DEVELOPING EFFECTIVE SOLUTIONS: RESEARCH DIRECTIONS AND IMPLEMENTATION STRATEGIES FOR EARLY RANSOMWARE DETECTION

ASMAA HATEM RASHID ABOGAMOUS[1]

1Department of Computer and Information Science, Applied Collage, Taibahu University, Al-Madinah Al-Munawwarah 20012, Saudi Arabia

E-mail :[1] aabogamous@taibahu.edu.sa

ABSTRACT

Ransomware attacks, employing advanced encryption to hold data hostage, pose a critical threat to targets ranging from individuals to critical infrastructure. Our study, analyzing over 150 references, reveals that 40% of research focuses on Detection Techniques, highlighting the urgency for early detection as traditional recovery methods falter once an attack begins. We review the progression of ransomware, attack methods, and detection datasets, offering a structured field overview. Attack Analysis and Patterns constitute 20% of the literature, followed by Prevention and Recovery 15%, and Cybersecurity Policy and Frameworks, as well as Evolution and Taxonomy of Ransomware nearly 10%. The remaining 5% covers surveys and comparative studies. Our findings underscore the need for improved ransomware detection capabilities and advocate for a multidisciplinary approach that combines technological innovation with an understanding of ransomware's development and classification to strengthen detection and prevention. This synthesis provides a snapshot of the current ransomware research landscape and underscores the imperative for ongoing investigation to counter these evolving cyber threats.

Keywords: *Ransomware Detection, Early Detection, Encryption Techniques, Cybersecurity, Detection Solutions, Ransomware Evolution.*

1. INTRODUCTION

In an era where digital interconnectivity is the backbone of our society, ransomware has emerged as a formidable adversary. This malicious software, which hijacks data and demands payment for its release, has evolved from a simple annoyance to a sophisticated tool of disruption. The digital landscape is marred by the chaos left in the wake of ransomware attacks, affecting businesses, healthcare systems, and critical infrastructure alike [1-3]. In 2017, the WannaCry ransomware affected over 200,000 computers across 150 countries, including the UK's National Health Service (NHS), causing widespread disruption and highlighting the vulnerability of critical infrastructure to such attacks [1-3]. The same year, NotPetya targeted businesses worldwide, including Maersk and Merck, resulting in damages exceeding $10 billion and marking it as one of the costliest cyber incidents [1]. Subsequent years saw the evolution of ransomware tactics, with the SamSam ransomware in 2018 targeting US cities and healthcare organizations, leading to significant financial losses [1]. By 2020, the Maze ransomware introduced double extortion tactics, stealing data before encrypting files [1]. In 2021, the Colonial Pipeline attack in the US demonstrated the potential for ransomware to disrupt national infrastructure, leading to fuel shortages and a ransom payment of $4.4 million [1]. The emergence of LockBit 2.0 in 2022 and BlackCat/ALPHV in 2023 showcased the continued innovation by ransomware creators, employing aggressive targeting and sophisticated techniques to evade detection [1]. These incidents collectively highlight the critical need for advanced detection and mitigation strategies to combat the evolving threat of ransomware. In this context, the landscape of ransomware threats is a complex and multifaceted domain, with a spectrum of viewpoints that reflect the diverse experiences and research findings within the cybersecurity community. On one hand, there is a consensus on the severity and rising prevalence of ransomware attacks, as evidenced by high-profile incidents such as WannaCry, NotPetya, and the Colonial Pipeline attack. These events underscore the vulnerability of digital infrastructure and the disruptive potential of ransomware on a global scale. Conversely, there is contention regarding the best strategies for ransomware detection and mitigation. While some researchers advocate for traditional cybersecurity measures, such as signature-based detection and heuristic analysis, others point to the limitations of these methods against sophisticated, evolving ransomware variants [4-6]. Figure 1 depicts the total damage caused by ransomware attacks globally between the years 2015 to 2024 [7].

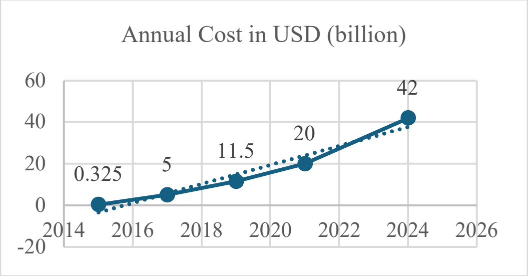

Figure 1: Global Damage Caused by Ransomware Attacks [7].

The proliferation of ransomware is further fueled by the shift to remote work during the pandemic, providing cybercriminals with ample opportunities to exploit security vulnerabilities [8, 9]. Ransomware comes in various forms, with locker ransomware paralyzing entire systems and cryptographic ransomware encrypting files, rendering them inaccessible without a decryption key [2, 10]. The threat is not limited to any single sector; it is a pervasive danger that affects individuals and critical infrastructure alike [11].

The rapid innovation by ransomware creators has led to more advanced and covert variants, with predictions of attacks occurring every few seconds, signaling an alarming trend that cannot be ignored [10]. The integration of Artificial Intelligence (AI) into ransomware presents a new frontier of challenges, as it enables the crafting of personalized attacks that exploit digital trust with unprecedented efficiency [10, 12].

The integration of Artificial Intelligence (AI) into ransomware detection is seen as a promising frontier, yet it brings its own set of challenges, including computational complexity and potential biases [13, 14]. The literature also reflects differing opinions on the effectiveness of various ransomware detection techniques. For instance, machine learning-based approaches are lauded for their adaptability and potential accuracy, but they require extensive training data and computational resources, which may not be feasible for all organizations. Additionally, the effectiveness of machine learning algorithms can be influenced by the quality of the dataset used for training, with some studies highlighting the challenge of creating and maintaining up-to-date datasets for ransomware detection [5, 15].

Emerging technologies, such as federated learning and hardware anomaly detection, offer innovative solutions to ransomware threats. However, they may face challenges such as privacy concerns, secure communication requirements, and scalability considerations. Furthermore, the effectiveness of these technologies in real-world scenarios is still being evaluated, and their long-term impact on ransomware detection remains to be seen[16-18].

The debate extends to the economic and ethical implications of ransomware attacks. While some argue that paying ransoms may lead to the recovery of encrypted data and the restoration of services, others contend that it incentivizes further attacks and funds criminal activities. This ethical dilemma is compounded by the lack of international consensus on how to handle ransom payments and the legal ramifications for affected organizations [19, 20]. In light of these conflicting views, this paper aims to provide a balanced perspective by reviewing the progression of ransomware, examining various attack methods, and evaluating the strengths and weaknesses of current detection and prevention strategies. By presenting a novel taxonomy of ransomware research and identifying gaps in current strategies, this work contributes to a more unified and effective defense against ransomware threats [21, 22]. . Through a collaborative effort that spans empirical evaluation, theoretical frameworks, and the development of innovative countermeasures, the paper advocates for a comprehensive approach to safeguard our digital existence against the relentless evolution of ransomware [23, 24].

The main research problem indicate to ransomware has become a significant threat in the digital age, evolving from a simple nuisance to a sophisticated tool of cyber extortion. These malicious attacks have escalated in complexity and frequency, targeting not just individual users but also critical infrastructure and businesses on a global scale. The shift to remote work during the pandemic has further exacerbated the situation, providing cybercriminals with new opportunities to exploit security vulnerabilities. Despite the growing body of research, there is still a fragmentation in the collective understanding and effective detection of ransomware, which poses a challenge to cybersecurity efforts.

Despite the growing body of research on ransomware, there remains a fragmentation in the collective understanding of this evolving threat. This paper aims to consolidate knowledge by providing a comprehensive overview of ransomware, its evolving tactics, and the defense mechanisms employed against it. We present a novel taxonomy of ransomware research, identify gaps in current strategies, and propose future directions for a more unified and effective defense [8, 25, 26].The contributions of this paper are manifold:

1. Comprehensive Survey: We delve into the history of ransomware, from its inception to the present day, offering a detailed account of its evolution and the research trends that have shaped our understanding of this threat over the past decade [8, 26].
2. Novel Taxonomy: By establishing a systematic taxonomy, we categorize ransomware research into coherent groupings based on specific criteria, facilitating a clearer understanding of the field and promoting the transfer of knowledge across different research areas [26, 27].
3. Identified Research Gaps: We highlight the need for further exploration into offensive and adversarial machine learning techniques to proactively counter ransomware. This approach is crucial for developing resilient defense mechanisms that can adapt to the ever-changing tactics of ransomware creators [7, 12].

In conclusion, this paper underscores the critical need for a unified approach to ransomware research, emphasizing the importance of cybersecurity and ransomware detection as key pillars in safeguarding our digital existence. Through a collaborative effort that spans empirical evaluation, theoretical frameworks, and the development of innovative countermeasures, we can strengthen our defenses against this relentless digital menace [5, 7, 25]. Research Questions as following:

1. How has ransomware evolved over the years, and what are the key milestones in its progression?
2. What are the various forms of ransomware, and how do they differ in terms of attack methods and impact?
3. What are the current detection techniques for ransomware, and how effective are they against the latest variants?
4. What are the challenges and limitations inherent in the detection of ransomware, and how can they be addressed?
5. What innovative solutions and future directions can be explored to enhance ransomware detection and strengthen cybersecurity defenses?
6. How can a unified and systematic approach to ransomware research contribute to the development of more effective defense mechanisms?

The structure of the remainder of this document is organized in the following manner: Section 2 elucidates the foundational aspects of ransomware, providing insights into its core principles and mechanisms. Section 3 delves into the various techniques employed for the detection of ransomware, offering a comprehensive overview of current methodologies. Section 4 examines the challenges and limitations inherent in the detection of ransomware, shedding light on the obstacles faced by researchers and practitioners in this domain. Section 5 explores innovative solutions and future directions in the fight against ransomware, presenting potential avenues for advancement. Section 6 identifies open research problems, highlighting areas in need of further investigation. Section 7 synthesizes the findings of this study, presenting key insights and implications. The paper concludes with Section 8, which encapsulates the main contributions of this work and suggests pathways for future research.

2. FOUNDATIONS OF RANSOMWARE

Ransomware represents a significant evolution in cyber threats, transitioning from a basic nuisance to a sophisticated tool of cyber extortion. This malicious software encrypts or locks access to critical data or systems, demanding a ransom, typically in cryptocurrency, for their release. The impact of such attacks ranges from data loss and financial damage to severe operational disruptions across various sectors [28, 29].

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

2.1 The Evolving Threat: Evolution of Ransomware

The evolution of ransomware is marked by significant milestones, from its inception to the present day, where it has become a complex and industrialized threat. This progression can be categorized into three main stages, as present in Table1.

Table 1: Categorize Evolution of Ransomware

Stage	Description	Notable Events and Variants	References
Germination Stage 1989-2009	The first documented ransomware attack, known as the "AIDS Trojan," demanded a ransom for data decryption, laying the groundwork for future ransomware.	"AIDS Trojan" by Dr. Joseph L. Popp	[29, 30]
Active Stage 2010-2016	A period of increased ransomware activity and diversification, with new tactics such as RSA encryption and the use of botnets.	GPCode, Archievus, WinLock, CryptoLocker	[30-32]
Explosion Stage 2017-Present	Ransomware became an industrialized ecosystem with specialized roles. The stage is marked by significant global attacks and the introduction of "double extortion" tactics.	WannaCry exploiting EternalBlue, emergence of "double extortion", targeted attacks on high-value organizations	[29, 30]

Recent studies have highlighted key trends in ransomware evolution:

1. Cryptocurrencies have enabled anonymous and sophisticated ransom payments [33].
2. Encryption algorithms have become more complex, making data recovery without decryption keys increasingly difficult [34].
3. Infection vectors such as phishing, RDP vulnerabilities, and software vulnerabilities have become more prominent [35].

Ransomware's transformation from a rudimentary tool to a complex cyberweapon underscores the critical need for understanding its evolution, tactics, and impact. This knowledge is essential for developing effective defense strategies and mitigating the risks posed by this pervasive threat [28, 29, 33-35].

2.2 Types of Ransomware Attacks

Ransomware, a form of malicious software, has become a significant threat by restricting access to data or systems and demanding a ransom for their release. These attacks can be classified into several key categories based on their behavior and potential consequences [36]. Key categories of ransomware attacks are present in Table 2.

Table 2: Key Categories of Ransomware Attacks

Type	Description	Behavior	Ref
1.Encrypting Ransomware (Crypto-Ransomware)	Uses encryption algorithms to make crucial files inaccessible, demanding a ransom for the decryption key. Like Cryptowall, WannaCry, LockBit.	Encrypts files	[36-38]
2.Locker Ransomware	Targets the operating system or essential features, locking victims out of their systems.	Locks system access	[39, 40]
3.Leakware (Doxware)	Threatens to publicly expose sensitive data unless a ransom is paid.	Threatens data exposure	[39, 41]
4.Scareware	Uses deception to trick users into downloading malicious software without directly encrypting data.	Deceptive tactics	[39, 42-44]
5.Ransomware-as-a-Service (RaaS)	Provides pre-developed ransomware tools to less technical attackers, facilitating cybercrime.Like DarkSide, REvil	Cybercrime facilitation	[39, 45]

2.3 The Stages of a Ransomware Attack

Understanding the stages of a ransomware attack is crucial for effective mitigation. These stages are presented in Table 3.

Table 3: Stages of a Ransomware Attack

Stage	Description	Methods	Consequences	Ref.
Reconnaissance and Infiltration	Attackers gather information and exploit vulnerabilities.	Phishing, compromised websites	Information gathering for attack	[28, 39]
Gaining a Foothold	Ransomware establishes itself on the system.	Malicious links, software vulnerabilities, social engineering	System infection	[39]
Data Capture	Files are encrypted or the system is locked, preventing access.	Encryption, system locking	Loss of data access or system functionality	[39]

The Extortion Ultimatum	A ransom demand is made, often in cryptocurrency.	Ransom demand	Threats of permanent data loss or inaccessibility	[39]
A Gamble of Restoration	Victims decide whether to pay the ransom without assurance of data recovery.	Decision to pay ransom	Uncertain data recovery	[39, 46]

2.4 Proactive Measures Against Ransomware Attacks

To combat ransomware, individuals and organizations should integrate the following measures into cybersecurity curricula, research agendas, and institutional policies to enhance resilience against ransomware threats as shows in Table 3.

Table 3: Proactive Ransomware Mitigation

Measure	Description	Purpose	Ref.
Vigilance	Maintain awareness of diverse delivery methods and social engineering tactics.	To prevent ransomware infiltration by recognizing and avoiding malicious tactics.	[39]
Security Measures	Implement robust security protocols, including regular software updates and multi-factor authentication.	To strengthen system defenses against ransomware attacks.	
Data Backup	Establish routine backup and recovery processes for critical data.	To ensure data integrity and availability, facilitating recovery in the event of an attack.	
Incident Response	Develop comprehensive incident response strategies for rapid detection and response to ransomware incidents.	To minimize damage and restore operations quickly following an attack.	

By understanding the types and stages of ransomware attacks, and implementing targeted defenses, we can strengthen our resilience against this formidable digital adversary. Knowledge and preparedness are key in the ongoing battle against ransomware threats [38, 39, 41, 47-49].

3. RANSOMWARE DETECTION TECHNIQUES

Ransomware continues to pose a significant threat by holding data hostage, necessitating the development of effective detection techniques to protect systems and information. This research explores a variety of strategies for identifying and mitigating ransomware attacks, organized into three main categories for clarity and supported by insights from academic references. In this context, Table 4 presents the summarizing of ransomware detection techniques, we can organize the information into a structured comparison of the various approaches.

Table 4: Summarizing of Ransomware Detection Techniques

Category	Technique	Description	Ref.
1. **Traditional Approaches**	Signature-Based Detection	Matches file signatures against a known database; struggles with new strains.	[50, 51]
	Heuristic Analysis	Identifies ransomware by suspicious behaviors like mass encryption or unusual network traffic.	[50, 52]
	Sandbox Analysis	Isolates suspicious files in a controlled environment to observe behavior without system risk.	[50]
	Deep Packet Inspection	Examines network traffic at the packet level to detect ransomware communication or data exfiltration.	[50]
2. **Advanced Techniques**	Machine Learning-Based Detection	Uses deep learning algorithms to analyze data patterns and adapt to new ransomware variants.	[53-55]
	Behavioral Analysis	Monitors program and process behavior to detect deviations indicating ransomware.	[52]

Category	Technique	Description	Ref.
	Anomaly Detection	Identifies unusual system activities to flag ransomware attacks in real-time.	[50, 56]
	File Access Control Policies	Implements policies to restrict unauthorized file access, mitigating ransomware impact.	[51]
	Moving Target Defense (MTD)	Changes system configurations continually to enhance resilience against ransomware.	[51]
3. **Emerging Frontiers**	Federated Learning	Distributed machine learning for scalable edge and fog-assisted detection and prevention.	[57]
	Analyzing System Information	Monitors log files and Windows Registry for insights into ransomware activities.	[50]
	Finite State Machines	Applies structured models to identify specific ransomware behaviors.	[50]
	Honeypots	Uses simulated environments to gather information on attacker tactics and behaviors.	[52]
	Hardware Anomaly Detection	Employs the HARD-Lite framework using hardware information and machine learning for detection.	[58]

Table 1 provides a concise comparison of various methods used to detect ransomware, categorized into Traditional Approaches, Advanced Techniques, and Emerging Frontiers. Traditional methods, such as Signature-Based Detection and Heuristic Analysis, offer reliable detection of known threats but may struggle with new variants. Advanced Techniques like Machine Learning-Based Detection and Behavioral Analysis are more adaptable and can identify novel ransomware patterns, though they may require significant resources. Emerging Frontiers, including Federated Learning and Finite State Machines, represent the latest innovations in ransomware detection, offering scalable and sophisticated solutions but may face challenges such as privacy concerns and adaptability to new threats. Table 1 underscores the importance of a diverse and evolving approach to ransomware detection, as no single method is universally effective against all types of ransomware attacks. Table 5 provides a detailed comparative analysis of ransomware detection techniques, highlighting the evolution of detection methods and incorporating the latest research findings. It underscores the importance of continuously adapting and exploring new solutions to combat the evolving cyber threat of ransomware, guided by insights from recent academic research.

Table 5: Comparative Analysis of Ransomware Detection Techniques

Technique	**Category**	**Description**	**Strengths**	**Weaknesses**	**References**
Signature-Based Detection	**Traditional**	Compares file signatures against a known database	Fast, efficient against known variants	Ineffective against new or modified strains	[7, 59]
Heuristic Analysis		Identifies suspicious behaviors (encryption, network traffic)	Detects unseen variants based on patterns	Requires continuous rule updates, prone to false positives	[7, 54, 60]
Sandbox Analysis		Isolates suspicious files in a controlled environment	Analyzes behavior without risking real system	Resource-intensive, may not capture all real-world interactions	[7, 59, 60]

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Technique	Category	Description	Strengths	Weaknesses	References
Deep Packet Inspection		Examines network traffic for malicious activity	Detects command-and-control, data exfiltration	Complex setup, potential performance overhead	[7, 59]
Machine Learning-Based Detection	Advanced	Analyzes data patterns to detect ransomware	Adapts to new variants, high accuracy potential	Requires training data, computational resources	[7, 59, 61, 62]
Behavioral Analysis		Monitors program and process behavior for deviations	Detects abnormal activities indicative of ransomware	Requires defining normal behavior baselines	[7, 59, 60, 62]
Anomaly Detection		Identifies unusual system activity (encryption spikes, unauthorized access)	Real-time detection of potential attacks	May generate false positives, requires fine-tuning	[7, 59, 60, 62]
File Access Control Policies		Restricts unauthorized access to files	Prevents ransomware from modifying or deleting files	Requires careful policy configuration, potential compatibility issues	[7, 59, 62]
Moving Target Defense (MTD)		Dynamically changes system configurations	Makes it difficult for ransomware to target specific files or systems	Complex implementation, potential performance impact	[7, 59, 62]
Federated Learning	Emerging	Distributed machine learning for scalable detection and prevention	Scalable solution, adapts to diverse environments	Privacy concerns, requires secure communication channels	[7, 62, 63]
Analyzing System Information		Monitors log files and Windows Registry changes	Detects early signs of ransomware activity	Requires log aggregation and analysis capabilities	[7, 62, 63]
Finite State Machines		Structured models for identifying specific ransomware behaviors	Efficient detection of known patterns	Limited adaptability to new variants	[7, 62, 63]
HARD-Lite		Uses low-level hardware information and machine learning for detection	Increases detection accuracy, reduces false positives	Requires separate machine for classifier, scalability considerations	[63]
Novel Ransomware Virus Detection		Utilizes machine and deep learning methods for early detection	Allows early identification and prevention of significant damage	Initial analysis and examination of each file and network packet required	[64]

Table 2 presents a comparative analysis of ransomware detection techniques, evaluating their strengths and weaknesses to guide organizational cybersecurity strategies. Traditional methods like Signature-Based Detection and Heuristic Analysis offer foundational security but have limitations, such as difficulty with new variants and false positives. Sandbox Analysis and Deep Packet Inspection provide in-depth threat analysis but can be resource-intensive and complex. Advanced strategies, including Machine Learning-Based Detection and Behavioral Analysis, represent progress in adapting to new threats and identifying abnormal behavior, though they require significant data and fine-tuning. File Access Control Policies and Moving Target Defense enhance security by preventing unauthorized changes and dynamically altering system configurations, yet they demand careful implementation. Emerging technologies like Federated Learning and System Information Analysis introduce innovative detection capabilities but face challenges such as privacy concerns and the need for advanced data management. Finite State Machines offer efficient pattern recognition but lack adaptability to new threats. Overall, the analysis emphasizes that a singular approach is insufficient against ransomware. A layered defense, combining multiple detection methods, is most effective. As ransomware continues to evolve, ongoing research and updates in detection techniques are crucial for maintaining strong cybersecurity defenses.

4. CHALLENGES AND LIMITATIONS IN RANSOMWARE DETECTION

Ransomware detection is a critical component of cybersecurity, but it faces several challenges and limitations that can hinder its effectiveness. These challenges are multifaceted, ranging from the technical aspects of detection to the evolving nature of ransomware threats. Table 6 shows ransomware detection challenges.

Table 6: Ransomware Detection Challenges

	Challenge	Description	Implications	References
1	Evolving Nature of Ransomware Attacks	Ransomware attacks constantly evolve, with cybercriminals developing new evasion techniques.	Detection systems must be regularly updated, posing a challenge to maintain long-term effectiveness.	[59, 65, 66]
2	Distinguishing Between Legitimate and Malicious Software	The need to accurately identify legitimate software from ransomware.	Risks of false positives disrupting operations and false negatives allowing ransomware execution.	[65]
3	Integration with Other Security Systems	Effective detection requires integration with a variety of security systems.	Integration complexity and the need for compatibility with diverse security solutions.	[65]
4	Scalability and Performance	As data volume and endpoints increase, systems must scale without compromising performance or security.	Challenges in maintaining scalability, performance, and security simultaneously.	[65]
5	Limited Visibility into Industrial Control Systems	Proprietary and outdated nature of ICS and SCADA systems limits visibility.	Traditional cybersecurity measures may be ineffective in protecting these systems.	[67]
6	Scientific Rigor and Experimentation	Lack of scientific rigor in ransomware detection research.	Affects the reliability of proposed detection mechanisms.	[68]
7	Computational Complexity and Bias in AI	Incorporating AI introduces computational complexity and potential biases.	Affects the accuracy and fairness of AI-based detection.	[69, 70]
8	Dynamic Analysis Limitations	Dynamic analysis may not detect subtle changes in malicious behavior.	Some ransomwares may evade detection.	[71, 72]
9	Dataset and Feature Selection	Creating and maintaining an up-to-date dataset for machine learning is challenging.	Affects the effectiveness of machine learning-based ransomware detection.	[73]
10	Hybrid Analysis	Combining static and dynamic analyses introduces complexity.	Leverages strengths of both methods but complicates the detection process.	[72, 74]
11	API Call Sequence Analysis	Distinguishing API call sequences through machine learning requires extensive data.	Shows promise but needs representative training data for high accuracy.	[75]

In conclusion, ransomware detection is a complex field that requires continuous research and development to address the challenges and limitations posed by the ever-changing threat landscape. Collaboration between academia and industry is essential to develop effective solutions that can adapt to new ransomware tactics and protect against these malicious threats.

5. EXPLORING NEW SOLUTIONS AND FUTURE DIRECTIONS

The field of ransomware detection is continuously evolving, with researchers and cybersecurity experts exploring new solutions and future directions to stay ahead of cybercriminals. Table 7 presents the forefront of ransomware detection research.

Table 7: New Solutions and Future Directions Ransomware

Research Area	Description	Key Innovations	References
Majority Voting and Scorecard Approaches	Utilizes multiple tests to enhance detection accuracy beyond single-test methods.	Cumulative scoring from discrete tests for comprehensive capability.	[50, 51]
Automated Ransomware Detection Trends	Reviews current trends and evaluates the strengths and limitations of automated detection techniques.	Chronology of ransomware attacks and insights into prevention, mitigation, and recovery strategies.	[62]
Theoretical Frameworks for Detection, Avoidance, and Mitigation	Develops frameworks like the DAM model to guide the classification and implementation of detection techniques.	Theoretical basis for comprehensive ransomware attack solutions.	[76]
Traffic Analysis and Metaheuristic Feature Selection	Proposes methods to improve ransomware detection accuracy on Android devices through optimized feature selection.	Use of traffic analysis and metaheuristic methods like PSO.	[58]
Comprehensive Reviews and Unified Metrics	Offers structured assessments of ransomware mitigation techniques and proposes unified metrics for evaluation.	Structured approach to assess strengths and weaknesses of existing solutions.	[77]
SSD-Assisted Detection and Data Recovery	Integrates detection and recovery techniques into SSD firmware for enhanced data protection.	Hardware-level security through SSD firmware integration.	[29]
Addressing Zero-Day Attacks	Employs deep learning models and ensemble classifiers to detect previously unknown ransomware threats.	Deep learning models like contractive autoencoders for zero-day attack detection.	[78]
Machine Learning for Android Ransomware Detection	Focuses on machine learning approaches for high-accuracy ransomware detection on the latest Android versions.	Updated feature lists including permissions and API package calls.	[79]
API Call Analysis	Investigates ransomware detection through the analysis of API call sequences.	Static analysis approach to distinguish between benign and malicious apps.	[80, 81]
Federated Learning for IIoT Systems	Proposes a targeted ransomware detection model for IIoT systems using federated learning and deep learning techniques.	Asynchronous Peer-to-Peer Federated Learning (AP2PFL) and DL techniques for IIoT.	[57]
Big Data in Cybersecurity	Highlights the growing importance of big data analysis in detecting ransomware activity.	Analysis of large datasets to uncover patterns and anomalies indicative of ransomware	[82]

Table 7 synthesizes the latest advancements and research directions in ransomware detection, emphasizing the development of integrated approaches that leverage machine learning, big data analytics, and hardware integration. Continuous innovation and collaboration are essential for adapting to the dynamic nature of ransomware threats.

6. OPEN RESEARCH PROBLEMS

The exploration of ransomware detection has unveiled a variety of innovative strategies and methodologies. However, several open research problems remain, which present opportunities for further investigation and development in the field. The following Table 8 outlines these problems and their corresponding references:

Table 8: Open Ransomware Research Problems

Open Research Problem	Description	References
valuation and Comparison of Detection Tools	The lack of a standardized dataset and unified evaluation metrics for ransomware detection tools complicates the comparison of different techniques.	[83]
Classification Strategies	While various ransomware detection and classification strategies have been proposed, there is a need for further refinement and development of these methods to enhance accuracy and efficiency.	[84]
Labeling for Anomaly Detection	The challenge of working with unlabeled data in anomaly detection necessitates innovative approaches to labeling, such as interactive and semi-supervised methods.	[85]
Systematic Detection Techniques	The evolution of ransomware into more intelligent forms that can spread over networks calls for systematic detection techniques that can quickly identify and respond to attacks.	[86]
Security of Cyber-Physical Systems (CPS)	The complexity and interconnectedness of CPS pose significant security challenges, requiring comprehensive strategies for attack surface detection and mitigation.	[87]
Machine Learning Algorithm Optimization	The optimization of machine learning algorithms for ransomware detection, including the selection of features and the tuning of hyperparameters, remains an area for further research.	[88]
Crypto Ransomware Attack Detection	The development of early detection models for crypto ransomware, particularly those capable of overcoming evasive mechanisms employed by attackers, is crucial.	[45]
Server-Side Database Ransomware Detection	The recent shift of ransomware attacks to server-side databases highlights the need for novel detection solutions, such as dynamic analysis of query sequences.	[89]

These open research problems underscore the dynamic and challenging nature of ransomware detection. Addressing these issues requires a multidisciplinary approach that combines insights from cybersecurity, machine learning, data science, and beyond. Future research directions should focus on developing standardized datasets, refining classification strategies, enhancing machine learning algorithms, and exploring new detection methodologies for both client and server-side attacks. Collaboration among researchers, industry professionals, and policymakers will be key to advancing the state of the art in ransomware detection and mitigation.

7. FINDINGS

This study categorizes ransomware detection techniques into three main groups: Traditional Approaches, Advanced Techniques, and Emerging Frontiers, each with distinct methodologies for identifying and mitigating ransomware threats. Traditional Approaches are foundational but may struggle with new ransomware strains due to their reliance on known signatures and behaviors. Techniques like Signature-Based Detection and Heuristic Analysis are efficient against known variants but require updates to tackle new strains. Sandbox Analysis and Deep Packet Inspection provide insights into suspicious behaviors and network traffic but may be resource-intensive and complex to set up. Advanced Techniques offer adaptability and potential for high accuracy. Machine Learning-Based Detection and Behavioral

Analysis utilize algorithms and behavioral monitoring to adapt to new threats, though they require significant resources for training and implementation. Anomaly Detection and File Access Control Policies provide real-time detection and prevent unauthorized file access, respectively, but require fine-tuning and careful policy configuration. Emerging Frontiers represent the cutting edge of ransomware detection research. Federated Learning promises scalable and sophisticated solutions but may face challenges such as privacy concerns and adaptability to new threats. Techniques like Analyzing System Information and Finite State Machines provide insights into ransomware activities and apply structured models to identify specific behaviors, respectively, but require robust log aggregation and analysis capabilities.

The findings highlight the importance of a multi-layered defense strategy that incorporates a variety of detection methods to address the diverse tactics employed by ransomware authors. As ransomware continues to evolve, so must the detection techniques used to combat it. The paper emphasizes the need for continuous adaptation and exploration of new solutions to stay ahead in the ongoing battle against this cyber threat.

8. CONCLUSION

The research presented introduces several novel contributions to the field of ransomware detection. Firstly, the development of a comprehensive taxonomy of ransomware research stands out as a significant contribution, providing a structured framework that categorizes existing research into coherent groupings based on specific criteria. This taxonomy not only facilitates a clearer understanding of the field but also promotes the transfer of knowledge across different research areas, which is crucial for the development of more robust and effective defense mechanisms. Secondly, the paper identifies critical gaps in current ransomware detection strategies, particularly highlighting the need for further exploration into offensive and adversarial machine learning techniques. By pinpointing these gaps, the research paves the way for future investigations that could lead to the development of more resilient defense mechanisms capable of adapting to the ever-changing tactics of ransomware creators. Lastly, the paper's focus on the integration of emerging technologies such as federated learning and hardware anomaly detection into ransomware defense strategies represents a forward-thinking approach to cybersecurity. These technologies offer innovative solutions that could potentially transform the way ransomware is detected and mitigated, although their real-world effectiveness and long-term impact are still under evaluation. The impact of this research is multifaceted. On a practical level, the insights provided by the study have the potential to significantly enhance the cybersecurity defenses of organizations and individuals against ransomware threats. By offering a detailed analysis of ransomware evolution, attack methods, and detection techniques, the paper equips cybersecurity professionals with the knowledge needed to develop more effective defense strategies. Academically, the research contributes to the body of knowledge on ransomware by synthesizing a vast array of literature into a comprehensive overview. This not only aids in the consolidation of existing research but also sets a foundation for future scholarly work in the field. The novel taxonomy and identification of research gaps serve as a roadmap for other researchers to build upon, fostering further innovation and collaboration in ransomware detection research. In conclusion, the research presented in this paper makes notable contributions to the field of ransomware detection by providing a novel taxonomy, identifying key research gaps, and exploring the integration of emerging technologies. The impact of this work is significant, offering practical insights for enhancing cybersecurity defenses and laying the groundwork for future academic research. Through a collaborative effort that spans empirical evaluation, theoretical frameworks, and the development of innovative countermeasures, this research underscores the critical need for a unified approach to ransomware research and the importance of continuous innovation in the fight against this relentless digital menace.

REFERENCES:

[1] Park, H., J.-e. Seo, and H. Kwon, Research for making smart city cybersecurity policy according to communication theory: Focus on the communication structure. DG.O 2022: The 23rd Annual International Conference on Digital Government Research, 2022.

[2] Nayak, S.C., V. Tiwari, and B.K. Samanthula, Review of Ransomware Attacks and a Data Recovery Framework using Autopsy Digital Forensics Platform. 2023 IEEE 13th Annual

Computing and Communication Workshop and Conference (CCWC), 2023: p. 0605-0611.

[3] Akbanov, M., V.G. Vassilakis, and M.D. Logothetis, WannaCry Ransomware: Analysis of Infection, Persistence, Recovery Prevention and Propagation Mechanisms. Journal of Telecommunications and Information Technology, 2019.

[4] Noorbehbahani, F., F. Rasouli, and M. Saberi, Analysis of Machine Learning Techniques for Ransomware Detection. 2019 16th International ISC (Iranian Society of Cryptology) Conference on Information Security and Cryptology (ISCISC), 2019: p. 128-133.

[5] Alraizza, A. and A. Algarni, Ransomware detection using machine learning: A survey. Big Data and Cognitive Computing, 2023. 7(3): p. 143.

[6] Trim, P.R. and Y.-I. Lee, Managing cybersecurity threats and increasing organizational resilience. 2023, MDPI. p. 177.

[7] Razaulla, S., et al., The Age of Ransomware: A Survey on the Evolution, Taxonomy, and Research Directions. IEEE Access, 2023.

[8] Alraizza, A. and A. Algarni, Ransomware Detection Using Machine Learning: A Survey. Big Data Cogn. Comput., 2023. 7: p. 143.

[9] Russia and China lead on offensive cyber skills. Emerald Expert Briefings, 2020.

[10] Karunakaran, S., et al., Internet of Things Assisted Automated Ransomware Recognition using Harmony Search Algorithm with Deep Learning. 2023 International Conference on Sustainable Communication Networks and Application (ICSCNA), 2023: p. 475-480.

[11] Aleshinskaya, E.V., Rhetorical structure of research paper introductions in computer science: a comparative analysis. RESEARCH RESULT Theoretical and Applied Linguistics, 2023.

[12] Horduna, M., S.-M. Lazarescu, and E. Simion, A note on machine learning applied in ransomware detection. IACR Cryptol. ePrint Arch., 2023. 2023: p. 45.

[13] Bhuva, B.D., P. Zavarsky, and S. Butakov, An Analysis of Effectiveness of StegoAppDB and Data Hiding Efficiency of StegHide Image Steganography Tools. 2021 2nd International Conference on Secure Cyber Computing and Communications (ICSCCC), 2021: p. 208-211.

[14] Dhotre, D., et al., The Rise of Crypto Malware: Leveraging Machine Learning Techniques to Understand the Evolution, Impact, and Detection of Cryptocurrency-Related Threats. International Journal on Recent and Innovation Trends in Computing and Communication, 2023.

[15] Pujari, R.A. and P.S. Revankar, Wrapper-based feature selection on ransomware detection using machine learning, in Recent Advances in Material, Manufacturing, and Machine Learning. 2023, CRC Press. p. 469-474.

[16] Al-Ameer, A.A.A. and W.S. Bhaya, Enhanced Intrusion Detection in Software-Defined Networks Through Federated Learning and Deep Learning. Ingénierie des Systèmes d'Information, 2023. 28(5).

[17] Ruzafa-Alcazar, P., et al., Intrusion Detection Based on Privacy-Preserving Federated Learning for the Industrial IoT. IEEE Transactions on Industrial Informatics, 2023. 19: p. 1145-1154.

[18] Zhang, L., et al., A Robust Game-Theoretical Federated Learning Framework With Joint Differential Privacy. IEEE Transactions on Knowledge and Data Engineering, 2023. 35: p. 3333-3346.

[19] Hider, U., Ransomware Attacks: Evolution, Impacts, and Countermeasures. 2024, EasyChair.

[20] Zaki, H., The Evolution, Impact, and Mitigation of Ransomware Attacks. 2024, EasyChair.

[21] Lachtar, N., D. Ibdah, and A. Bacha, The Case for Native Instructions in the Detection of Mobile Ransomware. IEEE Letters of the Computer Society, 2019. 2: p. 16-19.

[22] Mercaldo, F., F. Martinelli, and A. Santone, Image-Based Malware Detection Through a Deep Neuro-Fuzzy Model. 2023 IEEE International Conference on Fuzzy Systems (FUZZ), 2023: p. 1-7.

[23] Sumaryani, N.M. Kautilya's Views on Secret Activities of Intelligence in Arthasastra and Its Current Relevance. 2021.

[24] Alsoghyer, S. and I.M. Almomani, On the Effectiveness of Application Permissions for Android Ransomware Detection. 2020 6th Conference on Data Science and Machine Learning Applications (CDMA), 2020: p. 94-99.

[25] Prasetya, A.Y., K.I. Aini, and C. Lim, Comparative Analysis of Attack Behavior Patterns in Petya, CryptInfinite, and Locky

Ransomware Using Hybrid Analysis. 2023 IEEE International Conference on Cryptography, Informatics, and Cybersecurity (ICoCICs), 2023: p. 29-34.

[26] Razaulla, S., et al., The Age of Ransomware: A Survey on the Evolution, Taxonomy, and Research Directions. IEEE Access, 2023. 11: p. 40698-40723.

[27] Quiroz, J.T., M.A.A. Oscategui, and J. Armas-Aguirre, Cybersecurity Taxonomy: research and knowledge areas. 2021 IEEE 1st International Conference on Advanced Learning Technologies on Education & Research (ICALTER), 2021: p. 1-4.

[28] Alshaikh, H., H. Ahmed, and N. Ramadan, Crypto-Ransomware Detection and Prevention Techniques and Tools A Survey. International Journal of Computing and Digital Systems, 2023.

[29] Baek, S., et al., SSD-Assisted Ransomware Detection and Data Recovery Techniques. IEEE Transactions on Computers, 2021. 70: p. 1762-1776.

[30] Raymond, V.J. and R.J.R. Raj. A Comprehensive Study on Ransomware Attacks in Online Pharmacy Community. 2020.

[31] T. R., S. and S. K. T., A Review on Major Cyber Threats and Recommended Counter Measures. International Journal for Research in Applied Science and Engineering Technology, 2023.

[32] Al-Haija, Q.A. and A.A. Alsulami, High Performance Classification Model to Identify Ransomware Payments for Heterogeneous Bitcoin Networks. Electronics, 2021.

[33] Larsen, E., D. Noever, and K. MacVittie, A survey of machine learning algorithms for detecting ransomware encryption activity. arXiv preprint arXiv:2110.07636, 2021.

[34] DURMUŞ ŞENYAPAR, H.N., Digital Marketing in the Age of Cyber Threats: A Comprehensive Guide to Cybersecurity Practices. The Journal of Social Science, 2024.

[35] Raheem, A.H., et al., Estimation of Ransomware Payments in Bitcoin Ecosystem. 2021 IEEE Intl Conf on Parallel & Distributed Processing with Applications, Big Data & Cloud Computing, Sustainable Computing & Communications, Social Computing & Networking (ISPA/BDCloud/SocialCom/SustainCom), 2021: p. 1667-1674.

[36] Cen, M., et al., Ransomware early detection: A survey. Computer Networks, 2024. 239: p. 110138.

[37] Gómez Hernández, J.A., et al., Crypto-Ransomware: A Revision of the State of the Art, Advances and Challenges. Electronics, 2023. 12(21): p. 4494.

[38] Gómez Hernández, J.A., et al., Crypto-Ransomware: A Revision of the State of the Art, Advances and Challenges. Electronics, 2023.

[39] Cen, M., et al., Ransomware early detection: A survey. Computer Networks, 2023: p. 110138.

[40] Su, D., et al., Detecting Android Locker-Ransomware on Chinese Social Networks. IEEE Access, 2019. 7: p. 20381-20393.

[41] Moussaileb, R., et al. Watch Out! Doxware on the Way. in Crisis. 2019.

[42] Bagui, S.S. and H. Brock, Machine Learning for Android Scareware Detection. J. Inf. Technol. Res., 2022. 15: p. 1-15.

[43] Seifert, C., et al., Robust scareware image detection. 2013 IEEE International Conference on Acoustics, Speech and Signal Processing, 2013: p. 2920-2924.

[44] Gautam, A. and N. Rahimi, Viability of Machine Learning in Android Scareware Detection. EPiC Series in Computing.

[45] Alqahtani, A. and F.T. Sheldon, A survey of crypto ransomware attack detection methodologies: an evolving outlook. Sensors, 2022. 22(5): p. 1837.

[46] Roemsri, P., S. Puangpontip, and R. Hewett, On Detecting Crypto Ransomware Attacks: Can Simple Strategies be Effective? 2023 6th International Conference on Information and Computer Technologies (ICICT), 2023: p. 138-143.

[47] Bornmann, L. and R. Mutz, Growth rates of modern science: A bibliometric analysis based on the number of publications and cited references. Journal of the association for information science and technology, 2015. 66(11): p. 2215-2222.

[48] Sharma, N. and R. Shanker, Analysis of Ransomware Attack and Their Countermeasures: A Review. 2022 International Conference on Electronics and Renewable Systems (ICEARS), 2022: p. 1877-1883.

[49] Muniandy, M., et al., Evolution and Impact of Ransomware: Patterns, Prevention, and Recommendations for Organizational Resilience. International Journal of

Academic Research in Business and Social Sciences, 2024.

[50] Davies, S.R., R. Macfarlane, and W.J. Buchanan, Majority Voting Ransomware Detection System. Journal of Information Security, 2023.

[51] Davies, S.R., R. Macfarlane, and W.J. Buchanan, Majority Voting Approach to Ransomware Detection. arXiv preprint arXiv:2305.18852, 2023.

[52] Madanayaka, B.P.W., et al., A Proactive Approach for Behavior Based Ransomware Detection. 2023 5th International Conference on Advancements in Computing (ICAC), 2023: p. 346-351.

[53] Albin Ahmed, A., et al., Android Ransomware Detection Using Supervised Machine Learning Techniques Based on Traffic Analysis. Sensors, 2023. 24(1): p. 189.

[54] Ahmad, S., et al., A Recent Systematic Review of Ransomware Attack detection in machine learning techniques. 2023 4th International Conference on Artificial Intelligence and Data Sciences (AiDAS), 2023: p. 349-354.

[55] Hwang, J., et al., Two-Stage Ransomware Detection Using Dynamic Analysis and Machine Learning Techniques. Wireless Personal Communications, 2020. 112: p. 2597 - 2609.

[56] Dib, A., S. Ghazi, and M.M.S. Mehdi, Ransomware Attack Detection based on Pertinent System Calls Using Machine Learning Techniques. International journal of Computer Networks &amp; Communications, 2023.

[57] Al-Hawawreh, M.S., E. Sitnikova, and N. Aboutorab, Asynchronous Peer-to-Peer Federated Capability-based Targeted Ransomware Detection Model for Industrial IoT. IEEE Access, 2021. PP: p. 1-1.

[58] Hossain, M.S., et al., Android Ransomware Detection From Traffic Analysis Using Metaheuristic Feature Selection. IEEE Access, 2022. 10: p. 128754-128763.

[59] Kamil, S., et al., The Rise of Ransomware: A Review of Attacks, Detection Techniques, and Future Challenges. 2022 International Conference on Business Analytics for Technology and Security (ICBATS), 2022: p. 1-7.

[60] De Gaspari, F., et al., Evading behavioral classifiers: a comprehensive analysis on evading ransomware detection techniques. Neural Computing and Applications, 2022. 34: p. 12077 - 12096.

[61] Almomani, I., A. Alkhayer, and W. El-Shafai, E2E-RDS: Efficient End-to-End Ransomware Detection System Based on Static-Based ML and Vision-Based DL Approaches. Sensors, 2023. 23(9): p. 4467.

[62] Jegede, A., et al., Trends and Future Directions in Automated Ransomware Detection. Journal of Computing and Social Informatics, 2022.

[63] Woralert, C., C. Liu, and Z. Blasingame, HARD-Lite: A Lightweight Hardware Anomaly Realtime Detection Framework Targeting Ransomware. IEEE Transactions on Circuits and Systems I: Regular Papers, 2023. 70: p. 5036-5047.

[64] Charmilisri, A., et al., A Novel Ransomware Virus Detection Technique using Machine and Deep Learning Methods. 2023 7th International Conference on Intelligent Computing and Control Systems (ICICCS), 2023: p. 8-14.

[65] Zhuravchak, D., V. Dudykevych, and A. Tolkachova, STUDY OF THE STRUCTURE OF THE SYSTEM FOR DETECTING AND PREVENTING RANSOMWARE ATTACKS BASED ON ENDPOINT DETECTION AND RESPONSE. Cybersecurity: Education, Science, Technique, 2023.

[66] Urooj, U., et al., Ransomware Detection Using the Dynamic Analysis and Machine Learning: A Survey and Research Directions. Applied Sciences, 2021.

[67] Gazzan, M. and F.T. Sheldon, Opportunities for Early Detection and Prediction of Ransomware Attacks against Industrial Control Systems. Future Internet, 2023. 15: p. 144.

[68] Vilela, D.S. and M.P. Correia. Programmable Sandbox for Malware Analysis. 2021.

[69] Markevych, M. and M.E. Dawson, A Review of Enhancing Intrusion Detection Systems for Cybersecurity Using Artificial Intelligence (AI). International conference KNOWLEDGE-BASED ORGANIZATION, 2023. 29: p. 30 - 37.

[70] Rangaraju, S., AI SENTRY: REINVENTING CYBERSECURITY THROUGH INTELLIGENT THREAT DETECTION. EPH - International Journal of Science And Engineering, 2023.

[71] Nikolova, E.P., Markov Models for Malware and Intrusion Detection: A Survey. Serdica Journal of Computing, 2023.

[72] Al Obaidan, F. and S. Saeed, Digital Transformation and Cybersecurity Challenges. Handbook of Research on Advancing Cybersecurity for Digital Transformation, 2021.

[73] Herrera-Silva, J.A. and M. Hernández-Álvarez, Dynamic feature dataset for ransomware detection using machine learning algorithms. Sensors, 2023. 23(3): p. 1053.

[74] Aljubory, N. and B.M. Khammas, Hybrid Evolutionary Approach in Feature Vector for Ransomware Detection. 2021 International Conference on Intelligent Technology, System and Service for Internet of Everything (ITSS-IoE), 2021: p. 1-6.

[75] Lin, T.-L., et al., Ransomware Detection by Distinguishing API Call Sequences through LSTM and BERT Models. The Computer Journal, 2023.

[76] Kapoor, A., et al., Ransomware Detection, Avoidance, and Mitigation Scheme: A Review and Future Directions. Sustainability, 2021.

[77] McIntosh, T.R., et al., Ransomware Mitigation in the Modern Era: A Comprehensive Review, Research Challenges, and Future Directions. ACM Computing Surveys (CSUR), 2021. 54: p. 1 - 36.

[78] Zahoora, U., et al., Zero-day Ransomware Attack Detection using Deep Contractive Autoencoder and Voting based Ensemble Classifier. Applied Intelligence, 2022. 52: p. 13941 - 13960.

[79] Almomani, I.M., A. Alkhayer, and M. Ahmed, An Efficient Machine Learning-based Approach for Android v.11 Ransomware Detection. 2021 1st International Conference on Artificial Intelligence and Data Analytics (CAIDA), 2021: p. 240-244.

[80] Yadav, N., et al., A Complete Study on Malware Types and Detecting Ransomware Using API Calls. 2021 9th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO), 2021: p. 1-5.

[81] Alsoghyer, S. and I.M. Almomani, Ransomware Detection System for Android Applications. Electronics, 2019.

[82] 8Alani, M.M., Big data in cybersecurity: a survey of applications and future trends. Journal of Reliable Intelligent Environments, 2021. 7: p. 85 - 114.

[83] Berrueta, E., et al., Open Repository for the Evaluation of Ransomware Detection Tools. IEEE Access, 2020. 8: p. 65658-65669.

[84] Vehabovic, A., et al. Ransomware detection and classification strategies. in 2022 IEEE International Black Sea Conference on Communications and Networking (BlackSeaCom). 2022. IEEE.

[85] Theissler, A., et al. VIAL-AD: Visual Interactive Labelling for Anomaly Detection - An Approach and Open Research Questions. in IAL@PKDD/ECML. 2020.

[86] Lee, S.-J., et al., Study on Systematic Ransomware Detection Techniques. 2022 24th International Conference on Advanced Communication Technology (ICACT), 2022: p. 297-301.

[87] Chattopadhyay, A., A. Prakash, and M.A. Shafique, Secure Cyber-Physical Systems: Current trends, tools and open research problems. Design, Automation & Test in Europe Conference & Exhibition (DATE), 2017, 2017: p. 1104-1109.

[88] Usha, G., et al., Enhanced Ransomware Detection Techniques using Machine Learning Algorithms. 2021 4th International Conference on Computing and Communications Technologies (ICCCT), 2021: p. 52-58.

[89] Sendner, C., et al., Ransomware Detection in Databases through Dynamic Analysis of Query Sequences. 2022 IEEE Conference on Communications and Network Security (CNS), 2022: p. 326-334.