Journal of Theoretical and Applied Information Technology
31st May 2024. Vol.102. No. 10

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

# A REVIEW ON COGNITIVE BASED RANSOMWARE DETECTION USING MACHINE LEARNING AND DEEP LEARNING TECHNIQUES

**MR.M.S.BALAMURUGAN [1], DR.V.RAJENDRAN[2], DR.S.SUMA CHRISTAL MARY[3]**

[1]Associate Professor, Department of Electronics and Communication Engineering & Research Scholar of Vels University
[2]Director & Professor, Department of Electronics and Communication Engineering Vels University
[3] Professor, Department of Information Technology, Panimalar Engineering College

Corresponding Author :sumasheyalin@gmail.com

**ABSTRACT**

Ransomware attacks the most significant highly alluring dangers to cyber security throughout the modern era. Security software is frequently ineffective regarding extortion and zero-day spyware assaults; significant net breaches may cause considerable information loss. A competition for resources is being created by these assaults, which have become increasingly flexible and more capable of changing the way they appear. In this review article, the primary goal focusing on recent trends of ransomware detection routinely and possible directions for further research as well. This paper provides background information on ransomware, a timeline of attacks, and an overview of the virus. Additionally, it offers thorough analysis of current strategies for recognizing, averting, reducing, as well as recuperating from ransomware assaults. An additional benefit comprises an examination of studies conducted among 2016 to 2023. This gives booklover a current understanding of the most recent breakthroughs in ransomware detection and showcases improvements in techniques for preventing ransomware attacks.
**Keywords**- *Ransomware detection, Machine learning, Soft computing, Software Defined Network(SDN)*

## 1. INTRODUCTION

Some of the most critical cyber security concerns impacting enterprises currently the quick dissemination of ransomware attacks. In the last decade, ransomware has grown in popularity as a technique used by hackers to request compensation from victims in exchange seeking their decryption keys after securing the information they have provided. Every aspect within society have been affected by incidents involving ransomware, including government, educational institutions, and the financial along with medical sectors. Understanding the characteristics in attacks using ransomware, the manner in which they propagate, particularly the potential repercussions of becoming a target is vital considering the serious consequences implicated [1].

Cognitive science-based ransomware detection refers to the use of cognitive science principles and techniques to detect as well as mitigate such dangerous malware. A malicious program known as "ransomware" conceals the documents of a victim then requests an expense to unlock them. By leveraging cognitive science, which encompasses the study of human cognition and behavior, researchers and developers can create more effective detection mechanisms. This approach involves analyzing patterns, behaviors, and characteristics associated with ransomware attacks, as well as understanding the psychology and decision-making processes of both attackers and victims.

### 1.1 Research Challenges

The main research challenges comprises lack of knowledge about ransomware malware between users, illiterate regarding libraries of ransomware, deficiency in identification of malware also FPR. Potential study prospects involve growing into AESthetic, increasing RaaS assaults, border plus fog-assisted ransomware, which DeepFake ransomware, weaknesses with working remotely, even block chain-powered remedies.

The main intention of this review article is mentioned as follows:

- To provide widespread outline regarding ransomware malware risk site, examining how such malware gets increased which supportive for further researchers.
- Moreover existing architectural design for ransomware malware identification are discussed that helps various organization for preventing significant data from malware.
- Our goal is to assist people and businesses in strengthening their defenses towards ransomware attacks and decreasing the possible harm that such dangerous applications may inflict.
- In addition, how AI based approaches such as machine learning deep learning were employed for ransomware detection, SDN based malware detection are explained.
- Since ransomware protection as well as rehabilitation is becoming more and more complicated, ransomware preventative measures are particularly successful but require specialist attention.
- Existing work resolves several issues by preventing specific malware only hence this review provides comprehensive overview that makes further investigation much easier in predicting ransomware malware.

### 1.2 Contribution

In this review, the author contributed as follows:

Cognitive science-based ransomware detection systems may utilize machine learning algorithms to identify and classify ransomware-related activities. These algorithms can be trained on large datasets of known ransomware behaviors and patterns, allowing them to recognize and flag suspicious activities in real-time. Additionally, cognitive science principles can be applied to enhance user awareness and education about ransomware threats. By understanding how individuals perceive and respond to potential risks, security measures can be designed to effectively communicate the dangers of ransomware and encourage safe online practices.

It is important to note that while cognitive science-based approaches can improve ransomware detection, they are not foolproof. Cybercriminals constantly evolve their tactics, making it necessary to continually update and refine detection systems to stay ahead of emerging threats.

Overall statistics concerning ransomware malware [2] during the year 2020 to 2022 depicted as figure 1.

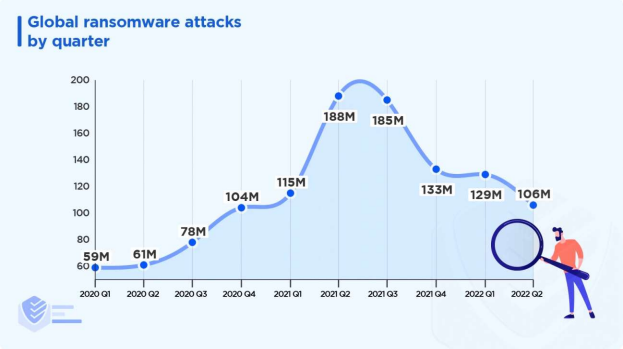


*Figure 1. Overall Statistics Regarding Ransomware During 2020 To 2022*

Several countries such as United States, United Kingdom, Canada, Germany, France, Australia, Japan, and Brazil were targeted by the gang of ransomware attackers. With nearly 51% of all cases, the United States remains among the globe's top victim for ransomware assaults during the year 2021. Hence, this research focused on finding ransomware malware based on cognitive science by which various IT sectors, institutions, human resources were prevented from such kind of malware [3].

## 2 BACKGROUND

The technique of finding malware by human assessment along with involvement as contrasted with technology that is automated is known as "manual ransomware detection." By examining computer logs, internet activity, and various other signs of penetration, this method looks for patterns of activity linked to malware assaults. Although traditional detection might be laborious and highly resource-intensive, it can serve as a useful backup to automatic detection procedures by assisting in the identification of novel or unidentified ransomware strains that automated equipment might miss. Although

automated identification of ransomware is successful, it does have certain drawbacks. It takes effort to avert ransomware due a number of factors. Risky software operates in a similar manner to ransomware, acting surreptitiously. Thus, at this point, identifying ransomware with attacks with zero-day vulnerabilities becomes essential. Kapoor et al. [4] detailed overview on detection and classification of ransomware, how such attacks are evaded with the help of Detection Avoidance Mitigation method along with traditional techniques for identifying such attacks including evolution from 1989 to 2020 shown in figure 2. Moreover, methodologies of most recent ransomware strains and offer some recommendations for halting their dissemination were demonstrated, an empirical investigation into highly notorious Djvu extortion were included.

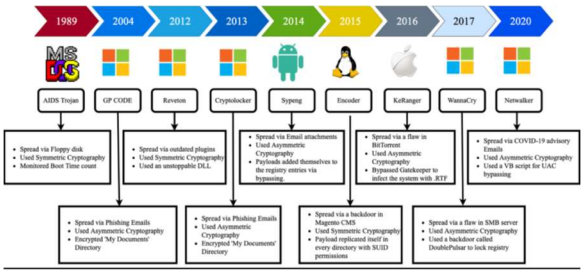


*Figure 2. Ransomware Evolution During 1989 To 2020*

### 2.1 Ransomware- Survey

Amjad et al. [5] reviewed several articles from 2017 to 2021 for ransomware attack detection, avoidance and upcoming confronts were discussed shown in figure 3.

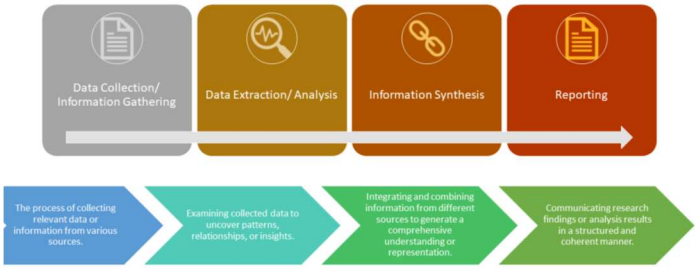


**Figure 3. Framework designed by Amjad [] for ransomware detection**

### 2.2 Kinds of ransomware during 2016-2023

Various kinds of ransomware based malware were identified from 2016 to 2023 are listed in table 1.

*Table 1. Kinds Of Ransomware 2016-2023*

| Month& Year | Kind of Ransomware | Narrative |
|---|---|---|
| Jan 2016 | Ransom32 | This malware affects windows and MacOs. |
| February 2016: | Locky | Phishing emails containing malicious macros in Word or Excel attachments were sent by the Locky ransomware via the Necurs botnet. On Windows OSes, files were encrypted. |
| March 2016: | SamSam | Once the targets have been identified, attackers employ both legal Microsoft utilities along with brute-force techniques for infecting particular computers. Digital currency compensation is required once the malicious software has taken effect. |
| April 2016 | Jigsaw | It crashes the system by sending malicious emails. |
| June 2016: | Zcryptor | This kind of malware affects the network and devices which are connected externally. |

| | | |
|---|---|---|
| September 2016: | Mamba | A genuine DiskCryptor encrypted software has been employed by Mamba, additionally referred to as HDDCryptor, a malware infection that encrypted disks and propagated throughout the system. |
| January 2017: | Spora | Propagates via infected zipped documents seen in emails that are phished. |
| May 2017: | Jaff | Jaff disseminated approximately five billion phishing messages daily using the Necurs network. |
| May 2017: | WannaCry/ WannaCrypt | Throughout a worldwide assault targeting more than 150 countries early May 2017, WannaCry was utilized. It was revealed in May 2019 that the malicious software had infected about 5 million susceptible machines. |
| June 2017: | Goldeneye | Spyware was used to propagate it any longer, resulting in encrypts information. |
| 2017 June | Not Petya | This Petya variation was named. Although Non-Petya is classified as the threat of ransom its primary objective being wiper ware is to delete information instead of obtaining payment. |
| 2017 Oct | Bad Rabbit | This malware encodes the MBR by taking advantage of Eternal Blue. A notice requesting a value of the digital currency displays upon a compromised computer. The payment amount rises when individuals fail to respond inside a forty-hour period. |
| 2018 Jan | Gand Crab | For purposes of confidentiality, it made the utilization of a.bit the highest positions realm that has not been authorized per the World Wide Web Organization over allocated names as well as Statistics. |
| 2018 August | Ryuk | This prevented victims from recovering either additional recovery with reversal technologies. |
| April ‘19 | Revil | Prior to Gand Crab's retiring, both of these variants shared a great deal in common thus worked jointly upon targets' computers during earliest attempts. |
| May ‘19 | Maze | Propagate through vulnerability items, assaults, including email viruses. This is among the initial instances using blackmail that uses twofold abduction. |
| May 2019: | Robbin Hood | This malware gains access to consumers' workstations via RDP assaults, worms, spamming tactics, and vulnerabilities within Motherboard LINUX drivers. Utilities plus defensive apps have to be turned off, connections to networks are disconnected, replicas of themselves are removed, plus Microsoft automated restoration is turned off. |
| December 2019: | Tycoon | This malware may conceal over decades then deactivate antivirus applications while encryption storage devices then requesting a monetary reward. |
| 2020 Aug | Dark Side | Amongst various covert methods, it employs complex concealment approaches, multiple extortion attempts, as well as management and oversight. |
| September 2020: | Egregor | A kind of double-crossing malware where its targets are humiliated in front of everyone. |

| | | |
|---|---|---|
| June '21 | RanHive | This malware collective first surfaced from the middle of the past year, attacking stores, IT firms, essential systems, including medical facilities. |
| November 2021: | Black Cat | This also happened to be among the earliest variants that combined a denial of service (DDoS) element with quadruple ransom tactics. |
| December 2021: | Lapsus | This malware communicates via others in the community, its perpetrators, and possible employees via an online chat service. |
| January 2022: | Royal | To evade being discovered via antivirus software and various other surveillance tools, Royalty encodes tiny quantities malware information. This makes malware to safeguard fewer messages, which speeds up the execution of assaults. |
| April 2022: | Black Basta | This malware employs the banking Malware with Printer Nightmare vulnerabilities in addition to increase the exploitation malware. |
| June 2022: | LockBit 3.0 | "Make Ransomware Great Again." |
| April 2023: | Rorschach | Considering how quickly it encrypts data, its latest version is among the quickest we've yet seen. |

The framework developed by the author for ransomware attack identification is depicted as figure 4.

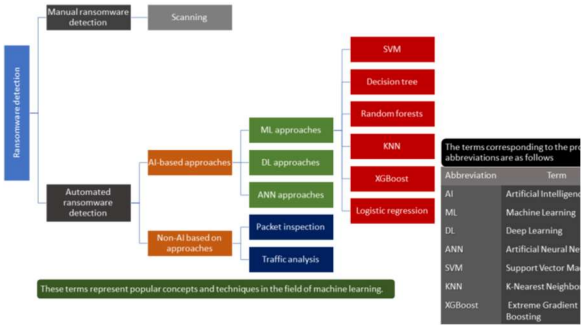


*Figure 4. Framework For Ransomware Identfication*

Craig et al. [6] examined current developments in ransomware detection and avoidance moreover pointed out prospective areas of such kind of malware was studied along with their issues. In addition, researchers conducted an investigation of several well-known examples of ransomware before developing AESthetic, a prototype malware which managed to avoid recognition by eight well-known antivirus apps.

Daniele et al. [7] analyzed ransomware malware by expressing their pros and cons, in addition usage of ransomware malware recognition. Also, a novel machine based model were introduced namely EldeRan which detects certain features of ransomware virus vigorously, classified too Ramesh et al. [8]. Such advanced learning method observed some tasks executed by apps while initial fixing which examine ransomware feature indication.

The authors of Jaeyun et al. [9] established the effectiveness of various behavior-based ransomware countermeasures, encompassing either for-profit or scholarly offerings. Additionally, some malware evasion methods which supervise certain ransomware behaviors superimpose with non-malicious one.

## 3. Techniques based AI

Several techniques such as machine learning, Artificial Neural Networks and deep based learning had employed for ransomware attack recognition automatically. Such behavioral approaches train the data to examine patterns as well as behaviours for detecting ransomware attacks. Conversely, deep based learning approaches train the neural networks for identifying ransomware attacks through examining huge quantity of industrial metadata.

Likewise, ANN approach helps in attack recognition as a result of evaluating metadata resources. Hence, techniques based on AI provides effective, trustworthy method for finding and averting ransomware attack leads to reduction of risks on various industries.

### 3.1 Machine based Ransomware

Abdullahi et al. [10] analyzed seven kinds of ransomware malware using machine based learning methods which is mentioned in figure 5.

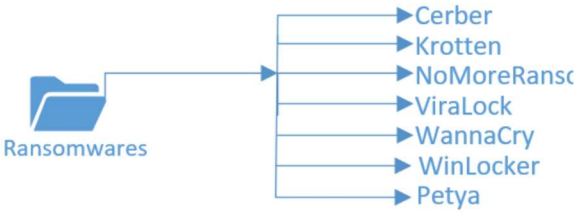


*Figure 5. Kinds Of Ransomware Detected By*

Here the authors gathered data relevant to ransomware malware which are fed into machine learning algorithms that train the data to detect ransomware malware based on classification approaches. Using the Microsoft Windows computer, researchers installed viruses, ransomware, and reputable applications. The information collected about ransomware, spyware, and reliable equipment can be transferred onto Ubuntu computer using the Python programming language.
Azka et al. [11] introduced new detection approach which identified ransomware malicious malware on IoT subsequent to detailed knowledge relevant to that domain. Here, the introduced method observes IoT based traffic made while data entering via SDN in which the controller helps in identification and enhancement of ransomware based IoT.

Initially the authors of Jagsir et al. [12] examined both malicious and non-malicious data samples via analyzing methods namely static and dynamic. From this analysis, exclusive characteristics have taken for differentiating malicious from non-malicious one. Subsequently, machine based classification techniques were utilized for ransomware malware labeling in efficient manner depends on the performance of machine learning classification models. The developed framework for ransomware detection via behavioral analysis along with its classification using machine learning models depicted as figure 6.

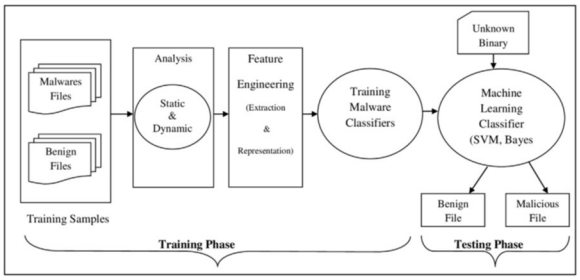


*Figure 6. Developed Architectural Design Using ML*

### 3.2 Ransomware identification with deep learning

Poudyal et al. [13] applied suitable AI based techniques such as machine and deep based models for finding and recovering malicious behaviors. Also, comparison made to express existing work deficiency, the methods to enhance effectiveness in detection of ransomware malware. Malware classification architecture proposed by this author illustrated as figure 7.

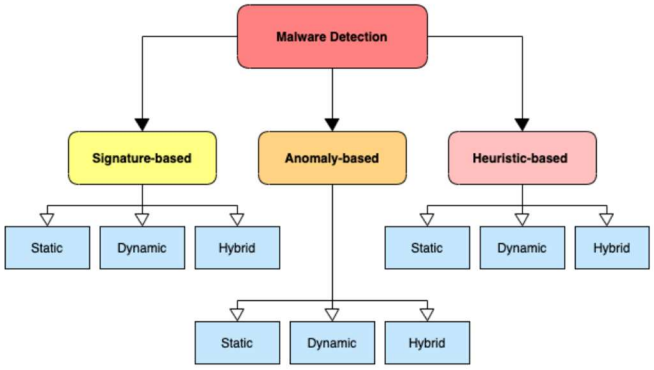


*Figure 7. Kinds Of Malware Detected By*

Khaled et al. [14] intended optimal machine learning with AA (Artificial Algae) method based machine and deep approaches for ransomware detection to secure data. The framework for identification of such malware is depicted in figure 8.

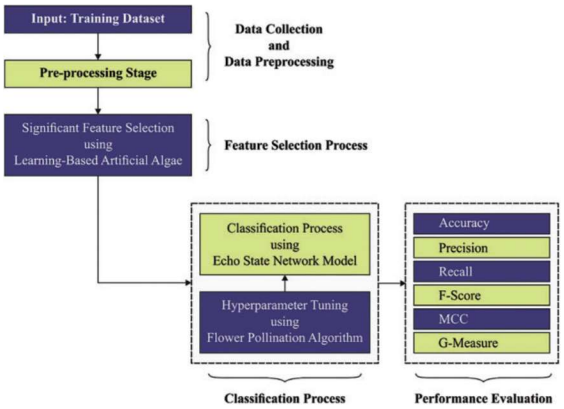


*Figure 8. Ransomware Detection Using ML Model []*

This work comprises four stages namely i) Data collection and Preprocessing- data samples have gathered from open source and preprocessing has done to extract only relevant features. ii) Features Selection- The features chosen using Artificial Algae method to select features/ characteristics of ransomware malware iii) Classification Process – During this phase echo state network were employed to perform classification moreover the parameters are tuned with flower pollination algorithm iv) Performance Evaluation- Finally the performance of classification model were evaluated in terms of accuracy, precision, recall, f-score, MCC and G-measure.

Kirubavathi et al. [15] detected ransomware based android malware on 331 features data samples via feature selection approach in addition malware classification has done via machine learning classification algorithms as Gradient Boosting, Decision tree and extra tree. In conclusion, the performances of classifiers were evaluated based on various measures such as precision, recall and classification accuracy. The architectural framework designed by this author shown in figure 9.

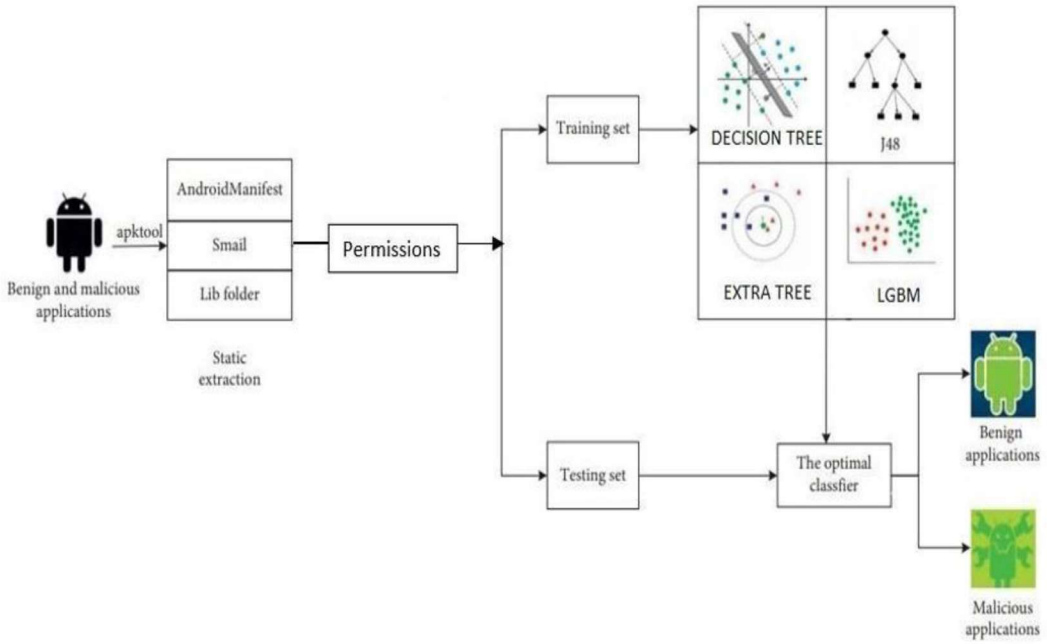


*Figure 9. Overview Of Ransomware Identification*

Mohammad Masum et al. [16] utilized machine based models such as logistic regression, naïve bayes, random forest, decision tree and neural network for ransomware malware categorization in which random forest method attains greater accuracy performance.

## 4. COGNITIVE BASED RANSOMWARE IDENTIFICATION

Juan et al. [17] aimed to create an approach for recognizing and avoiding the spread of cyberattacks using technologies to analyze, acquire knowledge, or comprehend intelligence regarding security in order to spot correlations

along with suspect activity. Overall framework proposed for ransomware detection, classified and validated to attain the performance of applied models depicts in figure 10.

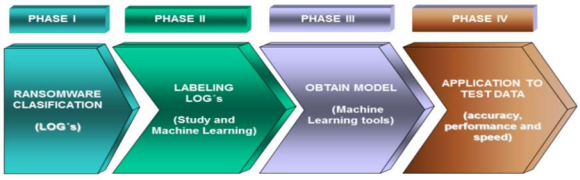


*Figure 10. Cognitive Based Ransomware Detection*

Moreover, EcuCERT data were analyzed to identify features of ransomware by which machine learning techniques provides effective and secure data maintenance supportive to various organization.

During the year 2020, percentage increases in risk of ransomware are described by Andrade et al. [18]. In America, 3% malware increased, whereas in Europe 4% raised and Asia country malware affected increased 6%. Through examining basic ideas for using cognitive technologies within information security, this work seeks to create a Cognition Cybercrime Platform.

## 5. SDN BASED RANSOMWARE DETECTION

Krzysztof et al. [19] identified the use of Software-Defined Networking (SDN) to enhance a ransomware reduction. Specifically, the characteristics of well-known malicious software called Crypto Wall along with information using mitigation approaches. After that, the authors designed an SDN-based system which was implemented using OpenFlow, most significant because it allows for a timely response to this threat moreover crucial in case of crypto ransomware while sustaining minimal impact regarding the network's overall functionality. Finally, the experimental findings verify the viability and effectiveness of the suggested technique.

Maxat et al. [20] identified and prevented ransomware malware via software defined network in which OpenFlow controller comprise switches controls while malevolent traffic entered. Ransomware namely WannaCry characteristics was analyzed both statically and dynamically. The architectural framework designed by this author depicted in figure 11.

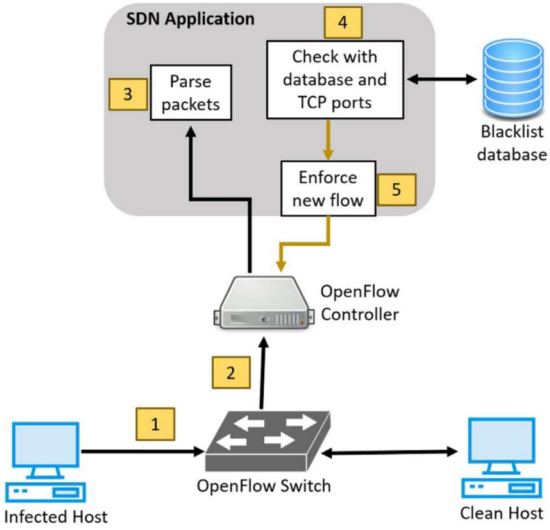


*Figure 11. Detection Of Ransomware Using SDN Approach*

Umar et al. [21] prevented ransomware malware with the help of RYU controller controls the incoming malicious data also virtual switch attached useful while non-malicious data entered. All happened in Software Defined Network which enhances secure information. Moreover, soft computing techniques were used for malware especially ransomware detection based on feature extraction automatically Nabeel et al. [22]. Revathy et al. [23] detected data traffic based malware in SDN network where SDN controller controls/blocks malicious entry whereas switches exchanges data that are malicious and non-malicious.

## 6. CONCLUSION

Malware known as "ransomware" encrypts personal information on their device, rendering it unreadable until they decode it. This effectively keeps the target's stuff captivity. Recent improvements in wannacry evaluation, recognition, plus protection have been examined throughout this article. Subsequently it was discovered revealed honeypots, monitoring network traffic, along with machine learning-inspired strategies are the main focuses of the majority of recent ransomware methods for detection. The majority of prevention methods concentrated on hardware-driven remedies, information and credential safeguards, as well as entry restriction. Nonetheless, it appears that

utilizing techniques based on machine learning to identify malware is becoming more popular.

## REFERENCES

[1] S. Alsoghyer and I. Almomani, ''Ransomware detection system for Android applications,'' Electronics, vol. 8, no. 8, p. 868, Aug. 2019.

[2] https://www.antivirusguide.com/cybersecurity/ransomware-statistics/

[3] https://www.techtarget.com/searchsecurity/feature/4-types-of-ransomware-and-a-timeline-of-attack-examples

[4] Kapoor, A.; Gupta, A.; Gupta, R.; Tanwar, S.; Sharma, G.; Davidson, I.E. Ransomware Detection, Avoidance, and Mitigation Scheme: A Review and Future Directions. Sustainability 2022, 14, 8. https://doi.org/10.3390/su14010008

[5] Alraizza, Amjad.; Algarni, A. Ransomware Detection Using Machine Learning: A Survey. Big Data Cogn. Comput. 2023, 7, 143. https://doi.org/10.3390/bdcc7030143

[6] *Craig Beaman* et. al. "Ransomware: Recent advances, analysis, challenges and future research directions", Computers & Security 111 (2021), 102490.

[7] Daniele Sgandurra "Automated Dynamic Analysis of Ransomware:Benefits, Limitations and use for Detection", arXiv:1609.03020v1 [cs.CR] 10 Sep 2016.

[8] Ramesh, Gowtham; Menen, Anjali (2020). *Automated dynamic approach for detecting ransomware using finite-state machine. Decision Support Systems, 138(), 113400–.* doi:10.1016/j.dss.2020.113400

[9] Jaehyun Han "On the Effectiveness of Behavior-Based Ransomware Detection", SecureComm 2020, LNICST 336, pp. 120–140, 2020.https://doi.org/10.1007/978-3-030-63095-9_7.

[10] Arabo, A., Dijoux, R., Poulain, T., & Chevalier, G. (2020). *Detecting Ransomware Using Process Behavior Analysis. Procedia Computer Science, 168, 289–296.* doi:10.1016/j.procs.2020.02.249

[11] Azka Wani "Ransomware protection in IoT using software defined networking", International Journal of Electrical and Computer Engineering (IJECE) · February 2020 DOI: 10.11591/ijece.v10i3.pp3166-3175

[12] Jagsir Singh, Jaswinder Singh, *Journal of Systems Architecture*, https://doi.org/10.1016/j.sysarc.2020.101861

[13] S. Poudyal, D. Dasgupta, Z. Akhtar, and K. D. Gupta, "Malware analytics:Review of data mining, machine learning and big data perspectives,"12 2019.

[14] Khaled M. Alalayah "Learning-Based Artificial Algae Algorithm with Optimal Machine Learning Enabled Malware Detection", Computer System Science and Engineering, DOI: 10.32604/csse.2023.034034.

[15] Kirubavathi G "Behavioural Based Detection of Android Ransomware Using Machine Learning Techniques", DOI: https://doi.org/10.21203/rs.3.rs-2555218/v1.

[16] Mohammad Masum "Ransomware Classification and Detection With Machine Learning Algorithms"

[17] Silva, Juan A. Herrera; Hernandez-Alvarez, Myriam (2017). [IEEE 2017 IEEE Second Ecuador Technical Chapters Meeting (ETCM) - Salinas, Ecuador (2017.10.16-2017.10.20)] 2017 IEEE Second Ecuador Technical Chapters Meeting (ETCM) - Large scale ransomware detection by cognitive security. , (), 1–4. doi:10.1109/ETCM.2017.8247484

[18] Andrade, R.O.; Fuertes,W.;Cazares, M.; Ortiz-Garcés, I.; Navas,G. An Exploratory Study of Cognitive Sciences Applied to Cybersecurity. Electronics 2022, 11, 1692. https://doi.org/10.3390/electronics11111692

[19] Krzysztof Cabaj, "Using Software-Defined Networking for Ransomware Mitigation: the Case of CryptoWall", https://doi.org/10.48550/arXiv.1608.06673

[20] Maxat Akbanov "Ransomware detection and mitigation using software-defined networking: The case of WannaCry", Computers and Electrical Engineering 76 (2019) 111–121, https://doi.org/10.1016/j.compeleceng.2019.03.012

[21] Rusydi Umar "Mitigating Ransomware Attack on Cloud Network using Software Defined Networking (SDN)", International Journal of Safety and Security Engineering, Volume 11, No 3, 2021, pp 239-246.

[22] Albishry Nabeel, AlGhamdi R, Almalawi A, Khan AI, Kshirsagar PR, BaruDebtera. An Attribute Extraction for Automated Malware Attack Classification and Detection Using Soft Computing Techniques. Comput Intell Neurosci. 2022 Apr 25;2022:5061059. doi: 10.1155/2022/5061059. PMID: 35510059; PMCID: PMC9061036.