International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING
ISSN:2147-6799 www.ijisae.org Original Research Paper

A Signature- based Ransomware Detection and Automated Data Backup to Safeguard the System from Ransomware Attack

[1]Srijita Bhattacharjee, [2]Dr. Dhananjay Dakhane

Submitted: 31/12/2023 **Revised**: 07/02/2024 **Accepted**: 15/02/2024

Abstract: Ransomware attacks have developed as a serious cybersecurity concern, causing significant financial losses and data breaches in a variety of industries. To tackle this threat, a reliable and efficient detection system is essential. To improve protection against ransomware assaults, a ransomware detection mechanism coupled with an automated backup method is proposed in this paper. To identify and isolate malicious code, our system uses signature-based analysis, leveraging a large database of known ransomware signatures. The system can quickly identify files by comparing them to these signatures of ransomware, allowing for quick response and backup. This method is successful in recognising known ransomware variants with high accuracy. In addition, the incorporation of an automated backup process supplements the detection system by maintaining data integrity and availability. When Ransomware samples are detected, the system immediately creates backups in secure storage. The ability to swiftly restore affected files from the backup repository reduces the motivation for attackers to demand ransom payments in the case of an attack involving ransomware.

Keywords: *Ransomware, Automated backup, Signature-based analysis, Ransomware variants, Backup.*

1. Introduction

The data or computer systems can be made inaccessible to authorised users by the ransomware using encryption. Ransomware attacks employ strategies, techniques, and processes while locking the systems or encrypt data and which are difficult to reverse. sensitive information from victims' computers and network infrastructure can be stolen due to the ransomware attack. Ransomware attacks could potentially target individual computers, corporate network and industrial automation systems [1]. Ransomware attacks have increased in recent years, posing a serious danger to the security, integrity, and availability of crucial data on a worldwide scale, harming individuals, organisations, and institutions.

This investigation delves deeply into this complicated cybersecurity dilemma and proposes a novel and strategic plan that blends signature-based ransomware detection with automatic backup systems. As the digital world evolves, the threat of ransomware has become more complex and ubiquitous, making it critical to handle this issue completely. Our investigation digs into the ever-changing world of cyber dangers, providing light on their varied nature as well as the rising sophistication of ransomware assaults [2]. The necessity of protecting data assets against these insidious attacks cannot be emphasised, hence we focused our study on the combination of signature-based detection algorithms with automatic backup procedures. This integrated strategy has the potential to greatly improve our collective cybersecurity defences, allowing us to proactively resist ransomware threats and, as a result, safeguard the digital infrastructure that underlies our modern way of life. This endeavour seeks to contribute valuable insights to the ongoing discourse surrounding the protection of our digital domains in the face of constantly evolving and increasingly sophisticated cyber threats by conducting an in-depth analysis of this methodology and its far-reaching implications. In this age of digital mutual dependence, the security of our data assets remains a top priority, and our objective is to provide a comprehensive and proactive solution to this long-standing difficulty.

Ransomware is appealing to thieves due to a number of characteristics. The first is ubiquitous internet use, which enables worldwide connectivity [3]. While this improves communication convenience, it also increases the possibility of cross-border cyberattacks. The second cause is the growing adoption of digital currencies such as the widely used bitcoin [4]. Because of bitcoin, which allows the owner to stay anonymous and makes it difficult for investigators to track down, the hacker has a secure method to obtain the ransom payment. The third element is an inclination for digital data storage. Nowadays, everyone is urged to keep data digitally rather than on paper. The fourth factor is the encryption algorithm's difficulty, availability, and significance. Encryption is a critical security approach that is utilised to achieve security goals [5]. In the case of

[1]Department of Computer Engineering, Ramrao Adik Institute of Technology, D.Y. Patil Deemed to be University Nerul, Navi Mumbai, 400706, Maharashtra, India, Department of Computer Engineering, Pillai HOC College of Engineering and Technology, University of Mumbai srijitacseengg2007@gmail.com
[2]Department of Computer Engineering Ramrao Adik Institute of Technology, D.Y. Patil Deemed to be University Nerul, Navi Mumbai, 400706, Maharashtra, India dhananjay.dakhane@rait.ac.in

ransomware, encoding is used to grab data from users and demand payment. The fifth feature is the simplicity with which ransomware may be distributed. The dark internet includes a ransomware creation kit that may be downloaded for free or purchased for a small fee. All of the aforementioned causes contributed to the proliferation and further growth of ransomware by hackers.

The research endeavour is motivated by the need to confront the expanding threat of ransomware in our increasingly digitalized environment. This study investigates and proposes a new technique that blends signature-based ransomware detection with automated backup solutions. This study has three aims. The initial goal of this project is to develop an early detection system capable of preventing or at least reducing the harm caused by a ransomware assault. The second goal of this study is to create a database of ransomware signatures. This database provides essential information on all ransomware discovered during this study, as well as ransomware identification. The hash value is created by the SHA-256 (Secure Hashing Algorithm) for the ransomware identification. We have utilized SHA-256 as it creates a compact and unique identifier. The Third aim is to create and deploy an automatic backup system to backup vital files and data on a regular basis. Backup policies, such as backup frequency, retention periods, and backup locations need to be included.

In order to achieve the aforementioned goals, the following contributions were made. The first contribution is to create a signature-based ransomware detection. The second contribution is an improved ransomware signature database, which will aid future study employing signature matching. The third contribution is to enable users to restore files from backups in case of a ransomware attack or accidental data loss. The data Backup is encrypted to protect the data from the cyberattack.

This study is further structured in that the second component is a review of previous research and identification of research needs. In the third section, we have presented the methodology and system workflow. The fourth section describes the experimental results and analysis, while the fifth portion offers suggestions for potential future research directions. Finally, we conclude our research work in six section.

2. Related Work

Ransomware encrypts data or computer systems, making them inaccessible to unauthorised users. Ransomware attacks lock computers or encrypt data, using methods, techniques, and procedures, making them difficult to reverse. From the victims' PCs and network infrastructure they may also obtain sensitive information. Ransomware assaults might target individual computers, commercial networks, or industrial control systems. Furthermore, we highlight the range of sensors used by Internet of Things customers [6]. A ransomware attack prevents authorised users from accessing a system or data using encryption process, until a ransom is paid. The victim can obtain the decryption key as soon as the attacker confirms that the ransom has been paid [7]. Various cyber security approaches and procedures are offered to decrease the threat of ransomware [8], and ransomware detection and prevention techniques have been studied [9]. To identify zero-day attacks caused by ransomware, monitor file system behaviour for I/O requests and secure the file [11]. Most malware, including ransomware, necessitates conventional precautions such as training for users and management of networks. Users may avoid ransomware by taking cautious precautions [10]. Mitigation, such as backup systems, is a popular recommendation in ransomware literature [12]. Data backup is regarded as the most effective approach for mitigating ransomware loss [13]. Ransomware necessitates early identification since it encrypts files and we lose the data until a ransom is paid. Techniques for countering ransomware assaults at an early stage must exist. Existing antivirus mostly employ signature-based detection methods, which are quick and accurate but may be too inflexible to identify zero-day threats [14]. Due to hackers' significant interest in ransomware, a new sort of ransomware that can circumvent antiviruses emerged at a quick pace [15]. Furthermore, Ransomware-as-a-Service [16], has been promoted as a service of ransomware, providing it easy access to a non-technical person with malicious intent. Based on this, it is clear that ransomware has reached alarming levels., establishing a coordinated mechanism among criminals, both computer adept and non-computer capable.

There are primarily two forms of analysis used to better understand the behaviour of ransomware: static analysis and dynamic analysis. Ransomware does not need to be executed in static analysis. In static analysis, the source code is examined so it is considered safer. The operation code is extracted from the source code and used to generate a sequence of n-gram codes [17]. Machine learning algorithms can be used to learn this pattern of n-gram codes to produce a predictive model for ransomware detection [18]. The ransom message [19] can be located, which might be in the source code or loaded after the encryption process is complete. The third technique involves getting a portable executable file’s header [20]. Another technique directly derives rules from source code using a formal mechanism [23]. The downsides of static analysis are that it is susceptible to trickery and that the original source of code being reviewed may be insufficient. The ransomware must be triggered in dynamic analysis [21], but in a confined environment known as the sandbox, which permits direct engagement and study of its behaviour. This is more reliable, but there is a chance that the ransomware will infect the host machine or that the

ransomware will become dormant once it realises it is in a sandbox. Tracking I/O operations allows you to watch the file system's actions [22] based on the fact that encryption requires recurrent file system activity. The encryption frequency can be monitored in order to discourage legal use and potential ransomware attacks [24]. The dynamic runtime opcode can be used to trace to carry out specific tasks [25]. The system API can be monitored because it monitors ransomware interactions with the operating system [26]. RansomWall builds a multi-layered detection and prevention mechanism by combining two types of analysis [27]. The intricacy of this may impede its implementation. Researchers offered many preventive strategies, including a layer of authentication to limit access to essential files [29], proactive monitoring of key directories, trapping using honeyfiles [28], and alertness to circumstances.

According to our literature review, we feel it is vital to detect ransomware as early as possible in order to do a minimal amount of damage to the victim's system. Even when the ransomware has been eliminated from the victim's PC, this remains true. Therefore, we proposed a solution to address this pressing issue by focusing on ransomware detection using signature and automated backup for the system data.

3. Methodology

As indicated in the aims section previously, this research had three objectives. We constructed our system workflow as illustrated in Fig.1, to meet all of these goals.

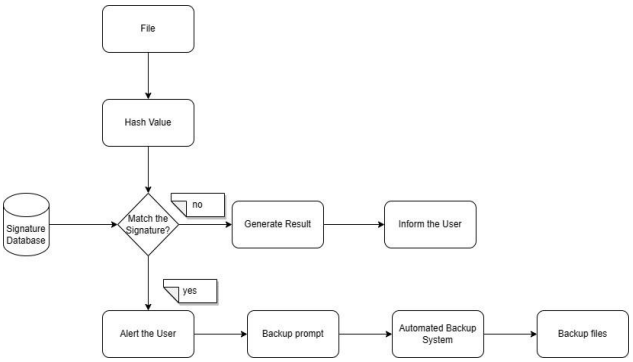

Fig. 1. Workflow of the system

There are four major areas of research activity: Sample, Hash Computation, Signature Database, Backup System, as illustrated in Fig. 2.

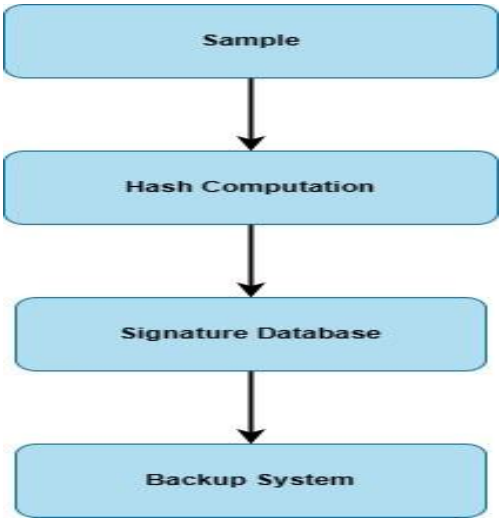

Fig. 2. Research framework

A. Sample

We started this investigation by obtaining samples from VirusShare (VS). We got additional samples of ransomware from the VS and Zoo (TZ) sources to keep our work up to date. VS is a malware archive that has made its contents public to researchers in security, incident management teams, forensic scientists, and anyone who are simply inquisitive. To utilise this repository, users must first register and be validated by the website's administrators. TZ is a GitHub open access repository containing malware. There are no restrictions on who can get samples from this repository. We have obtained a total of 38,157 ransomware samples.

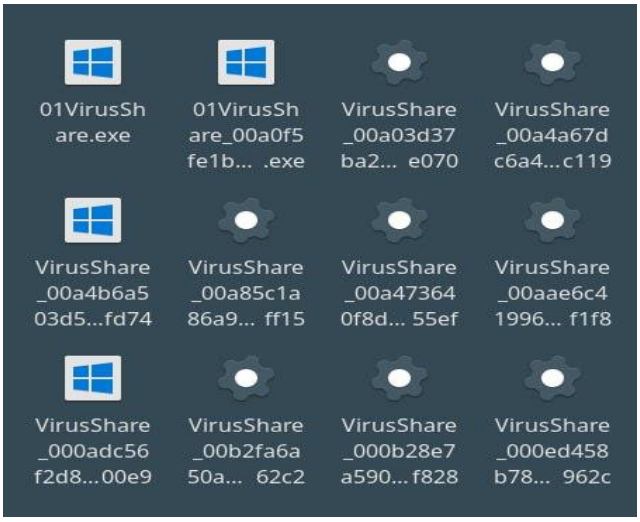

Fig. 3. Samples collected from VS repository

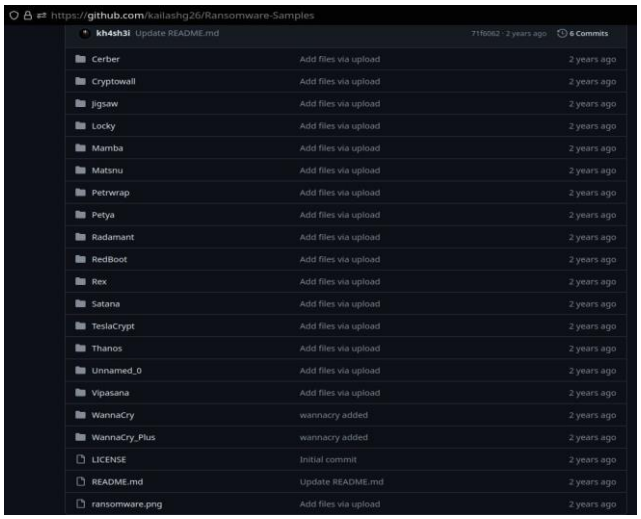

Fig. 4. Samples collected from TZ repository

B. Hash Computation

Hashing is a method that can only create hash code, not decrypt it. It is extensively used to confirm the message's integrity by the comparisons of the generated digest code, because even little changes in the content might result in an entirely different digest code. This is an excellent tool for creating one-of-a-kind ransomware signatures. While executing SHA-256, first, the message length is calculated. In addition, bits are included, with the first bit set to one and the second bit set to zero, until the message's length falls below 512 bits. The modulo of the original message multiplied by 232 will be used to fill the last 64 bits. The newly formed 512 bits will be compressed. The hashing procedure will then be performed 64 times to generate the final digest code.

To compute the Hash values for each of the 38,157 samples, we have used a script that can automate the process. A simple Python script that runs through all the samples and computes the hashes as well as the relevant information for each sample (filename, extension, size etc.). The SHA-256 algorithm will be used to produce hashes. For each sample, it creates a 256-bit hash value. This hash value may be thought of as a Virus Sample's Unique Fingerprint. It is unaffected if some file information changes.

C. Signature Database

The signature of ransomware was generated by the hashing technique used on ransomware file using SHA-256, which yielded a 64-character fixed-length code. Hashing allows for the rapid and easy matching of file information. This method can immediately identify ransomware without the need for Cuckoo Sandbox to study it. Cuckoo Sandbox takes roughly 3-4 minutes to analyse one file on average. As a result, this procedure was significantly safer, quicker, and more accurate. However, in order to function at all, a signature repository must be established. This procedure is also quite rigorous and any minor alterations would render it worthless. All hashing data is dumped into a JSON file, which can then be simply processed and uploaded to our database. MongoDB, a NoSQL database, will be used for this purpose. It has a free tier, and the Atlas edition is a cloud-based version of MongoDB's database. Thus, it would spare us the trouble of establishing the database on our local workstation and would be advantageous in terms of scalability if required later on.

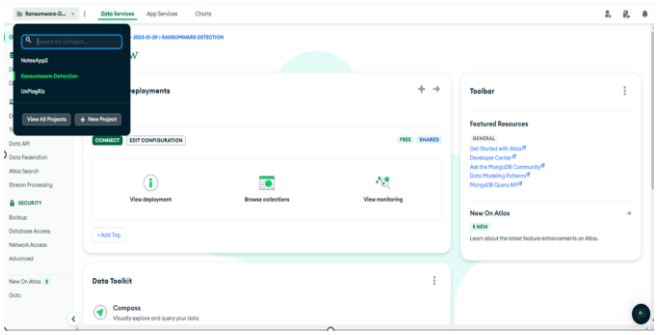

Fig. 5. Creation of signature database

We have visited the MongoDB Atlas Official Website. Following registration, we have built a New Project and a database to store our Ransomware samples. After creating the database, we just attach our previously produced JSON file into the dialogue to upload the signatures to our Signature Database.

1) Compare: In this study, a robust approach for ransomware detection is built by creating hash values for files and comparing them to a signature-based hash value repository. This procedure begins with the creation of a hash value for a particular file, which is then used to generate a unique digital fingerprint using cryptographic hash algorithms. The signature-based hash value repository, vetted by cybersecurity professionals and organisations, serves as a centralised database collecting known hash values connected with proven ransomware strains. In the comparison step, the resulting hash value is compared against entries in the repository to see whether it matches any known ransomware versions. A positive match indicates the existence of ransomware, but a lack of match shows the presence of a non-malicious file based on current repository information. This strategy provides speedy and efficient detection while taking into account factors such as regular repository updates and collaboration within the cybersecurity community to ensure efficacy against developing ransomware attacks. While hash-based detection is quick, regular monitoring and frequent updates assist to reduce possible false positives, leading to a proactive ransomware defence approach.

2) Signature Matching: A vital stage in ransomware detection is matching the signature hash value, which involves comparing the hash value of a given file to known

hash values maintained in a signature-based hash value repository. This technique, which begins with the creation of a file's hash value using a cryptographic hash function, creates a unique digital fingerprint for the file. The signature-based repository serves as a centralised database that is vetted by cybersecurity specialists and contains hash values connected with proven ransomware strains. When a file is analysed, its estimated hash value is compared against entries in the repository to see if they match. A positive match indicates that the file has similarities to a known ransomware strain, triggering an alarm for further study or quick removal. Continuous monitoring, frequent repository updates, and communication within the cybersecurity community are critical considerations for mitigating false positives caused by genuine file changes or alterations.

D. Backup System

The Automatic Backup System is a complicated system in and of itself. As a result, it is vital to predefine the libraries and packages that may be required. The watchdog library was used to monitor the file system and identify any changes that occur in the given source directory. Because the Automatic Backup Service must operate in the background even while the GUI is closed, we must build some form of multiprocessing within our programme. To build a distinct process for our Auto-Backup logic, we'll utilise the multiprocessing module. We also need to replicate the files as they are, so we have used the shutil module for that. It is also critical that our programme maintains its state across sessions. As a result, we have used the config.json file to contain stateful information like the Automatic Backup Process's process PID. To terminate processes, the psutil module has utilised.

Because ransomware is a severe danger, backup-based software with the main advantage of automated real-time backup has been offered. The system offers a variety of backup choices, including backup, auto backup, and encryption backup. First, the user must choose the type of backup they want, then the system parameters for backup, and finally the source and destination folders for backup. Once this is done, we are all set, and every time the user saves a new file in the source folder, the software detects it in real time and backs it up automatically. To secure the backup folder against ransomware assaults, the programme also includes an encryption method. The programme will run from an external SSD, so even if a ransomware assault occurs, the software and backup are safe, and consumers will not have to worry about data loss. Fig. 6. shows the flow of the backup system.

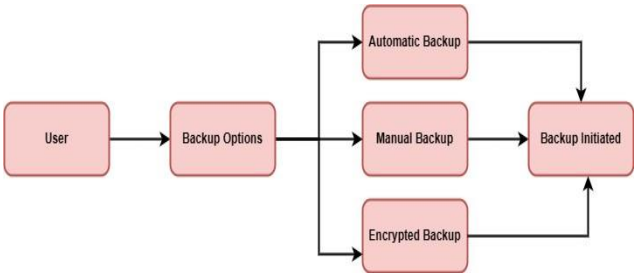

Fig. 6. Backup flow

4. Result

Alerting the user becomes critical in the ransomware detection process, especially after identifying a positive match with the hash value. This occurs when the system identifies a link between the computed hash value of a file and the known hash values stored in the signature-based repository. The instant warning acts as a real-time signal, informing appropriate security staff or system administrators of the probable existence of ransomware. This alerting system fits smoothly into a larger incident response workflow, which includes extensive investigation, impact assessment, and the development of a strategic action plan by the incident response team. Simultaneously, user education is critical in assisting users in understanding the possible hazards and adopting safe habits. Continuous monitoring keeps an eye out for new threats, and collaboration within the cybersecurity community, along with incident reporting, helps to a collective defence against ransomware and other cyber threats, boosting overall cybersecurity resilience. Fig. 7. shows the alert is generated to inform user about the ransomware.

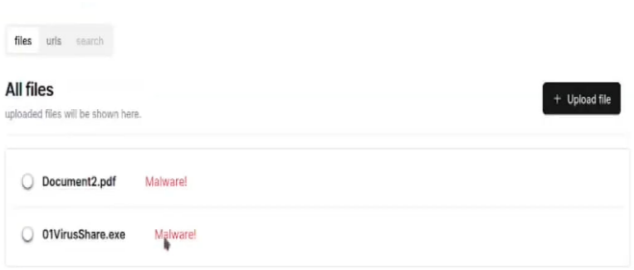

Fig. 7. Alert generation

We have developed the user interface using customTkinter, which is a fork of the standard Python library Tkinter. CustomTkinter includes curved border radii for GUI components, as well as more customised and attractive themes, as well as support for dark mode and dynamic theming. It features a syntax that is quite similar to Tkinter's, but with more attractively designed components. Fig. 8. Shows the user interface created with the CustomTkinter package. It may then be built into an executable file that runs on a Windows computer.

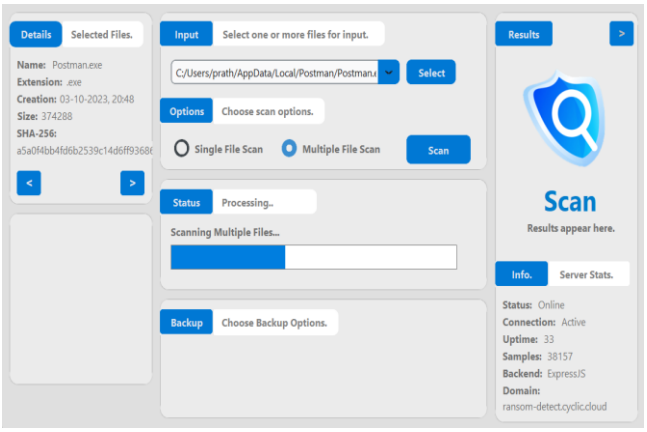

Fig. 8. File Scanning

Files can be scanned using the select option and the multiple files can be scanned at a sane time. From the user interface, a user can check the status of the file scan from the progress bar. After scanning , the result will be produced and if ransomware is identified then it will alert the user and the backup process will be initiated. Fig. 8. Shows the result of a file and it shows the information about the file. The hash value of the file is compared to the signature database and the result is returned.

For backup, we have kept three options as automatic backup, manual backup and encrypted backup to safeguard the data from ransomware attack. Backup types can be choosen from these three options and source and destination address need to specify. One of the features integrated into this programme, as stated earlier is automated backup, which intends to automatically backup your files as soon as you connect your HDD or connect your Android Phone, with only a few clicks after correct configuration. The backup location adjusts itself to the current state of the backup folder with each update, so that when you restore, you receive the same state as your last backup. You may also search for and restore old files or previous versions of your files.Fig. 9 shows a glimse of automatic backup systen. We need to click stop autobackup if we want to stop monitoring and the backup.

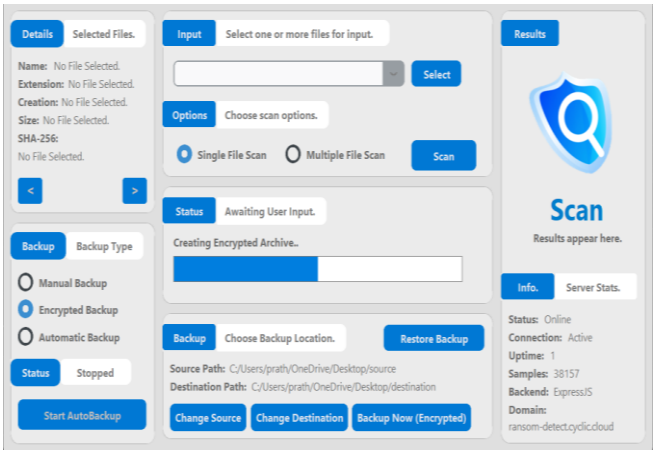

Fig. 9. Backup system

In encrypted backup, It simply automates the creation of encrypted zip or rar files containing backup files. Only the given password may be used to access the encrypted zip file. The backup file can be decrypted using the key and the data can be recovered.

5. Discussion and Future Work

Ransomware, which is a particularly deadly infection, uses powerful encryption to render its victim's electronic documents inaccessible, which may be irreparable even if the ransom is paid. To address the issue of the damage caused by ransomware attack, we have proposed a backup system, which can implement backup solutions that will automatically backup critical data to secure, isolated storage and the data must be encrypted to ensure it remains secure even in the case of a ransomware attack. To detect ransomware, we have collected different live malware samples and created a huge signature database. We have compared the signature of an infected or malicious file with our database.

Our approach offers rapid and efficient detection and our efforts contribute to a proactive ransomware defence plan. But the inability of signature-based detection methods to detect unknown threats is one of their most severe shortcomings. Malicious actors can escape detection by simply changing attack sequences within malware and other sorts of assaults. Malware or harmful behaviour patterns that may signal an attempted breach or attack are identified using behavior-based solutions. These solutions can be accomplished through the use of software agents that monitor application or user activity and interactions. In the future, unsupervised learning must be utilised to identify new ransomware variations. Furthermore, by merging static and dynamic investigations, the advantages of these two methodologies may be used for future research. Our strategy can serve as a model for developing a ransomware repository, automated backup mechanism and a user interface to help the administrator to detect the infected file, safeguard the data to recover in future and a design structure to interact and manage the system with ease.

6. Conclusion

This study of ransomware detection using signature of ransomware and as well as automated backup offers an important step forward in combating the ever-increasing menace of ransomware in our digital ecosystem. By combining signature-based detection with automated backup, this study has established a strong and proactive defence mechanism against ransomware assaults. We demonstrated that this integrated method dramatically improves cybersecurity by not only detecting ransomware with high accuracy, but also assuring the availability and integrity of vital data via automatic backups. This initiative has highlighted the significance of adaptation in

cybersecurity, since ransomware techniques develop and standard methods may fall short. To keep one step ahead of cyberthreats as we move forward, we must remain attentive and constantly improve our defence measures. The lessons gained and approaches created in this study add significant insights to continuing efforts to safeguard our digital infrastructure and preserve our data assets in an era when the stakes for cybersecurity have never been greater.

References

[1] Beaman C, Barkworth A, Akande TD, Hakak S, Khan MK. "Ransomware: Recent advances, analysis, challenges and future research directions. " Comput Secur. 2021 Dec;111:102490. doi: 10.1016/j.cose.2021.102490. Epub 2021 Sep 24. PMID: 34602684; PMCID: PMC8463105.

[2] Taran Cyriac John, Muhammad Shabbir Abbasi, Harith Al-Sahaf, Ian Welch, Julian Jang-Jaccard, Evolving malice scoring models for ransomware detection: An automated approach by utilising genetic programming and cooperative coevolution, Computers & Security, Volume 129, 2023, 103215, ISSN 0167-4048, https://doi.org/10.1016/j.cose.2023.103215.(https://www.sciencedirect.com/science/article/pii/S0167404823001256)

[3] J. A. Diro, H. Reda, N. Chilamkurti, A. Mahmood, N. Zaman and Y. Nam, "Lightweight Authenticated-Encryption Scheme for Internet of Things Based on Publish-Subscribe Communication," in *IEEE Access*, vol. 8, pp. 60539-60551, 2020, doi: 10.1109/ACCESS.2020.2983117

[4] Chesti, I.A.; Humayun, M.; Sama, N.U.; Jhanjhi, N. Evolution, mitigation, and prevention of ransomware. In Proceedings of the 2020 2nd International Conference on Computer and Information Sciences (ICCIS), Sakaka, Saudi Arabia, 13–15 October 2020; pp. 1–6. [Google Scholar]

[5] F. Cicala and E. Bertino, "Analysis of Encryption Key Generation in Modern Crypto Ransomware," in *IEEE Transactions on Dependable and Secure Computing*, vol. 19, no. 2, pp. 1239-1253, 1 March-April 2022, doi: 10.1109/TDSC.2020.3005976.

[6] Celdrán, A.H.; Sánchez, P.M.S.; Castillo, M.A.; Bovet, G.; Pérez, G.M.; Stiller, B. Intelligent and behavioral-based detection of malware in IoT spectrum sensors. Int. J. Inf. Secur. 2022, 22, 541–561. [Google Scholar] [CrossRef]

[7] Philip, K.; Sakir, S.; Domhnall, C. Evolution of ransomware. *IET Netw.* 2018, *7*, 321–327. [Google Scholar]

[8] Silva, J.A.H. , Barona, L. , Valdivieso, L. , Alvarez, M. , 2019. "A survey on situational awareness of ransomware attacks –detection and prevention parameters, " *RemoteSens.* 2019, *11*(10),1168; https://doi.org/10.3390/rs11101168.

[9] Bander Ali Saleh Al-rimy, Mohd Aizaini Maarof, Syed Zainudeen Mohd Shaid, "Ransomware threat success factors, taxonomy, and countermeasures: A survey and research directions, " Computers & Security, Volume 74, 2018, Pages 144-166, ISSN 0167-4048, https://doi.org/10.1016/j.cose.2018.01.001.(https://www.sciencedirect.com/science/article/pii/S016740481830004X)

[10] Mohurle, S., Patil, M.R., 2017. "A brief study of wannacry threat: ransomware attack, " 2017. Int. J. Adv. Res. Comput. Sci. 8 (5), 1938–1940. http://www.ijarcs.info/ index.php/Ijarcs/article/view/4021

[11] Kharraz, A., Robertson, W., Balzarotti, D., Bilge, L., Kirda, E. (2015). "Cutting the Gordian Knot: A Look Under the Hood of Ransomware Attacks," In: Almgren, M., Gulisano, V., Maggi, F. (eds) Detection of Intrusions and Malware, and Vulnerability Assessment. DIMVA 2015. Lecture Notes in Computer Science(), vol 9148. Springer, Cham. https://doi.org/10.1007/978-3-319-20550-2_1

[12] Laszka, A., Farhang, S., Grossklags, J. (2017). "In: Rass, S., An, B., Kiekintveld, C., Fang, F., Schauer, S. (eds) Decision and Game Theory for Security, " GameSec 2017. Lecture Notes in Computer Science(), vol 10575. Springer, Cham. https://doi.org/10.1007/978-3-319-68711-7_21

[13] Anghel, Mihail, and Andrei Racautanu. "A note on different types of ransomware attacks." Cryptology ePrint Archive (2019).

[14] Celiktas, B., Karacuha, E., 2018. "The Ransomware Detection and Prevention Tool Design by Using Signature and Anomaly Based Detection Methods," Istanbul Technical University. (2018). 10.13140/RG.2.2.16758.29765.

[15] Ren, Amos & Liang, Chong & Hyug, Im & Brohi, Sarfraz & Jhanjhi, Noor. (2018). "A Three-Level Ransomware Detection and Prevention Mechanism, " EAI Endorsed Transactions on Energy Web. 7. 162691. 10.4108/eai.13-7-2018.162691.

[16] Alhawi, Omar & Baldwin, James & Dehghantanha, Ali. (2018). "Leveraging Machine Learning Techniques for Windows Ransomware Network Traffic Detection, " 10.1007/978-3-319-73951-9_5.

[17] Zhang, Hanqi & Xiao, Xi & Mercaldo, Francesco & Ni, Shiguang & Martinelli, Fabio & Kumar, Arun. (2018). "Classification of ransomware families with machine learning based on N -gram of opcodes," Future Generation Computer Systems. 90. 10.1016/j.future.2018.07.052.

[18] Davide Berardi, Saverio Giallorenzo, Andrea Melis, Simone Melloni, Loris Onori, Marco Prandini, "Data Flooding against Ransomware: Concepts and Implementations," Computers & Security, Volume 131, 2023, 103295, ISSN 0167-4048,https://doi.org/10.1016/j.cose.2023.103295.(https://www.sciencedirect.com/science/article/pii/S0167404823002055)

[19] Kenan Begovic, Abdulaziz Al-Ali, Qutaibah Malluhi "Cryptographic ransomware encryption detection: Survey," Computers & Security (IF 5.6), 2023, DOI: 10.1016/j.cose.2023.103349

[20] Moreira, Caio & Moreira, Davi Carvalho & Jr, Claudomiro. (2023). "Improving Ransomware Detection based on Portable Executable Header using Xception Convolutional Neural Network," Computers & Security. 130. 103265. 10.1016/j.cose.2023.103265.

[21] Arzu Gorgulu Kakisim, Mert Nar, Ibrahim Sogukpinar, Metamorphic malware identification using engine-specific patterns based on co-opcode graphs, Computer Standards & Interfaces, Volume 71, 2020, 103443, ISSN 0920-5489, https://doi.org/10.1016/j.csi.2020.103443.(https://www.sciencedirect.com/science/article/pii/S0920548919302685)

[22] Berrueta, Eduardo & Morato, Daniel & Magaña, Eduardo & Izal, Mikel. (2022). "Crypto-ransomware detection using machine learning models in file-sharing network scenario with encrypted traffic,"

[23] Cimitile, Aniello & Mercaldo, Francesco & Nardone, Vittoria & Santone, Antonella & Visaggio, Corrado Aaron. (2018). "Talos: no more ransomware victims with formal methods," International Journal of Information Security. 17. 10.1007/s10207-017-0398-5.

[24] Zhen Li,Qi Liao, "Preventive portfolio against data-selling ransomware—A game theory of encryption and deception," Computers and Security, Volume 116, Issue C, May 2022, https://doi.org/10.1016/j.cose.2022.102644

[25] Molina, Ricardo & Torabi, Sadegh & Sarieddine, Khaled & Bou-Harb, Elias & Bouguila, Nizar & Assi, Chadi. (2021). On Ransomware Family Attribution Using Pre-Attack Paranoia Activities. IEEE Transactions on Network and Service Management. PP. 10.1109/TNSM.2021.3112056.

[26] S. H. Kok, A. Abdullah and N. Jhanjhi, "Early detection of crypto-ransomware using pre-encryption detection algorithm," Journal of King Saud University–Computer and Information Sciences, https://doi.org/10.1016/j.jksuci.2020.06.012

[27] Shaukat, Saiyed & Ribeiro, Vinay. (2018). "RansomWall: A layered defense system against cryptographic ransomware attacks using machine learning," 356-363. 10.1109/COMSNETS.2018.8328219.

[28] J.A. Gómez-Hernández, L. Álvarez-González, P. García-Teodoro, "R-Locker: Thwarting ransomware action through a honeyfile-based approach, " Computers & Security, Volume 73, 2018, Pages 389-398, ISSN 0167-4048, https://doi.org/10.1016/j.cose.2017.11.019. (https://www.sciencedirect.com/science/article/pii/S0167404817302560)

[29] Ami, Or & Elovici, Yuval & Hendler, Danny. (2018). "Ransomware prevention using application authentication-based file access control ", SAC '18: Proceedings of the 33rd Annual ACM Symposium on Applied Computing. 1610-1619. 10.1145/3167132.3167304.