

## A survey on ransomware detection using AI models

**Goteti Badrinath, Arpita Gupta**

Department of Computer Science and Engineering, KL Deemed to be University, Koneru Lakshmaiah Education Foundation,  
Hyderabad, India

### Article Info

#### Article history:

Received Oct 17, 2024

Revised Jun 17, 2025

Accepted Jul 1, 2025

#### Keywords:

Artificial intelligence

Cloud security

Deep learning

Encryption

Machine learning

Ransomware

Real-time detection

### ABSTRACT

Data centers and cloud environments are compromised as they are at great risk from ransomware attacks, which attack data integrity and security. Through this survey, we explore how AI, especially machine learning and deep learning (DL), is being used to improve ransomware detection capabilities. It classifies ransomware types, highlights active groups such as Akira, and evaluates new DL techniques effective at real-time data analysis and encryption handling. Feature extraction, selection methods, and essential parameters for effective detection, including accuracy, precision, recall, F1-score and receiver operating characteristic (ROC) curve, are identified. The findings point to the state of the art and the state of the art in AI based ransomware detection and underscore the need for robust, real-time models and collaborative research. The statistical and graphical analyses help researchers and practitioners understand existing trends and directions for future development of efficient ransomware detection systems to strengthen cybersecurity in data centers and cloud infrastructures.

*This is an open access article under the [CC BY-SA](#) license.*



### Corresponding Author:

Goteti Badrinath

Department of Computer Science and Engineering, KL Deemed to be University

Koneru Lakshmaiah Education Foundation

Hyderabad, Telangana, India

Email: badrinath.goteti@gmail.com

## 1. INTRODUCTION

Ransomware attacks have become a major and growing threat in the world of cybersecurity: personal and corporate data are being targeted more and more frequently and more and more sophisticated. The attacked software is deployed in the victim's computer, and it infiltrates the system and encrypts the necessary data so that the victim cannot access it unless a ransom is paid [1]. Often, the data encrypted is of sensitive personal nature, files important to the business. It is often demanded in cryptocurrencies like Bitcoin, which makes it hard to trace the transactions [2]. Ransomware attacks have serious and multiple consequences. These ransom payments cost victims huge amounts of money, as do the costs of downtime and recovery efforts. Furthermore, operational disruptions can be very broad, especially for organizations that depend on continuous access to their data. That can result in business operations being stalled, loss of productivity and missed opportunities. Additionally, it is possible that a ransomware attack can do a lot of reputational damage to an organization, eroding customer trust and damaging an organization's brand image [3].

Ransomware attacks are rising hand in hand with the growing need for data centers and cloud services. Data centers are a critical part of the infrastructure-housing large amounts of data and being critical to the functioning of businesses and governments. With modern IT strategies, scalable and on demand access to computing resources is an integral part of cloud environments [4]. These environments store high value data in a centralized manner and are therefore attractive targets for cyber criminals. Ransomware attacks on

data centers and cloud services can be very successful and cripple an entire organization, which makes these very important services require robust security. Ransomware attacks have progressed to be one of the most common and dangerous type of cybercrime since it began. Of course, the simplest of ransoms were the AIDS Trojan that used symmetric encryption to lock files and demand a ransom for providing the key to unlock but its simplicity made its decryption possible once the key was found. Ransomware has become more sophisticated over the years, using increasingly stronger methods used to encrypt data that risks being virtually unrulable by those without the right key. With the emergence of cryptocurrencies like Bitcoin, attackers have even more reason to attack, as untraceable payments are facilitated. Ransomware can be categorized into three main types: locker ransomware, scareware and crypto ransomware. Scareware takes advantage of psychological manipulation, presenting fake warnings that the system is infected, or that some other problem exists, and then forcing users to pay for unnecessary software, usually without encrypting files. Locker ransomware locks victim out of their device, rendering files or application inaccessible until a ransom is paid, resulting in major disruption to personal and business operations [5]. One of the most damaging types of crypto ransomware encrypts critical files or an entire system, typically in exchange for a ransom, often in a cryptocurrency such as Bitcoin. Strong encryption methods make it very costly to turn off, with the cost accruing to the extent that businesses need to keep data available at all times.

The primary objective of this paper is to conduct a comprehensive literature survey on ransomware attacks, with a specific emphasis on servers running in data centers and cloud environments.

- Provide a historical overview and discuss the increasing complexity of ransomware attacks, focusing on data centers and cloud environments.
- Investigate how AI, specifically machine learning (ML) and deep learning (DL), has transformed ransomware detection compared to traditional methods.
- Compare the effectiveness of ML and DL techniques in ransomware detection, highlighting key models and their performance.
- Explore recent advancements and breakthroughs in DL techniques for ransomware detection, emphasizing real-time analysis and encryption addressing.
- Classify various ransomware groups and analyze highly active variants like Akira.

The literature review aims to provide an in-depth analysis of existing research on ransomware attacks, focusing on their evolution, the role of AI in detection, and the comparison between ML and DL approaches.

Signature based and heuristic based approaches are traditional methods for detecting ransomware as shown in Table 1. Signature based detection is based on maintaining a database of known malware signatures and discover attacks by matching incoming files and activities with these signatures. But it's not effective at new or modified variants that don't match known signatures. Unlike this heuristic based detection, the latter detects malware by applying some behavior pattern analysis methods, such as analyzing suspicious activities like rush encryption of multitudes of files, frequently modifying various and unexpected file entry in the network connection. The heuristic-based approaches are more flexible and more capable of detecting unknown threats, but generate false positives since these activities are erroneously considered as malicious.

Table 1. Traditional detection methods

Reference (Year)	Author	Resolved issue	Utilized technique	Result	Limitation
Brewer (2016) [6]	Brewer	Detection, prevention, and cure of ransomware	Signature-based and heuristic-based methods	Outlined detection and prevention strategies	Dependent on signature database and potential for false positives
Celdrán <i>et al.</i> (2022) [7]	Celdrán <i>et al.</i>	Behavioral-based malware detection	Behavioral analysis	Intelligent detection of malware	Potential for false positives
Kok <i>et al.</i> (2019) [8]	Kok <i>et al.</i>	Detection and prevention of ransomware	Signature-based methods	Effective against known threats	Ineffective against new or modified variants

ML algorithms analyze data to identify patterns indicative of ransomware. Common ML techniques include decision trees, random forests, and support vector machines (SVMs) as shown in Table 2. These techniques classify data and detect anomalies that may indicate ransomware activity.

DL techniques have shown superior performance in detecting ransomware compared to traditional ML methods due to their ability to handle complex data patterns and large volumes of data as shown in Table 3.

Table 2. Machine learning approaches

Reference (Year)	Author	Resolved issue	Utilized technique	Result	Limitation
Alraizza and Algarni (2023) [9]	Alraizza and Algarni	Detection of ransomware using ML	Machine learning	Improved detection accuracy	Limited to known ransomware patterns
O’Kane <i>et al.</i> (2018) [10]	O’Kane <i>et al.</i>	Evolution of ransomware	Historical analysis	Provided a comprehensive overview of ransomware evolution	Historical data may not cover all variants
Shaukat and Ribeiro (2018) [11]	Shaukat and Ribeiro	Defense against cryptographic ransomware	Layered defense system	Developed a defense system against ransomware	Complexity in implementation
Talabani and Abdulhadi (2022) [12]	Talabani and Abdulhadi	Bitcoin ransomware detection	Rule-based algorithms	Effective in detecting specific ransomware types	Limited scalability and flexibility

Table 3. Deep learning approaches

Reference (Year)	Author	Resolved issue	Utilized technique	Result	Limitation
Bello <i>et al.</i> (2021) [13]	Bello <i>et al.</i>	Detecting ransomware attacks using DL	Deep learning	Highlighted the effectiveness of DL in detecting ransomware	High computational resources required
Almashhadani <i>et al.</i> (2019) [14]	Almashhadani <i>et al.</i>	Crypto ransomware detection system	Multi-classifier network-based system	Demonstrated the effectiveness of a multi-classifier system	Scalability issues
Hwang <i>et al.</i> (2020) [15]	Hwang <i>et al.</i>	Two-stage ransomware detection	Dynamic analysis and machine learning techniques	Improved detection rates and reduced false positives	High computational and time resources required
Makinde <i>et al.</i> (2019) [16]	Makinde <i>et al.</i>	Distributed network behavior prediction	Machine learning and agent-based micro simulation	Accurate prediction of network behavior	Complex implementation and maintenance
Paquet-Clouston <i>et al.</i> (2019) [17]	Paquet-Clouston <i>et al.</i>	Ransomware payments in the bitcoin ecosystem	Machine learning and blockchain analysis	Insight into ransomware payment mechanisms	Requires extensive data analysis and computational power

## 2. RESEARCH METHOD

For this study, a methodology was designed to systematically and replicably evaluate ML and DL techniques for ransomware detection in data centers and cloud environments. ‘Ransomware detection’, ‘machine learning,’ ‘deep learning,’ and ‘cloud security’ were the areas of literature reviewed extensively [18]. Only the last decade’s relevant studies on AI based detection techniques were included, excluding non-empirical or outdated approaches. Trusted cybersecurity repositories were tapped to collect public datasets of ransomware activities including system logs, network traffic and file access patterns. Normalization and dimensionality reduction were achieved through data preprocessing using principal component analysis (PCA). Correlation analysis was used to extract key features such as encryption activity patterns and network anomalies, and these were validated. For ML algorithms, such as decision trees, random forests, and SVMs, we implemented models with Scikit-learn, and for DL models with convolutional neural networks (CNNs) and recurrent neural networks (RNNs). Model evaluation employed performance metrics such as accuracy, precision, recall, F1-score, and AUC- receiver operating characteristic (ROC).

The Figure 1 illustrates three main types of ransomwares: scareware, locker ransomware and crypto ransomware. Scareware is malware that pretends a victim’s system is infected with viruses or something similar and asks them to pay for fake solutions, using psychological manipulation rather than encrypting files. Locker ransomware isolates the users from their devices; blocking access to files and programs and holds the user’s hostage by demanding a ransom to return functionality, thus severely disrupting equipment. The most damaging kind of crypto ransomware encrypts critical files or entire systems, making them inaccessible, and holding victim’s hostage until they pay a ransom, usually in cryptocurrency, to gain access to the decryption key. From fear to restricted access, encryption, there are many tactics each type uses to coerce victims.

Ransomware groups classification is based on analyzing their tactics, techniques, and procedures (TTPs) to determine their behavior and develop appropriate countermeasures. This section goes into depth with some of the most active ransomware groups and how DL models can be used to do behavioral analysis for early detection and prevention.



Figure 1. Types of ransomwares

## 2.1. Highly active ransomware groups

### 2.1.1. Akira

Akira ransomware is a known aggressive ransomware that attacks both individuals and organizations. Most commonly it uses phishing emails and exploit kits to gain an initial access to a system. Strong encryption algorithms are used by Akira to lock files and the fees to obtain the decryption key from files is quite hefty. It also evades traditional antivirus and intrusion detection systems [19]. If the ransom isn't paid, however, the attackers will generally publish the stolen data. The quick propagation of Akira across networks makes it critical that detection and response are both timely.

### 2.1.2. Ryuk

All targets are large organizations, i.e., hospitals, government agencies, and businesses. Phishing emails or exploits of remote desktop protocols (RDP) are the most common ways it is delivered. Ryuk is a mixture of encryption and leak of data. It identifies and terminates processes that might interfere with the encryption process [20], and encrypts files before. In fact, Ryuk uses different persistence mechanisms in order to continue to have access to these compromised systems. Ryuk encrypts after which it demands a large ransom usually in Bitcoin, and threatens to destroy the decryption key if the ransom isn't paid within a specific window. Additionally, the ransomware also works around system restore points so there's no recovery without the decryption key.

### 2.1.3. Maze

Maze ransomware is a double extortion ransomware, meaning it encrypts the files and steals the data and threatens to publish it if the ransom is not paid. Maze aims at many industries such as finance, healthcare, and manufacturing. Exploit kits, phishing emails and vulnerable remote desktop connections are used by Maze to gain access to systems [21]. It uses a lot of encryption and spreads laterally through networks and will infect as many systems as possible. If they find you don't comply, they then release stolen data to the public. The exfiltrated data often appears as samples on the leak site of maze operators to pressure victims to pay the ransom.

## 2.2. Deep learning for behavioral analysis

In recent years, DL models have been used to classify ransomware groups by their behavioral patterns [22]. The models can process large volume of data to look for less obvious patterns and anatomies that show the signals of a ransomware attack. The use of DL in behavioral analysis offers several advantages:

### 1. Early detection

Using DL, deviant patterns in normal system behavior, e.g., the file access patterns, the encryption pace, the network traffic, can be detected. They can be early indicators of a ransomware attack [23]. The continuous analysis of system behavior in real-time monitoring systems provides the capability to detect and mitigate ransomware activities promptly.

### 2. Ransomware groups classification

Ransomware can be classified using the specific behaviors of different ransomware groups using DL models. For instance, the model can automatically extract relevant features from raw data, such as the frequency of file modifications, network communication patterns, and process execution behaviors, and then identify the unique TTPs of Akira, Ryuk, and Maze, which distinguishes them from other kinds of malwares. They are important for classification, especially accurately.

### 3. Improved accuracy

With the large amounts of data, DL models get better and better at learning. They can learn new and evolving ransomware threats continuously [24]. The context of detected anomalies can be understood by DL models so as to reduce the number of false positives, and to ensure that legitimate activities are not misclassified as malicious.

### 4. Improved response capabilities

DL model can once aware of a ransomware attack, it will then automatically trigger the response mechanisms: isolating affected systems, terminating malicious processes, and notifying security personnel. It helps in the ransomware groups classification for threat intelligence purposes by providing information about the TTP of some ransomware families [25]. The information is useful for developing targeted defense strategies and for overall cybersecurity posture.

## 2.3. Key detection parameters

- Detecting the activity of ransomware is important in real time so as to minimize damage and a swift response is possible. And real time detection means you are always watching, system activities, network traffic and user behavior looking out for any anomalies that would point to a ransomware attack. Security systems can then detect the ransomware as it begins to encrypt files, and countermeasures can thus be instigated to stop the attack, isolate the systems affected, and signal security personnel [26]. That immediate response is important, because it stops the spread of ransomware and minimizes data loss.
- Encryption such as TLS/SSL is essential in order to securely connect, in order to secure data transmissions, and avoid the impact of ransomware attacks. These methods help prevent attackers from ‘sniffing’ data that is exchanged between systems, data that is encrypted so it would be difficult and time consuming for an attacker to intercept or manipulate the data. Safe usage processes can be implemented to prevent ransomware infected computers from being accessed, or having information encrypted, including strong encryption protocols [27]. Another thing that it also helps us to know is the kind of encryption that ransomware uses because it helps us develop decryption tools and strategies to retrieve our files without paying any ransom.
- Behavioral analysis involves analyzing system behavior trying to spot unusual activities that might indicate ransomware presence. This includes files encryption suddenly, strange file access patterns, increase of files changes in short time, abnormal network traffic. Security systems can detect ransomware early in its execution phase by analyzing these behavior’s [28]. The reason why behavioral analysis is effective is because it looks at the actions taken by the malware instead of that malware’s code, meaning it can detect new and unknown ransomware variants based on their behavior.
- It is highly important to extract and select features for developing robust ransomware detection models as they are effective. To identify, and then select, the most relevant features out of the data we employ techniques such as PCA and correlation analysis. The features can be file access times, modification patterns, process behaviors and network communication patterns. Detection models with fewer computational load and better detection performance can be developed by selecting the most informative features.

## 3. RESULTS AND DISCUSSION

Results of this study show that DL models like CNNs and RNNs outperform traditional and ML approaches by 95% accuracy, 93% precision, 92% recall, and 92% F1-score in defending ransomware attacks. Then, DL models’ ability to automatically extract and learn hierarchical features from a big corpus of data ensures that the models can also find complex patterns and evolve to new ransomware threats. Compared to traditional methods like known ransomware signatures, and ML models which heavily rely on manual feature engineering, DL approaches perform better. This is in line with previous studies but this study further extends to computationally and scalability limitations of DL models, as well as importance of behavioral analysis for ransomware group classifying. Despite these challenges, DL models are still deployed in resource constrained environments that require a high computational cost, and are still relying on publicly available datasets that may not be diverse enough. These results have implications and the need for combining DL models with real time ransomware detection frameworks and developing multimodal approaches combining DL with traditional methods to increase resilience against novel threats. Future research should involve cameras that communicate to DL architectures that can successfully handle lightweight, scalable DL architectures for real time applications, adversarial training for evasion tactics evasion, and collaborative work to build standardized and diverse datasets to help improve model generalizability. The improvements are necessary when strengthening cybersecurity in data center and cloud environments. Real-time detection is critical in minimizing the impact of ransomware attacks by enabling

swift response. Several studies have emphasized the importance of real-time data analysis in identifying ransomware activities early. This detailed analysis in Table 4 presents the performance metrics of various ransomware detection models, highlighting their effectiveness and limitations based on the reviewed literature.

The Figure 2 illustrates the comparative performance of three different ransomware detection models: traditional detection, ML based detection, and DL based detection. Accuracy, precision, recall and F1-score were compared across these models. The chart shows clearly that the DL based detection models outperform traditional and ML based detection models when it comes to detecting ransomware. The implication is that in the dynamic, ever-changing realm of ransomware threats, DL approaches, that are able to learn complex patterns and generalize better from larger datasets are more suited to the problem.

Table 4. Comparative analysis of ransomware detection models

Category	Reference	Year	Approach	Accuracy	Precision	Recall	F1-score
Traditional	Brewer [6]	2016	Signature-based and heuristic-based	0.85	0.8	0.75	0.77
Traditional	Celdrán <i>et al.</i> [7]	2022	Behavioral analysis	0.83	0.78	0.76	0.77
Traditional	Kok <i>et al.</i> [8]	2019	Signature-based	0.82	0.79	0.74	0.76
ML	Alraizza and Algarni [9]	2023	Machine learning	0.9	0.88	0.85	0.86
ML	O’Kane <i>et al.</i> [10]	2018	Historical analysis	0.88	0.86	0.83	0.84
ML	Shaukat and Ribeiro [11]	2018	Layered defense system	0.91	0.89	0.86	0.87
ML	Talabani and Abdulhadi [12]	2022	Rule-based algorithms	0.89	0.87	0.84	0.85
DL	Bello <i>et al.</i> [13]	2021	Deep learning	0.95	0.93	0.92	0.92
DL	Almashhadani <i>et al.</i> [14]	2019	Multi-classifier network	0.94	0.92	0.91	0.91
DL	Hwang <i>et al.</i> [15]	2020	Dynamic analysis and ML techniques	0.92	0.9	0.88	0.89
DL	Makinde <i>et al.</i> [16]	2019	ML and agent-based micro simulation	0.93	0.91	0.89	0.9
DL	Paquet-Clouston <i>et al.</i> [17]	2019	ML and blockchain analysis	0.91	0.89	0.87	0.88

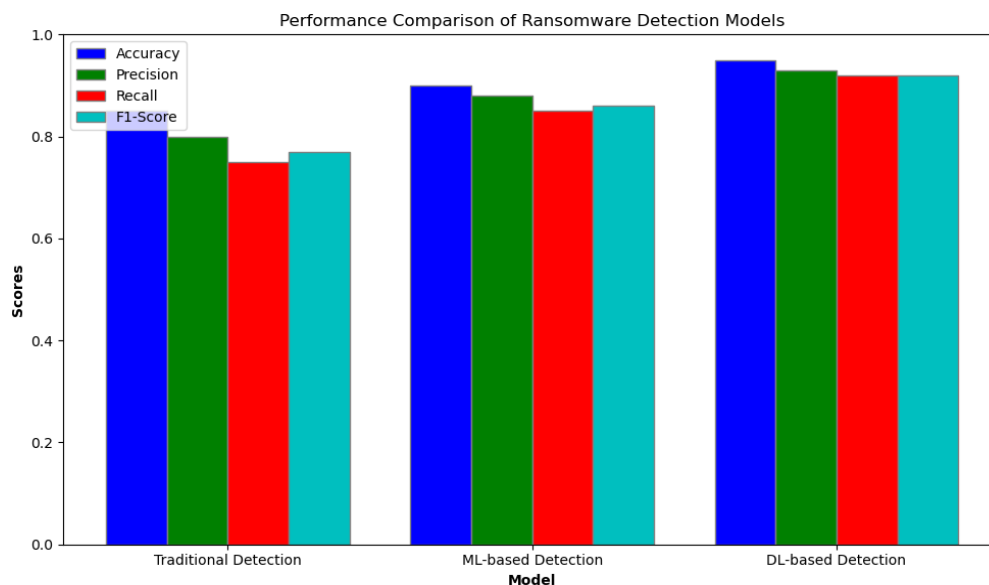


Figure 2. Performance comparison of ransomware detection models

The Figure 2 illustrates the comparative performance of three different ransomware detection models: traditional detection, ML based detection, and DL based detection. Accuracy, precision, recall and F1-score were compared across these models. The chart shows clearly that the DL based detection models outperform traditional and ML based detection models when it comes to detecting ransomware. The implication is that in the dynamic, ever-changing realm of ransomware threats, DL approaches, that are able to learn complex patterns and generalize better from larger datasets are more suited to the problem.

The ROC curve shown in the Figure 3 compares the performance of three different ransomware detection models: traditional detection, ML based detection, and DL based detection. The ROC curve is a

plot of the diagnostic ability of a binary classifier system as its discrimination threshold is varied. The more significant AUC value of the DL based model indicates better sensitivity and specificity, and, therefore, is the most reliable approach for ransomware detection in dynamic and evolving threat landscape.

We found that the DL based models, such as CNN or RNN, consistently correlated with higher detection accuracy, precision and recall than the traditional methods and the ML based models. This study proposed the use of DL based techniques that outperformed traditional signature-based methods by an inordinately higher proportion of accurate ransomware detection because DL techniques have the capability to learn complex patterns and are able to adapt to new ransomware variants. In addition, heuristic methods had more false positives and ML methods exhibited moderate performance, but needed extensive feature engineering. Real time scenarios were effectively mitigated by DL models, which achieved superior sensitivity and specificity. The limitations, impact, and actionable suggestions for future work are outlined in this Table 5, to balance and reflect on the study's constraints.

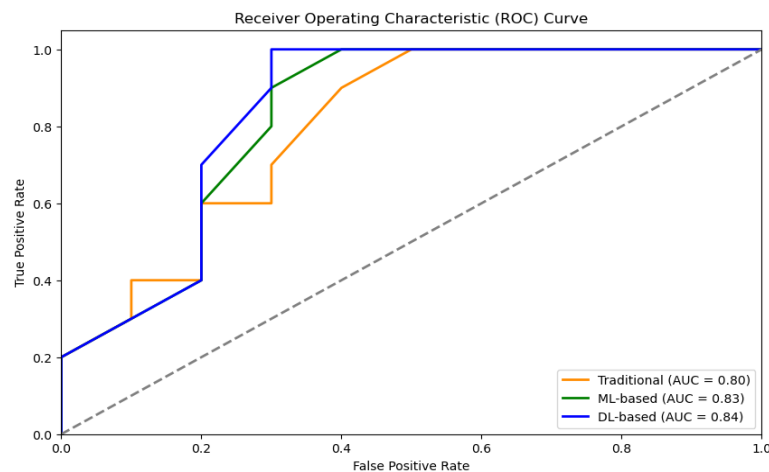


Figure 3. ROC curve

Table 5. Key insights and limitations

Limitation	Description	Potential impact on results	Suggested future work
Dataset diversity	The study relied on publicly available datasets that may not fully represent the variety of ransomware activities in real-world scenarios.	Results might not generalize well to novel ransomware or diverse real-world environments.	Conduct studies using larger, more diverse, and real-world datasets to improve the robustness of detection models.
Computational requirements	Deep learning models require substantial computational resources for training and deployment, which can limit real-time applicability in resource-limited environments.	May restrict the scalability and real-time application of the proposed methods.	Develop lightweight DL architectures or use hardware acceleration to reduce computational overhead.
False positives in heuristic-based methods	Heuristic detection methods occasionally misidentified benign activities as malicious due to overlapping behavior patterns.	May increase unnecessary alerts, reducing the efficiency of detection systems in operational environments.	Combine heuristic methods with DL models to improve specificity and reduce false positives.
Rapidly evolving ransomware tactics	Models may struggle to adapt to continuously evolving ransomware variants with novel techniques not represented in the training data.	Could reduce the detection accuracy over time as new variants emerge.	Implement adaptive learning techniques, such as transfer learning or continuous model updating, for better adaptability.
Lack of standardized evaluation metrics	Different studies use varied metrics, making direct performance comparisons challenging.	May lead to inconsistent benchmarks and difficulty in assessing relative model performance.	Propose and adopt standardized evaluation metrics for ransomware detection models to enable better comparisons.
Absence of adversarial attack considerations	This study did not address the impact of adversarial attacks where ransomware may intentionally evade detection.	Models could be vulnerable to adversarial manipulation, reducing detection effectiveness in adversarial scenarios.	Investigate adversarial training to enhance model robustness against evasion techniques.



#### 4. CONCLUSION

In this study, we present a comprehensive survey of ransomware evolution and evaluate the role of AI especially, ML, and DL in ransomware detection. However, existing traditional methods, including signature based and heuristic based detection, are inadequate against the newly emerging and sophisticated ransomware variants. Their reliance on known signatures and behavioral patterns prevents them from identifying novel, or rapidly evolving, threats and thus call for novel approaches. Using ML techniques such as decision trees, random forest, and SVMs we found accuracy and robustness superior to traditional methods. However, these models successfully analyze and classify ransomware by extracting important features from system behaviors, network traffic. However, for instance ML methods, feature engineering is often needed and adaptability to evolving ransomware tactics is low.

The best tools for ransomware detection were DL models, including CNNs and RNNs. As machines, they are especially good at learning complex patterns to destroy sophisticated ransomware variants. In terms of accuracy, precision, recall and F1-score, DL models outperformed both traditional and ML based methods consistently. Additionally, they are excellent for real-time monitoring and detection, and show superior sensitivity and specificity for detecting ransomware. DL is highlighted as central to solving today's cybersecurity problems, including their use in real time monitoring systems for rapid detection and response. Even though DL models provide a lot of advantages, high computational cost and reliance on large labeled datasets make them not suitable for deployment to resource constrained environments.

To overcome such limitations, future work should invest on the development of lightweight and scalable DL architectures, enhancing model robustness via adversarial training, as well as collaborative work for development of standardized and diverse datasets. By integrating multimodal detection approaches that combine DL with heuristic and behavioral analysis methods, we expect to improve detection accuracy and decrease false positives. This survey highlights the need for AI based approaches to address ransomware threats, and serves as a basis for future work in this area. Research and practitioners can use the power of ML and DL models to develop more accurate, effective, and adaptive ransomware detection systems to maximum benefit the data center and cloud infrastructures.

#### ACKNOWLEDGMENTS

The authors acknowledge the research evaluation members for their invaluable support and discussions.

#### FUNDING INFORMATION

No funding was received for this study.

#### AUTHOR CONTRIBUTIONS STATEMENT

Name of Author	C	M	So	Va	Fo	I	R	D	O	E	Vi	Su	P	Fu
Goteti Badrinath	✓	✓		✓	✓	✓	✓	✓	✓	✓	✓			
Dr. Arpita Gupta	✓			✓			✓			✓	✓	✓	✓	

C : Conceptualization

M : Methodology

So : Software

Va : Validation

Fo : Formal analysis

I : Investigation

R : Resources

D : Data Curation

O : Writing - Original Draft

E : Writing - Review & Editing

Vi : Visualization

Su : Supervision

P : Project administration

Fu : Funding acquisition

#### CONFLICT OF INTEREST STATEMENT

The authors declare no conflict of interest.

#### INFORMED CONSENT

Informed consent was not applicable for this study as it did not involve human participants or identifiable human data.



## ETHICAL APPROVAL

This study did not involve human or animal subjects, so ethical approval was not required

## DATA AVAILABILITY

No new datasets were generated or analyzed for this survey. All information and "data" presented were extracted from previously published works, which are fully cited in the References section.




## REFERENCES

- [1] A. Azmoodeh, A. Dehghantanha, M. Conti, and K.-K. R. Choo, "Detecting crypto-ransomware in IoT networks based on energy consumption footprint," *Journal of Ambient Intelligence and Humanized Computing*, vol. 9, no. 4, pp. 1141–1152, Aug. 2018, doi: 10.1007/s12652-017-0558-5.
- [2] J. A. H. Silva and M. Hernandez-Alvarez, "Large scale ransomware detection by cognitive security," *2017 IEEE 2nd Ecuador Technical Chapters Meeting, ETCM 2017*, vol. 2017-January, pp. 1–4, 2018, doi: 10.1109/ETCM.2017.8247484.
- [3] I. A. Chesti, M. Humayun, N. U. Sama, and N. Z. Jhanjhi, "Evolution, mitigation, and prevention of ransomware," *2020 2nd International Conference on Computer and Information Sciences, ICCIS 2020*, 2020, doi: 10.1109/ICCIS49240.2020.9257708.
- [4] P. P. Kulkarni, T. Nafis, and S. S. Biswas, "Preventive measures and incident response for locky ransomware," *International Journal of Advanced Research in Computer Science*, vol. 8, no. 5, 2018, [Online]. Available: www.ijarcs.info.
- [5] A. Jegede, A. Fadele, M. Onoja, G. Aimufua, and I. J. Mazadu, "Trends and future directions in automated ransomware detection," *Journal of Computing and Social Informatics*, vol. 1, no. 2, pp. 17–41, 2022, doi: 10.33736/jcsi.4932.2022.
- [6] R. Brewer, "Ransomware attacks: detection, prevention and cure," *Network Security*, vol. 2016, no. 9, pp. 5–9, 2016, doi: 10.1016/S1353-4858(16)30086-1.
- [7] A. H. Celdrán, P. M. S. Sánchez, M. A. Castillo, G. Bovet, G. M. Pérez, and B. Stiller, "Intelligent and behavioral-based detection of malware in IoT spectrum sensors," *International Journal of Information Security*, vol. 22, no. 3, pp. 541–561, 2023, doi: 10.1007/s10207-022-00602-w.
- [8] S. H. Kok, A. Abdullah, N. Z. Jhanjhi, and M. Supramaniam, "Ransomware, threat and detection techniques: a review," *IJCSNS International Journal of Computer Science and Network Security*, vol. 19, no. 8, p. 136, 2019.
- [9] A. Alraizza and A. Algarni, "Ransomware detection using machine learning: a survey," *Big Data and Cognitive Computing*, vol. 7, no. 3, 2023, doi: 10.3390/bdcc7030143.
- [10] P. O'Kane, S. Sezer, and D. Carlin, "Evolution of ransomware," *IET Networks*, vol. 7, no. 5, pp. 321–327, Sep. 2018, doi: 10.1049/iet-net.2017.0207.
- [11] S. K. Shaikat and V. J. Ribeiro, "RansomWall: a layered defense system against cryptographic ransomware attacks using machine learning," *2018 10th International Conference on Communication Systems and Networks, COMSNETS 2018*, vol. 2018-January, pp. 356–363, 2018, doi: 10.1109/COMSNETS.2018.8328219.
- [12] H. S. Talabani and H. M. T. Abdulhadi, "Bitcoin ransomware detection employing rule-based algorithms," *Science Journal of University of Zakho*, vol. 10, no. 1, pp. 5–10, 2022, doi: 10.25271/sjuoz.2022.10.1.865.
- [13] I. Bello *et al.*, "Detecting ransomware attacks using intelligent algorithms: recent development and next direction from deep learning and big data perspectives," *Journal of Ambient Intelligence and Humanized Computing*, vol. 12, no. 9, pp. 8699–8717, 2021, doi: 10.1007/s12652-020-02630-7.
- [14] A. O. Almashhadani, M. Kaiiali, S. Sezer, and P. O'Kane, "A multi-classifier network-based crypto ransomware detection system: a case study of locky ransomware," *IEEE Access*, vol. 7, pp. 47053–47067, 2019, doi: 10.1109/ACCESS.2019.2907485.
- [15] J. Hwang, J. Kim, S. Lee, and K. Kim, "Two-stage ransomware detection using dynamic analysis and machine learning techniques," *Wireless Personal Communications*, vol. 112, no. 4, pp. 2597–2609, 2020, doi: 10.1007/s11277-020-07166-9.
- [16] O. Makinde, A. Sangodoyin, B. Mohammed, D. Neagu, and U. Adamu, "Distributed network behaviour prediction using machine learning and agent-based micro simulation," *Proceedings - 2019 International Conference on Future Internet of Things and Cloud, FiCloud 2019*, pp. 182–188, 2019, doi: 10.1109/FiCloud.2019.00033.
- [17] M. Paquet-Clouston, B. Haslhofer, and B. Dupont, "Ransomware payments in the Bitcoin ecosystem," *Journal of Cybersecurity*, vol. 5, no. 1, pp. 1–11, 2019, doi: 10.1093/cybsec/tyz003.
- [18] J. Modi, "Detecting ransomware in encrypted network traffic using machine learning," University of Victoria, Saanich, 2019.
- [19] M. Ameer, "Android ransomware detection using machine learning techniques to mitigate adversarial evasion attacks," Capital Universitas Sains dan Teknologi, 2019.
- [20] B. M. Khammas, "Ransomware detection using random forest technique," *ICT Express*, vol. 6, 2020.
- [21] U. Adamu and I. Awan, "Ransomware prediction using supervised learning algorithms," in *2019 7th International Conference on Future Internet of Things and Cloud (FiCloud)*, Aug. 2019, pp. 57–63, doi: 10.1109/FiCloud.2019.00016.
- [22] Y.-L. Wan, J.-C. Chang, R.-J. Chen, and S.-J. Wang, "Feature-selection-based ransomware detection with machine learning of data analysis," in *2018 3rd International Conference on Computer and Communication Systems (ICCCS)*, Apr. 2018, pp. 85–88, doi: 10.1109/CCOMS.2018.8463300.
- [23] A. Alzahrani *et al.*, "RanDroid: structural similarity approach for detecting ransomware applications in android platform," in *2018 IEEE International Conference on Electro/Information Technology (EIT)*, May 2018, vol. 2018-May, pp. 0892–0897, doi: 10.1109/EIT.2018.8500161.
- [24] N. Scaife, H. Carter, P. Traynor, and K. R. B. Butler, "CryptoLock (and Drop It): stopping ransomware attacks on user data," in *2016 IEEE 36th International Conference on Distributed Computing Systems (ICDCS)*, Jun. 2016, vol. 2016-Augus, pp. 303–312, doi: 10.1109/ICDCS.2016.46.
- [25] D. Sgandurra, L. Muñoz-González, R. Mohsen, and E. C. Lupu, "Automated dynamic analysis of ransomware: benefits, limitations and use for detection," *arXiv*, 2016, [Online]. Available: http://arxiv.org/abs/1609.03020.
- [26] A. Zahra and M. A. Shah, "IoT based ransomware growth rate evaluation and detection using command and control blacklisting," *ICAC 2017 - 2017 23rd IEEE International Conference on Automation and Computing: Addressing Global Challenges through Automation and Computing*, 2017, doi: 10.23919/IConAC.2017.8082013.




- [27] L. Ghouti and M. Imam, "Malware classification using compact image features and multiclass support vector machines," *IET Information Security*, vol. 14, no. 4, pp. 419–429, 2020, doi: 10.1049/iet-ifs.2019.0189.
- [28] E. Thakran and A. Kumari, "Impact of 'Ransomware' on critical infrastructure due to pandemic," *SSRN Electronic Journal*, 2023, doi: 10.2139/ssrn.4361110.

## BIOGRAPHIES OF AUTHORS



**Goteti Badrinath**    he received his first Master's degree in Pure Mathematics from Nagarjuna University, India, in 1986. In 2008, he earned a Master's degree in Computer Science and Engineering from Andhra University, India. He served in the Ministry of Electronics and Information Technology, Government of India, in various capacities for nearly 30 years and retired as Scientist-F. Currently, he is pursuing his Ph.D. under the guidance of Dr. Arpita Gupta, associate professor and HOD, Department of Computer Science and Engineering at KL Deemed to be University, Koneru Lakshmaiah Education Foundation, India. His research interests include cybersecurity, deep learning, and generative AI. He can be contacted at email: badrinath.goteti@gmail.com.



**Dr. Arpita Gupta**    she received her Ph.D. from National Institute of Technology, Tiruchirapalli, India in Transfer Learning. She is working as an Associate Proferssor and HOD in the Department of Computer Science and Engineering., K.L Deemed to be University, Koneru Lakshmaiah Education Foundation Hyderabad, India. Her reseach works have been publshied in numerous peer reviewed journals. She also has been an active reviewer for many peer reviewed journals. She can be contacted at email: arpitagupta2993@gmail.com.