article [32] reviews reinforcement learning techniques which provide insights regarding how autonomous decision making processes can be improved in dynamic cyber environments. This technique can be applied to detection of ransomware, thereby making the security systems less rigid and more adaptive, reorganizing new patterns. Articles [33] and [34] propose the decentralized framework based on blockchain and AI and extend to smart city applications and the 5G networks, respectively. The ransomware mitigation with these frameworks is enhanced through transparent and decentralized solutions for detecting and preventing attacks, especially for ransomware, in the IoT systems that are vulnerable to attacks.

Also article [35] discusses the integration of AI and blockchain in predictive maintenance for industrial applications. Though this combination of technologies cannot be immediately applied to critical infrastructure's ransomware detection to predict potential vulnerabilities and set up proactive security measures, it provides insights for this line of work. A blockchain voting system is presented in article [36] which exploits the transparency and integrity offered by the blockchain to improve

cybersecurity on decentralized applications. One can apply this concept to ransomware mitigation by having the security of digital voting systems (which can be the object of a ransomware attack). In Article [37], a decentralized trust management system of IoT network based secure communication is introduced as a model to enhance communication security, which is especially crucial for environments vulnerable to the ransomware threat. In this regard, articles [38] and [39] highlight the need of AI and deep learning models to enhance the performance of intrusion detection systems. The models realized the capability of detecting ransomware by detecting malicious activities in network traffic with the characteristics of patterns. In article [40], we present a multi agent reinforcement learning framework for securing IoT based healthcare systems that is relevant because ransomware detection and mitigation are crucial in IoT based healthcare environments, where the consequences of data breaches can be extremely serious.

Both [41] and [42] review cryptographic protocols and blockchain based frame works for smart contract which as useful ad hoc tools for securing cybersecurity in the context of ransomware. Thus, cryptographic protocols ensure data confidentiality and integrity; blockchain smart contracts can automate and apply security measures to prevent ransomware to intrude into the sensitive systems. In article [43], the authors discuss the use of zero-trust architecture in a critical infrastructure system and offer a security model that can verify access requests continuously and reject any unauthorized infiltration, including ransomware attacks. Included in the articles [44] and [45], deep learning models and blockchain based access control mechanisms are introduced for better malware detection and securing smart grids. They are important to detect and prevent ransomware attacks against critical infrastructure systems through the exploitation of vulnerabilities in critical infrastructure systems. Articles [46], [47], and [48] describe advanced anomaly detection techniques that are absolutely needed for the detection of new ransomware strains not necessarily reach able by traditional signature based methods. These articles propose more effective ways for deep learning and variational auto encoders to improve IoT and cloud based systems against ransomware threats.

Articles [49], [50], [51] discuss the contribution of deep learning to IoT security, dealing with a growing number of threats and privacy rights with respect to portable gateway devices. In these articles we see how the pattern which indicates compromise can be used to trace the ransomware inside the IoT network using the deep learn ing models. Article [52] then examines relationships between advanced persistent threats (APTs) and geopolitical factors which provide context for understanding how ransomware is utilized as an instrument in the wider use of cyber warfare. Articles [53, 54] introduce cryptographic schemes and remote attestation protocols that can increase the ability of detecting and mitigating ransomware by guaranteeing that data in cloud environment are reliable and trusted. Last, article [55] reviews machine and deep learning techniques for malware detection in drones that can be adapted to detect ransomware in the diverse set of new and emerging technologies.

4.1 Answer to Reseacrch Questions

With the extraction and the synthesis of data from the articles, it is evident that the integration of the AI, machine learning, blockchain, and cryptography is the key that leads to the advancement of ransomware detection and prevention approaches.

Adaptive and decentralized are afforded by these technologies, which are the right technologies to address the changing nature of ransonware threats, especially in domains such as IOT, cloud computing, and decentralized financials. The findings from these articles highlight the need for a holistic approach to cybersecurity that incorporates both traditional and modern techniques to combat ransomware effectively.

RQ1: What characteristics and dimensions are most commonly used to classify ransomware attacks?

RQ1 contains the articles that give an overall description of ransomware attacks and their various characteristics and dimensions for classification and how it has evolved to meet the technological needs. On a broader more multidisciplinary note, Article [26] focuses on the detection of ransomware detection that involves multiple layers of the cybersecurity mechanisms to improve classification strategies. This aligns with the growing need for such multidimensional analysis to account for the fact that ransomware attacks have become more numerous and target more traversed layers in the systems. Advanced applications of blockchain and IoT technology in the field of cybersecurity, as we see in articles [27] and [28], are helpful in identifying the ransomware embedded in such a decentralized and connected environment. The ransomware in these articles is also described in terms of how it relates to smart contracts and IoT devices, in which the ransomware behavior may not necessarily only impact individual devices, but the vulnerabilities in networked ecosystems also. Articles [29] and [30] present the new frameworks, such as federated learning, which can provide more privacy reserved and secure ransomware classification by decentralized data processing. This technology also adds another layer of classification of ransomware behavior in edge computing environment where data processing is done on an origin as opposed to centralised systems. Additionally, this research explores how to use machine learning and AI models to detect ransomware in articles [31], [38], and [44]. One technology classifies ransomware based on patterns in source data traffic, looking for abnormal behaviors, and classifying new strains of ransomware based on previously utilized attack vectors. In rapidly evolving environment, application of AI driven models in ransomware classification is critical as traditional methods do not work well. Additional details on these dimensions can be found in articles [45], [49] and [50], which explore how AI models and deep learning networks can be implemented for continuous learning and adaptation, necessary to keep pace with changes in ransomware tactics that are occurring at a rate of speed that is light years faster than any gunner, hacker, spy or warrior could do through a bulky battle tank. In the end, article [52] discusses the geopolitical links of advanced persistent threats (APTs) which provide critical contextual dimension to understand the global dimension of ransomware and its categorization in terms of a wider threat landscape.

RQ2: How do existing taxonomies contribute to the understanding, detection, and mitigation of ransomware threats?

RQ2's articles greatly advance our understanding of how the use of existing taxonomies enhance ransomware detection and mitigation. As one example, article [32] about reinforcement learning techniques can be added to existing ransomware detection frameworks in order to aid in decision making in changing dynamics. In fact, these techniques lead to faster learning in the taxonomy for new ransomware strains, enhancing the ability of taxonomy to detect and respond to attacks in real time. Related articles [33] and [34] deal with blockchain and AI based framework to improve ransomware detection through decentralized and transparent way. These frameworks also contribute to taxonomies by introducing mechanisms of tracking ransomware behavior over distributed networks as well as increasing the visibility of attack pathways. Strains of ransomware are not the only thing blockchain's immutable ledger and AI's pattern recognition capabilities can be used to develop taxonomies that can identify not only known strains of ransomware, but also new and evolving strains respectively. Articles [35] and [36] highlight the use of an integration of AI and blockchain in the improvement of industrial applications' and voting systems' cybersecurity. They're useful since these are the days when ransomware targets critical infrastructure, and existing taxonomies need to be expanded to cover new complexity in system security and data integrity. Similarly to this, articles [37], [40], and [41] also deal with trust management as well as cryptographic techniques that may be necessary to undermine ransomware through secure communications within the compromised system. As article [43] shows, the use of zero trust architecture is a security model of introduction that continuously verify that to prevent ransomware is spread within networks without control. This concept can help significantly improve taxonomies by developing the dynamic access verification techniques that mitigate ransomware risks. Three articles, [46], [47], and [48], introduce anomaly detection systems critical for ransomware detection, capable to recognize new attack patterns that cannot be described by conventional malware definitions. These systems introduce some layer of flexibility to existing taxonomies so that it can identify new ransomware strains also which leave no signatures for traditional signature based detection. Finally, article [55] discusses the use of machine and deep learning methods in malware detection; it points out the importance of AI in strengthening understanding of behaviour of ransomware as well as building taxonomies using learning models.

RQ3: What are the gaps and limitations in the current taxonomic frameworks for ransomware, and how can they be addressed? In this paper, RQ3 is addressed by identifying several gaps and limitations in current ransomware taxonomies, concerning the reviewed articles. For instance, articles [26], [27], [28], and [29] have shown that current taxonomies are not suitable to deal with the increasing intricacy of ransomware in decentralized and IoT environment. Vulnerabilities in these environments are being increasingly exploited, and therefore existing frameworks are inadequate to deal with the different attack vectors these environments introduce. The articles [27] and [29] discuss that while Blockchain and smart contract based attacks are undervalued in taxonomic models, they almost always ignore typical centralized attacks. This is further developed in articles [30] and [31], which cover the challenges of utilizing existing taxonomies in the cloud security and federated learning environment, where data can be decentralized and distributed across multiple nodes. As is the case with current frameworks, they were designed for more traditional, centralized forms of security. Existing taxonomies of ransomware are ill equipped to do so, as they lack the adaptation to these new paradigms. In addition, as the current taxonomies cannot keep up with the fast evolving technologies used by ransomware to mutate and adapt, articles [38], [39], and [44] note a danger here too: that the current taxonomies are ineffective against evolving AI and machine learning techniques used by ransomware. Ransomware would use these technologies to defeat normal detection systems and with such new, more sophisticated types of malware, existing taxonomies are inadequate to define the genre. Furthermore, article [45] brings to attention that although the deployment of blockchain based access control mechanisms is helpful in reducing the effect of ransomware, such a cryptographic security mechanism is not fully incorporated in existing taxonomic models that usually overlook the decentralized security aspect. As IoT and connected vehicle systems have complex and heterogeneous environments that require more specialized models of detection and mitigation, articles [48] and [50] also emphasize that ransomware classification for those systems presents additional challenges. Another area in which current frameworks 'do not work' are the use of remote attestation and encryption protocols, which are described in articles [53] and [54]. While these techniques provide strong security, the existing taxonomies do not cover new and modern disruptive risks, and so there is a need to adapt taxonomies with new and modern disruptive technologies. For these gaps to be addressed, there is need for building more adaptive, decentralized and AI driven taxonomies to detect and resolve ransomware live at scale over various attack vectors. With the advancement of technologies like blockchain, AI and an anomaly detection, taxonomies can evolve and handle the threats from the contemporary ransomware.

5. Discussion

Ransomware attacks are now one of the most pressing cybersecurity threats across the globe due to the increasing frequency, sophistication, and destructiveness of such attacks. This study conducts a systematic literature review (SLR), reviewing existing taxonomies, detection mechanisms and mitigation strategies of ransomware and shows strengths and gaps of existing taxonomic frameworks. This review is interpreted in the context of other cybersecurity scholarship and practice, and forward thinking for future research and application is proposed. In the first piece of research, I examined the characteristic that are most commonly used to categorize ransomware attacks. In the reviewed literature, ransomware schemes were mainly classified according to attack vectors, encryption methods, target systems, ransom payment mechanisms, and operational motives (e.g., financial or political) aimed at. In a recent observation, it is noticed that modern ransomware uses a manytangled attack vector such as phishing emails, exploit kits and Remote Display Protocol (RDP) vulnerabilities along with increasingly complex social engineering tactics. These vectors provide several taxonomies which classify ransomware based on how the attacker tries to infect and where he or she enters. Encryption methods are another crucial dimension upon which ransomware variants vary in terms of their use of cryptographic algorithms. Weak encryption is used in some variants, which allow easy decryption without payment, whereas strong encryption (like AES-256) is used in others that make data almost unreadable without the attacker's key.

In addition, taxonomies also include various targeted system types as dimension. While ransomware campaigns that once spewed free for all over will continue to operate with full force, attackers today are increasingly targeting critical infrastructure sectors such as healthcare, energy, and government services. In particular, these sectors have proved extremely prone to catastrophic service disruption. Finally, a classification criterion of the payment methods (for example, ransom payment) is also used for the purpose of anonymity, which is the desire of attackers. Additionally, motives for ransomware attacks — whether financial extortion, corporate espionage or politically motivated cyberterrorism — are important to taxonomic categorization. The study suggests that AI, machine learning, blockchain and federated learning could complement the traditional classification schemes by contributing towards augmenting them. These technologies enable real time anomaly detection, pattern recognition in complex data stream and decentralization of data, which are critical not only for running a current ransomware strains, but also for being real time and allied to rapidly mutate. The second research question is posed to determine to what extent established taxonomies aid in the comprehension, identification, and prevention from being a victim of a ransomware threat. Structured frameworks are found in literature as having an important role in identifying, analyzing and responding to Ransomware incidents. As taxonomies group attacks according to stable elements, they allow incident responders to quickly spot new threats, forecast what other attack paths an attacker could take and deploy adequate countermeasures.

Detection systems are greatly helped by taxonomies, which define behavioral patterns and IOCs commonly linked to different ransomware families. These taxo nomic frameworks are used as the tool to train anomaly detection techniques, machine learning algorithms and deep learning models. However, this study reviewed the articles that emphasized that AI driven taxonomies are productive in making the detection tools more flexible by helping them detect unknown and previously un known ransomware strains. Also, taxonomies have important roles in mitigation and recovery planning. By understanding ransomware variants delivery, how they spread and how much ransom they ask for, cybersecurity teams are able to prioritize asset prevention, work on stack defense approaches, and to run targeted education campaigns. Taxonomic insights used in Zero Trust architectures can aid in thwarting lateral movement and attacks aimed at privilege escalation by ransomware actors. Among their contributions to ransomware resilience, blockchain and federated learning frameworks were also mentioned. Through the technology of decentralizing data processing and making it transparent to transactions, these technologies solve the problem of single points of failure and enable collaborative threat intelligence shar ing. Such technological dimensions are already incorporated in existing taxonomies, thus allowing adaptation of the mitigation strategies for the distributed computing environments like cloud services, IoT networks, and smart city components. The third research question aimed to find the existing weaknesses in existing ransomware taxonomies and the possibility of improving them. There were several critical gaps identified from the systematic review.

First, most of the current taxonomies are static and are not dynamic enough to evolve rapidly as ransomware itself evolves rapidly. The polymorphic and metamor phic techniques used in modern ransomware attacks change the code structure to the point that signature detection becomes obsolete. For that reason, static taxonomies are not fit to house new attack methods and ransomware variants. Second, existing taxonomies do not integrate well decentralized computing environments including IoT, edge computing and clouds. All of these present unique vulnerabilities, as they are run without much processing power, across many domains with decentralized data storage, and much larger attack surface. In this study, reviewed articles noted that many ransomware targeting these infrastructures often exploits unlatched firmware, default configurations and weak authentication protocols. Thus taxonomies must evolve in that they need to include attributes specific to such contexts. Furthermore, current taxonomies do not adequately cover recent attack methods, such as Ran somware as a Service (RaaS) business models as well as double or triple extortion. Ransomware operators in these more sophisticated attacks do not only encrypt the data of victim systems, but also exfilate from the infected systems and then threaten to publish it if they are not paid the ransom. The multitude of threat aspects makes existing taxonomies often less than granular for classification or action. Fourth, the literature identifies a need for taxonomies that consider the geopolitical aspects of the ransomware campaigns. Ever more frequently, state sponsored ransomware groups are trying to leverage critical national infrastructure for the sake of economic and political power. According to the reviewed articles, geo political context should be factored in taxonomies including attribution challenges, legal implications and nation state strategies. Third, psychological and social impacts absent of a ransomware taxonomy are underexplored. In reviewing the literature, our classification dimensions are generally operational and financial with victim trauma, public distrust, and severe impact on the long term reputation of the affected organizations not considered. Ransomware incident should be comprehensive covered under broad taxonomies, which can incorporate socio psychological dimensions to get real comprehensive picture from all aspects. The last was articles that highlight limitations of legal and regulatory integration within a ransomware taxonomy. Ransomware response frameworks ignore the classes of attacks based on technical attributes, and pay little attention to compliance,.setDataBreach, and jurisdictional problems often featured in ransomware response. Adding legal dimensions to taxonomies would greatly increase their practical applicability in practice of incident management.

Since, these limitations are provided, the review proposes several future directions for creating more effective ransomware taxonomies. Above all, taxonomies have to evolve from static to dynamic frameworks, that are able to update continuously on the fly based on real time intelligence. The integration of machine learning models and AI can automate the process of taxonomy updates, allowing classification systems to classify novel ransomware corelations and their tactics in evolution. Second, future taxonomies should be multidimensional, including technical, operational, geopolitical, legal, psychological and economical attributes. Such holist frameworks will provide cybersecurity professionals with such comprehensive tools to assess, plan and respond to ransomware attacks effectively. Third, taxonomies must also include decentralized and distributed computing environments, particularly, IoT, cloud, and edge computing infrastructures. By including certain attributes about device type, connectivity protocols, or constraints of operation, more specific classification of ransomware aimed at these ecosystems could be possible. Third, frameworks must interweave evolving attack techniques like the ransomware that targets critical infrastructure and ransomware associated with RaaS (ransomware as a service) and double/triple extortion. These sophisticated campaigns have to be captured in taxonomies, and that means including operational workflow, affiliate structure and data leak site characteristics. The fifth is to have geopolitical awareness baked in ransomware taxonomies. Which includes constructing attacks campaigns on geopolitical tensions, state sponsored groups and also nation state cyber strategies. Attribution and incident response prioritization would also be enhanced if one understood the geopolitical motivations behind ransomware attacks, and international policy coordination would be supported. Sixth, taxonomies have to grasp for psychological and social effects,

understanding that ransomware attacks affect information systems and data, but also human welfare, corporate morale, and public confidence. The inclusion of qualitative dimensions in taxonomies would enhance risk assessment and incident recovery plan. Secondly, legal and regulatory attributes should be included in ransomware taxonomies for operationalizing compliance driven incident response. It includes assignment of attack types to applicable data protection laws and breach notification requirements (where required) and jurisdictional limits.

Finally, the implications of these findings for cybersecurity practice and policy are quite significant. The adoption of dynamic, AI enhanced taxonomies for practitioners could greatly increase the speed and accuracy of the cord detection, and by so, foster proactive incident prevention. The lack of a comprehensive classification framework makes cybersecurity teams to give a certain priority to the resources, tailor defenses and quickly engage in forensic investigations. The results show that policymakers need to create internationally harmonized classification standards for ransomware. These standards would help enable cross border information sharing and joint investigation as well as coordinated response strategies. Standardized taxonomies should be mandated to be integrated into critical infrastructure cyber security program to have consistent threat monitoring and reporting practices. Further, public-private partnerships should be created to joint development of the taxonomic framework utilizing the practical knowledge of industry stakeholders and strategic oversight of governmental bodies. Emerging threat intelligence could further contribute to additional collaborative research initiatives that refine taxonomies and could also evaluate the efficacy of their use in the real world. With ransomware getting more common in various educational institutions, they also have an important role in pushing ransomware research forward. To prepare future professionals to counter sophisticated cyber threats, taxonomic methodologies ought to be integrated into cybersecurity curricula. Additionally, more multidisciplinary research in the crossover area of computer science, psychology, law and international relations would further the work of developing comprehensive taxonomies.

6. Conclusion

Ransomware, one of the most destructive forms of cybercrime, has gone from being one of the most puny forms of malware a couple of years ago to one of the most pervasive and widespread items today with a disastrous capacity to stop liveli hoods, disable infrastructure and terrorize nations. This study has comprehensively conducted the systematic literature review to address existing taxonomies, detection methodologies, mitigation strategies and critical gaps in current research landscape. This investigation reveals that due to the success of classification and knowledge of ransomware threats, there is a dire need for dynamic, multidimensional, and interdisciplinary approaches to forecast, detect, and respond to the evolving threat. This research brings forth an important point regarding taxonomy in the domain of cybersecurity, especially for ransomware. Foundational for the classification of ransomware are taxonomic frameworks, which structure the ransomware classification based on different dimensions (attack vectors, encryption algorithm, techniques of data transmission for requesting ransom, targeted systems, the motives of running the operation, and geopolitical affiliations). Any detection or mitigation strategy will be highly effective or ineffective based on the underlying granularity and flexibility of its associated taxonomy. Without a good process to understand how these exploits map to a standard taxonomy, it is incredibly hard for cybersecurity pros, law enforcement, or policymakers to cooperate when these exploits arise. As affirmed by the reviewed literature, modern ransomware threats lie in the dynamic side, and other than being useful, traditional taxonomies are no longer enough to deal with the dynamic nature of ransomware threats. Now ransomware attacks have gone beyond isolated targeting of individual devices to highly coordinated attacks on private enterprises, as well as critical infrastructure and sectorial public bodies. These days attackers of course use multivector tactics, like phishing, remote desktop protocol vulnerabilities, exploit kits and sophisticated social engineering, in order to infiltrate systems. On top of that, there have been new operational complexities brought on by double and triple extortion: data encryption is done, and accompanied by threats to publish stolen data or disable services until more ransoms are paid.

One of the consistent observation across the studies reviewed is the increasing op erational scope of ransomware campaigns targeting even distributed and decentralized computing environment like Internet of Things (IoT) networks, cloud infrastructure and edge computing systems. Through such environments, the vulnerability is even greater in these environments for two primary reasons: Unsecured configurations, limited processing capabilities and vast attack surfaces. While organizations have emerged to assist with ransomware incident response and investigation, the taxonomies that exist to classify ransomware threats in these contexts have not adequately evolved to capture these emerging patterns. The frontiers these days of ransomware detection are in incorporating advanced technologies like artificial intelligence (AI), machine learning (ML), federated learning etc. Rapid anomaly detection, pattern recognition and adaptive classification of the novel ransomware strain can be performed using their AIs and ML models, outperforming traditional signature based detection system. Data privacy and security is improved by decentralizing training of detection models in federated learning, eliminating the risk of access to centralized data repositories.

The ability of Blockchain to have physical, decentralized ledger of system activity provides immutable, transparent records of system activity which are perfect for incident investigation and threat attribution. While there have been big leaps in ransomware taxonomy since 2011, several key points are still missing. The existing frameworks, however, are typically static, reactive and very focused on technical attributes. Usually, ransomware attacks are missed because it fails to grasp broad op erational, geopolitical, psychological and legal outlooks that surround these malicious activities. The literature shows that there is a growing trend of including geopolitics into ransomware crimes, so that state sponsored actors engage in ransomware as a form of economic sabotage and political coercion. These strategic dimensions need to be accommodated in the taxonomies to better understand the motives and patterns of the attacker.

The third area of research not yet explored is socio-psychological impact of ransomware attacks. Despite these emphasis on financial and operational consequences, the psychological trauma inflicted on the victims, organizational leaders, employees and customers are seldom taken into consideration. The long term effects from ransomware attacks have been fear, the risk of becoming less safe or worry about getting raided, damage to reputation and loss of public trust and the long term effect on a community. Including these human-centric aspects into taxonomic frameworks will be a step towards a qualitative evaluation of the scope of societal impact to ransomware. Additionally, a dearth of integration between ransomware taxonomist and legal and regulatory frameworks is found. As data protection laws and breach notification requirements grow in importance and jurisdictions become increasingly challenging, it is increasingly important for taxonomies to closely align with legal and compliance requirements. The mapping of ransomware attack types to applicable legal obligations would improve coordination of incident response, standardization of reporting and compliance. Based on these findings, this study offers dynamic, multidimensional ransomware taxonomies that reflect technical, operational, geopolitical, psychological and legal attributes. Such frameworks need to be updated constantly as per real time threat intelligence to allow the quick change in ransomware variants and attack methodologies. Automating this updatesof taxonomies can be done by AI driven classification models which update taxonomies and keep it up to date with the evolving threat landscape. In addition, taxonomies have to be customized to deal with the problems by the decentralized and distributed computing environments. It pertains to identifying ransomware in terms of device type, connectivity protocols, constraints in terms of operations, as well as system interdependencies from the perspective of IoT, cloud, and edge computing networks. Through implementation of attributes related to these environments, taxonomies may be more helpful for classifying and even offer guidance on defensive strategies.

Taxonomic frameworks should explicitly deal with integration of new ransomware tactics, including Ransomware as a service (RaaS) and double/triple extortion. It would describe operational workflows, affiliate structure and ransom negotiation prac tices that would help in understanding attacker methodologies and better developing of the proactive defence measures. Like, geopolitical analysis can be similarly mapped into taxonomies to aid attribution, strategic threat modeling, formulation of policies and others. Ransomware attacks don't cause people to get cash and end; they are a systematic and psychological attack, and their impact on society and psychology is also equally important. Stress levels, erosion to public trust, and organizational morale represent key qualitative dimensions out of which to assess the full repercussions of an incident of ransomware. Such incorporations would enable taxonomies to be used in comprehensive risk assessments, recovery planning and victim support activities. The indetermination is common to all forms is caused by its current position as a new, rapid developing phenomenon; ransomware taxonomies should include legal and regulatory considerations as well. The data breach incidents will be classified into the legal implications, obligations, and jurisdictional constraints affecting different attacks and such a classification will increase compliance management and incident reporting. This would mean that it is aligned so that cybersecurity practitioners and legal teams would work together within a single framework during a ransomware response. The result of this research has implication both for cybersecurity practice, policy making, and academic inquiry. Dynamic, AI-enhanced taxonomies would enable practitioners to speed up, make more accurate and comprehensive reference for the detection and response of ransomware. Incident responders could classify and triage threats better, extend asset protection to some extent, and target countermeasures most efficiently.

The study shows for policymakers that international harmonized ransomware classification standards are needed. These standards would help with cross border information sharing, joint investigatory activity and joint crafted response plans. Regulatory bodies should mandate that the critical infrastructure cybersecurity pro grams use standardized taxonomies, so that threat monitoring and reporting are on consistent protocols. To build and maintain ransomware taxonomies, public private partnerships need to be strengthened to help collectively develop and maintain them. Government agencies possess strategic oversight and regulatory guidance and industry stakeholders have valuable operational insights. Such cooperative research initiatives would maintain current, practical and reflective taxonomies of the real world threat landscapes. Ransomware research and taxonomy development also has an important role in academic institutions. Attaching taxonomic methodologies to cybersecurity curricula will be enabling to the next generation of professionals in providing an alytical skills able of classifying and handling sophisticated cyber threats. Other research that bridged computer science, psychology, international relations and law would further enrich taxonomic frameworks and make them more and more relevant and applicable. This must also be done

as ransomware evolves: That is to say, with the methods used to classify, detect and mitigate ransomware evolving accordingly. The dynamic nature of cybercrime necessitates continuous innovation, international collaboration, and a holistic understanding of its multifaceted impacts. Through the development of comprehensive, adaptable, and multidimensional taxonomies, the cybersecurity community can better navigate the complex ransomware landscape, safeguarding critical infrastructure, organizational assets, and public trust. In con clusion, this systematic literature review has not only highlighted the importance of ransomware taxonomies but also illuminated their current limitations and potential for enhancement. By embracing emerging technologies, integrating diverse disci plinary perspectives, and prioritizing dynamic adaptability, the global cybersecurity community can forge stronger, more resilient defenses against the persistent and growing menace of ransomware.

7. Future Directions

In the ever growing ransomware threat landscape, having adequate robust, adap tive and multidimensional countermeasures, needs to be explored and established at the synergistic intersection of cybersecurity researchers, practitioners and policy makers. This study also presented the systematic literature review highlighting the already existing strength and the limitation of the current ransomware taxonomies as well as the dynamism of the threat and the need for developing new approaches to counter its threat. Based on these findings, several future research direction, practical implementations and local and policy recommendations are proposed for enhancing ransomware detection, classification and prevention mechanism. Dynamic ransomware taxonomies that perpetually evolve in the face of a continually changing threat are one of the most important future directions. Although static taxonomies are an excellent starting point, they miss the mark regarding the pace at which modern ransomware campaigns evolve and adapt. Future taxonomies are designed as learning systems that grow and adapt to new types of threat intelligence, new ways to launch attacks, and new ransomware strains. In this domain, artificial intelligence (AI) and machine learning (ML) models hold a great promise. These technologies can be applied towards automating the classification process, detecting the new ransomware patterns and timeLine updating. Adaptivity of these frameworks can be further enhanced by reinforcement learning techniques and deep learning models to achieve proactive, rather than reactionary, cybersecurity strategies. Future research should involve the use of AI-based taxonomies in feeding into Security Information and Event Management (SIEM) systems and Intrusion Detection Systems (IDS) to improve Threat detection and Threat classification.

In the context of recent developments in ransomware, which is increasingly targeting decentralised environments, such as the Internet of Things (IoT) network, cloud infrastructure and edge computing systems, future taxonomies need to take into consideration specific vulnerabilities as well as operational constraints in particular situations. Future research should aim to classify ransomware with respect to device type, connectivity and communication protocols and the interdependencies of systems within these environments and within respective operational contexts. Blockchain technology may also be beneficial in its use to increase security and transparency of these distributed systems. Future research should investigate how blockchain based ledgers can record and certify system activities; detect changes to system activities that do not adhere to a specific publish or perish policy or policy that prohibits unlawful change; and attribute ransomware attacks. Finally, research standing to be conducted that integrates decentralized identifiers (DIDs) and zero-knowledge proofs (ZKPs) into ransomware taxonomies are the combination of privacy preserving authentication and verification mechanisms. Ransomware operations these days are extremely innovative with tactics such as Ransomware as a Service (RaaS), double and triple extortion and affiliate based campaigns. These new operational workflows, affiliate structures and ransom negotiation practices imply that future taxonomies should be designed to classify ransomware on agreed taxonomy, based upon what it all means. Better understanding of attacker incentives, affiliate recruitment strate gies and revenue distribution mechanisms would be provided if one enhanced their detailed categorization of these business models. Other areas of financial infras tructure that should be explored further include ransomware operations, including cryptocurrency laundering techniques, dark web marketplaces, and platforms for ransom payment negotiation. This would make it possible to develop taxonomies to classifying ransomware attacks while mapping the broader ransomware economy and ecosystem.

These ransomware attacks are further Queenslanding as they intersect with geopolitical tensions, particularly as state-sponsored actors turn the ransomware they've likely been using for decades to their benefit and abuse ransomware for economic disruption, espionage, and political coercion. Geopolitical dimension should be included in future taxonomies for ransomware campaigns, by mapping their campaigns to geopolitical events, provenance of nation states and their strategic objectives. In this area of research we could explore the identification of markers of state sponsorship by observing places where operational patterns meet or overlap, base and infrastructure overlaps, and behaviors of C2 of known APT groups. A better understanding of the ransomware taxonomy requires the development of attribution models that include geopolitical analysis as a layer of integration with technical indicators, and this would dramatically improve the accuracy and usefulness of the ransomware taxonomy. There have a been existed taxonomies that concentrate on more technical, financial and operational consequences of ransomware attacks, while overlooking its psychological and social impacts. Future taxonomies of cyber terrorism, especially ransomware, should include non quantitative metrics that evaluate the human centric effect of ransomware incidents, such as stress level, public trust erosion, employee morale, and community resilience. In these research initiatives, psychological,

sociological, and public health officials might join interdisciplinary collaboration to standardize the assessment tools for measuring emotional and social costs of the ransomware attacks. This would support a focused victim support service and community resilience programs framework incorporating a more holistic risk assessment.

Future ransomware taxonomies will need to reflect legal and compliance frame works in light of increasing significance of data protection regulations and breach notification mandates. The type of a ransomware attack should be mapped accord ingly to the appropriate legal obligations such as GDPR, CCPA, HIPAA, etc., and national cybersecurity laws. Ransomware attacks are to be classified in the taxonomies by their legal implications, data breach notification requirements, jurisdictional con straints and regulatory reporting standards. It would also enable coordination during incidents, facilitate law enforcement proceedings against ransomware actors, as well as enable regulatory compliance. Furthermore, there is an opportunity to research on building international ransomware classification standards to be able to consistently report risk, collaborate on investigations and coordinate cross border law enforcement. These standards could be established and sustained by public private partnerships and international treaties. Ransomware attacks require multidisciplinary approach that involves computer science, psychology, International relations, law, economics and public policy. Future research should focus on interdisciplinary collaboration to create an integrative taxonomy that would encompass these multifaceted forms of ransomware threats. There are joint research initiatives, cross sector cybersecu rity consortia, and academic industry partnerships that can support the exchange of knowledge and best practices in regard to ransomware taxonomies that are not only current, practical, and relevant to reality but can also evolve. Knowledge sharing and capacity building in this domain can also be facilitated by multisource multidisciplinary conferences, workshops, training programs, etc.

For ransomware, it is important to quickly share threat intelligence. Future research can investigate the creation of standardized ransomware taxonomy standards and threat intelligence sharing rules to enable effortless communication of information between organizations, Governments and global partners. By integrating blockchain based threat intelligence platforms, the security, integrity, immutability of shared data can improve through integrated data, thereby reducing the risk of tampering and misinformation. The future taxonomies should be defined to accommodate the automated exchange of threat intelligence based on open standards such as STIX and TAXII. Signature based detection methods are becoming less effective against this modern breed of ransomware mostly due to the fact that it uses polymorphic and metamorphic techniques. Future research should explore the development of anomaly detection systems and behavioral analysis models that will be able to distinguish ransomware based their irregularities with respect to normal system behaviors and users' activities. Ransomware detection has been made possible using machine learning and deep learning models such as recurrent neural network (RNN) and convolutional neural networks (CNN), which are capable of detecting discreet, but yet important, anomalies related to the activity of ransomware. Future taxonomies should include behavioral attributes such as file access patterns, process execution sequences, network traffic anomalies, and encryption behaviors in their integration to achieve greater detection accuracy.

Future studies should focus on the development of proactive and predictive cybersecurity mechanisms rather than the reactive defense strategies. Predictive analytics models that are able to predict ransomware attack probability given his torical data, threat intelligence, and environmental factors are also included in this. Predictive indicators should be included into future taxonomies as they would enable organisations to predict the risk exposure, as well as identify the assets that need to be prioritised for protection, and carry out the preventive countermeasures. As organizational resilience, contrary to ransomware taxonomies, depends on proactive defence mechanisms, such as decoy systems (honeypots), deception technologies and AI driven vulnerability management, these should be integrated into ransomware taxonomies. To respond to the ransomware threat, an educated, trained, skilled and knowledgeable cyber workforce is needed. Cybersecurity education and training programs could incorporate methodologies of ransomware taxonomy in the future research to enhance its impact on future learners and students. This would give the future professionals what analytical skills required for ransomware threat classification, detection, and response. With the first topic, academic institutions should be working with industry partners to develop curriculum modules, simulation exercises and certification programmes around ransomware taxonomy development and application. Also, diversity and inclusion in workforce development initiatives should be prioritized so that a wide variety of perspectives and expertise are being brought to ransomware taxonomy research and practice.

With ransomware attacks rising in frequency, insurance has become the demand in the field of cybersecurity. And future research should explore the economic consequences of ransomware incidents and consider just what insurance could mean to risk management strategies. Economic impact metrics should be part of taxonomies - ransom payment amounts, operational downtime costs recovery costs, as well as reputational damage. Research also needs to focus on development of standardized models of insurance risk, and underwriting guidelines that are based on attributes of ransomware classification. Specifically, future ransomware taxonomies should include future development of victim support and recovery frameworks. Ransomware incidents should be classified based on such factors as data criticality, recovery feasibility, psychological impact and legal obligations, and these frameworks should be applicable for classifying ransomware incidents. There should be further research

into what constitutes best victim support service practice, such as crisis counseling, legal assistance, public relations management, and technical recovery service. Recovery and support attributes that help toward taxonomies would allow for coordinated, victim centered strategies of incident response.

Ransomware research and defense that evolves in the dynamic, multidimensional, and interdisciplinary taxonomies melded with the rapid changes in threat landscapes is the future of ransomware research and defense. Future taxonomies can do more than that by combining advanced technologies, geopolitical analysis, the psychological metrics, legal frameworks and economic impact assessments to build a framework that can detect, classify and mitigate the ransomware threat. Ransomware taxonomy development will require collaboration research initiatives, public and private part nerships as well as international cooperation. In an increasingly digital world global capacity building, continuous innovation and knowledge sharing can help the global community to protect critical infrastructure, organizational assets, as well public trust against ransomware.

Funding: This research received no external funding.
Conflicts of Interest: The authors declare no conflict of interest.
Publisher's Note: All claims expressed in this article are solely those of the authors and do not necessarily represent those of their affiliated organizations, or those of the publisher, the editors and the reviewers.

References

[1] Aboaoja, F. A., Zainal, A., Ghaleb, F. A., Al-Rimy, B. A. S., Eisa, T. A. E., and Elnour, A. A. H. (2022). Malware detection issues, challenges, and future directions: A survey. *Applied Sciences*, 12(17):8482.
[2] 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.
[3] Benmalek, M. (2024). Ransomware on cyber-physical systems: Taxonomies, case studies, security gaps, and open challenges. *Internet of Things and Cyber-Physical Systems*, 4:186–202.
[4] Gorment, N. Z., Selamat, A., Cheng, L. K., and Krejcar, O. (2023). Machine learning algorithm for malware detection: Taxonomy, current challenges, and future directions. *IEEE Access*, 11:141045–141089.
[5] 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.
[6] Krishna, R. R., Priyadarshini, A., Jha, A. V., Appasani, B., Srinivasulu, A., and Bizon, N. (2021). State-of-the-art review on iot threats and attacks: Taxonomy, challenges and solutions. *Sustainability*, 13(16):9463.
[7] Ladisa, P., Plate, H., Martinez, M., and Barais, O. (2022). Taxonomy of attacks on open-source software supply chains. *arXiv preprint arXiv:2204.04008*.
[8] Moussaileb, R., Cuppens, N., Lanet, J.-L., and Bouder, H. L. (2021). A survey on windows-based ransomware taxonomy and detection mechanisms. *ACM Computing Surveys (CSUR)*, 54(6):1–36.
[9] Oz, H., Aris, A., Levi, A., and Uluagac, A. S. (2022). A survey on ransomware: Evolution, taxonomy, and defense solutions. *ACM Computing Surveys (CSUR)*, 54(11s):1–37.
[10] Park, J. H., Singh, S. K., Salim, M. M., Azzaoui, A. E., and Park, J. H. (2022). Ransomware-based cyber attacks: A comprehensive survey. *Journal of Internet Technology*, 23(7):1557–1564.
[11] Plachkinova, M. (2023). A taxonomy for risk assessment of cyberattacks on critical infrastructure (traci). *Communications of the association for information systems*, 52(1):1.
[12] Plachkinova, M. and Vo, A. (2022). A taxonomy of cyberattacks against critical infrastructure. *Journal of Cybersecurity Education, Research and Practice*, 2021(2). Rabitti, G., Khorrami Chokami, A., Coyle, P., and Cohen, R. D. (2025). A taxonomy of cyber risk taxonomies. *Risk Analysis*, 45(2):376–386.
[13] Razaulla, S., Fachkha, C., Markarian, C., Gawanmeh, A., Mansoor, W., Fung, B. C., and Assi, C. (2023). The age of ransomware: A survey on the evolution, taxonomy, and research directions. *IEEE Access*, 11:40698–40723.
[14] Reshmi, T. (2021). Information security breaches due to ransomware attacks-a systematic literature review. *International Journal of Information Management Data Insights*, 1(2):100013.
[15] Roseline, S. A. and Geetha, S. (2021). A comprehensive survey of tools and tech niques mitigating computer and mobile malware attacks. *Computers & Electrical Engineering*, 92:107143.
[16] Urooj, U., Al-Rimy, B. A. S., Zainal, A., Ghaleb, F. A., and Rassam, M. A. (2021). Ransomware detection using the dynamic analysis and machine learning: A survey and research directions. *Applied Sciences*, 12(1):172.
[17] Victor, P., Lashkari, A. H., Lu, R., Sasi, T., Xiong, P., and Iqbal, S. (2023). Iot malware: An attribute-based taxonomy, detection mechanisms and challenges. *Peer-to-peer Networking and Applications*, 16(3):1380–1431.
[18] Xenofontos, C., Zografopoulos, I., Konstantinou, C., Jolfaei, A., Khan, M. K., and Choo, K.-K. R. (2021). Consumer, commercial, and industrial iot (in) security: Attack taxonomy and case studies. *IEEE Internet of Things Journal*, 9(1):199–221. appendix inputAppendices/AppendixA inputAppendices/AppendixB