IJFANS INTERNATIONAL JOURNAL OF FOOD AND NUTRITIONAL SCIENCES
ISSN PRINT 2319 1775 Online 2320 7876
 Journal Volume 14, Iss 04, 2025

TECHNIQUES FOR THE DETECTION OF RANSOMWARE THAT MAKE USE OF MACHINE LEARNING

Kole Supriya[1], Aditya Goud P[2], Modulla Jeyendra Reddy[3], Killa Spoorthi[4], Ravula Jeevitha[5], M Susmitha [6]

[1,2,3&4]Ug Schoalr, Department Of Cse(Ai&Ml), Narsimha Reddy Engineering College (Ugc-Autonomous), Maisammaguda (V), Kompally, Secunderabad, Telangana-500100

[5]Assistant Professor, Department Of Cse(Ai&Ml), Narsimha Reddy Engineering College (Ugc- Autonomous), Maisammaguda (V), Kompally, Secunderabad, Telangana-500100

[6]Assistant Professor, Department Of Civil Engineering, Narsimha Reddy Engineering College (Ugc- Autonomous), Maisammaguda (V), Kompally, Secunderabad, Telangana-500100

ABSTRACT

Given the increasing prevalence and sophistication of ransomware attacks, there is an escalating need for dynamic and effective detection and mitigation strategies. Traditional mark-based methodologies often exhibit deficiencies in identifying new and emerging variants of ransomware. This research examines the use of machine learning techniques for ransomware detection, aiming to enhance the accuracy and adaptability of detection tools. It offers a comprehensive analysis of several machine learning techniques and algorithms, evaluating their effectiveness in detecting ransomware trends. The results provide critical insights into the evolution of cybersecurity strategies that are more robust and proactive in addressing the evolving environment of ransomware threats.

1.INTRODUCTION

The evolving nature of digital threats within the technological environment has significantly transformed the complexity and character of assaults [1]. Among the myriad of digital dangers, ransomware has emerged as a particularly formidable adversary, causing extensive disruption to individuals, organizations, and critical infrastructure. Exploiting vulnerabilities in cybersecurity measures, ransomware encrypts critical data and demands exorbitant payments for its restoration. Although traditional mark-based detection tools are very effective, they often struggle to keep pace with the rapid growth of ransomware variants that use sophisticated tactics to evade detection. The alarming premise of this test has drawn significant attention to the integration of machine learning techniques into cybersecurity systems [4-5]. Machine learning enables frameworks to learn and adapt via validated data and emerging trends, providing the possibility for adaptability and proactive risk identification [6-7]. This study examines ransomware detection, specifically emphasizing the use of various machine learning techniques to enhance the accuracy and effectiveness of detection systems. The next sections will do a thorough study of several machine learning techniques for ransomware detection. We will examine the advantages

and disadvantages of supervised learning algorithms, unsupervised learning techniques, and deep learning models [9]. Additionally, the article will provide a comprehensive methodology for integrating machine learning into existing cybersecurity infrastructures, addressing the practical problems related to real-world implementation. As we start our research, it is crucial to emphasize the significant role that machine learning plays in improving the flexibility and efficacy of ransomware detection systems. Our goal is to use clever algorithms to identify and mitigate current ransomware threats while also anticipating and countering the adaptive tactics used by thieves. We expect our study to provide critical insights, allowing cybersecurity experts to outpace ransomware perpetrators in the ongoing cat-and-mouse dynamic [10]. The study is divided into the following sections: it begins with an introduction that contextualizes the research, followed by Section II, which specifically delineates the primary goals. Section III of the literature review rigorously evaluates previous research, pinpointing deficiencies and situating the study within the wider academic context. Section IV examines several machine learning techniques for ransomware detection. Section V delineates the study strategy and data gathering methods, while Section VI on data preparation elucidates the procedures used to organize and format the dataset for analysis. Results are examined in Section VII, while Section VIII discusses the results in connection to the study goals and current literature. Ultimately, Section IX concludes by summarizing important contributions and delineating suggestions for further study. This systematic methodology guarantees a comprehensive examination of machine learning in ransomware detection, including theoretical principles, actual application, and analytical evaluation.

2. LITERATURE REVIEW

1. Kok, S. H., Abdullah, A., & Jhanjhi, N. Z. (2022). Early detection of crypto-ransomware using pre-encryption detection algorithm. Journal of King Saud University-Computer and Information Sciences, 34(5), 1984-1999.

Crypto ransomware is a kind of malware that encrypts a victim's files, rendering them inaccessible until a ransom is paid. Its popularity has surged rapidly among the cybersecurity community owing to several successful global assaults. The encryption used inflicted irreparable harm on the victim's digital data, even if the victim opts to pay the ransom. This study introduces the Pre-Encryption Detection Algorithm (PEDA), capable of identifying crypto-ransomware during the pre-encryption phase, prior to any encryption occurring. PEDA has dual detection levels; the first level identifies ransomware before to activation by a signature comparison with that of known crypto-ransomware. The signature was produced using SHA-256 (Secure Hashing Algorithm), facilitating rapid and precise comparison of the file content. The secondary detection level used a Learning Algorithm (LA) capable of identifying crypto-ransomware using pre-encryption application program interfaces (APIs). The LA achieved a 100% recall rate using an 80:20 training and testing ratio, and a 99.9% recall rate during a 10-fold cross-validation test. This study successfully found fourteen significant APIs that may

distinguish between ransomware and legitimate software. Three APIs were mostly found in ransomware, but less often in legitimate software; is a kind of virus that restricts access to its victim's resources by altering system logins or encrypting digital information. It then requires a ransom from the victim to access the resources. This virus became notorious in cybersecurity after the global cyber-attack of WannaCry in 2017, which compromised over 200,000 machines in 150 countries. As of now, ransomware remains one of the foremost malware threats identified by cybersecurity experts. Despite a reduction in its infection rate, the financial losses have escalated. This is due to thieves using ransomware to target certain corporations instead than the general populace. Consequently, the requested ransom is significantly increased

2. Kok, S. H., Abdullah, A., Jhanjhi, N. Z., & Supramaniam, M. (2019). Prevention of crypto-ransomware using a pre-encryption detection algorithm. Computers, 8(4), 79.

Ransomware is a novel kind of intrusion assault designed to extract a ransom from its victim. This study only examines crypto-ransomware, a form of ransomware attack that renders data irretrievable once the victim's files are encrypted. This study proposes the use of machine learning to identify crypto-ransomware before to the initiation of its encryption process, namely at the pre-encryption stage. Effective detection at this juncture is essential to prevent the assault from accomplishing its goal. Upon the victim's recognition of the crypto-ransomware, important data and files may be backed up to an alternative place, followed by an effort to eradicate the ransomware with little risk. Consequently, we presented a pre-encryption detection method (PEDA) including two steps. During PEDA-Phase-I, a Windows application programming interface (API) produced by a dubious software will be recorded and examined using the learning algorithm (LA). The LA can ascertain if the dubious software is crypto-ransomware by using API pattern recognition. This methodology was used to guarantee the most thorough identification of both known and undiscovered crypto-ransomware, however it may exhibit a significant false positive rate (FPR). If the prediction indicated crypto-ransomware, PEDA would create a signature of the suspect application and deposit it in the signature repository, located in Phase II. In PEDA-Phase-II, the signature repository facilitates the early identification of crypto-ransomware at the pre-execution stage using the signature matching mechanism. This approach is capable of detecting just known crypto-ransomware; despite its rigidity, it is both accurate and quick. The two steps of PEDA established dual levels of early detection for crypto-ransomware, guaranteeing no data are lost to the user. In this study, we concentrated on Phase I, which was the LA. Our findings indicate that the LA exhibited the lowest false positive rate (FPR) of 1.56%, in contrast to Naive Bayes (NB), Random Forest (RF), Ensemble (NB plus RF), and EldeRan, a machine learning methodology for analyzing and classifying ransomware. A low false positive rate (FPR) indicates that the logistic algorithm (LA) has a minimal likelihood of erroneously classifying goodware. Encryption is the process of transforming a communication from a comprehensible format to an

incomprehensible one to safeguard its content from unwanted access. This technique is extensively used in network security to guarantee that only the designated receiver may view its information. Encrypting the data was essential, particularly during its transmission over the network, since it is susceptible to theft. It is well established that encryption is a double-edged sword.At one end, it was an effective strategy for cybersecurity to attain its goals of data secrecy, data integrity, data authenticity, and non-repudiation. Conversely, it was used by cybercriminals to encrypt victims' data and then demand a ransom. This exploitation is evident in an intrusion assault known as crypto-ransomware. Ransomware is a novel kind of intrusion assault aimed at extorting a ransom from its victim, which is reflected in its nomenclature. The first category is referred to as scareware. This kind of ransomware poses no genuine threat to its victim. Its primary objective is to intimidate the victim into remitting the ransom. One strategy used by scareware is impersonating an authority figure that has identified some misconduct by the victim. It will need a payment to evade legal action. A kind of scareware, known as leakware, threatens to disclose the victim's misconduct to their family and friends.

3. Urooj, U., Maarof, M. A. B., & Al-rimy, B. A. S. (2021, January). A proposed adaptive pre-encryption crypto-ransomware early detection model. In 2021 3rd International Cyber Resilience Conference (CRC) (pp. 1-6). IEEE.

Crypto-ransomware is a kind of malware that use the system's cryptographic features to encrypt user data. The irreversible nature of crypto-ransomware makes survival post-attack more difficult than with other malware types. A crypto-ransomware assault encrypts user files, rendering them inaccessible without the decryption key. The accessibility of ransomware creation toolkits, such as Ransomware as a Service (RaaS), has led to the proliferation of many ransomware variations. This adds to the increase in ransomware assaults seen today. Nonetheless, the traditional methodologies used by malware detection systems are inadequate for identifying ransomware. Ransomware must be identified prior to the initiation of encryption. These threats can only be properly managed if identified during the pre-encryption process. The early identification of ransomware attacks is difficult owing to the few data accessible prior to encryption. This work proposes an adaptive pre-encryption model designed to address the population concept drift of crypto-ransomware, considering the limited data acquired during the pre-encryption phase of the attack lifecycle. Due to its versatility, the model can retain current information about attack behaviors and detect polymorphic ransomware that incessantly alters its behavior. Cybersecurity is a domain focused on safeguarding data, devices, and networks against cyber threats. Cyberattacks are executed with the purpose to access, modify, or obliterate user data or to disrupt company activities. The implementation of cybersecurity is both essential and formidable due to a diminishing workforce and an increasing number of devices. Malefactors often possess malevolent intentions aimed at obtaining, modifying, or obliterating user data and reputation.

Cybersecurity cannot be guaranteed without addressing malware threats [1]. The advancement of antivirus software and intrusion detection systems has prompted attackers to create increasingly sophisticated tactics, driven by the pursuit of profit. Ransomware may execute several additional functions, like terminating processes or issuing shutdown orders. It may also create a virtual desktop to prevent the user from completing his tasks [6, 7]. These assaults have increased owing to financial incentive. Ransomware files that trigger attacks are often disseminated by drive-by downloads, exploiting weaknesses in internet-accessible systems, phishing emails, and targeted site compromises. Ransomware has developed throughout time. Various versions are being made daily. Numerous ransomware families are created alongside distinct ransomware variants. New versions are created by using many obfuscation techniques, including garbage code insertion, variable renaming, polymorphism, metamorphism, and packing. The evolution, growth pace, and substantial volume underscored the need for adaptive and pre-encryption crypto-ransomware detection systems [8]. User-friendly kits and financial incentives are the primary catalysts propelling crypto-ransomware. Even attackers with little expertise may execute a potent cryptoransomware assault, facilitated by Ransomware as a Service (RaaS). While current solutions attempt to identify ransomware in the pre-encryption phase, they fail to account for the evolving characteristics of ransomware assaults. The emergence of zero-day attacks complicates detection efforts. Consequently, an adaptive pre-encryption detection system is essential for the prompt identification of crypto-ransomware assaults prior to the initiation of extortion [10]. This work aims to overcome the deficiency in adaptive pre-encryption ransomware detection.

4. Al-Rimy, B. A. S., Maarof, M. A., Alazab, M., Alsolami, F., Shaid, S. Z. M., Ghaleb, F. A., ... & Ali, A. M. (2020). A pseudo feedback-based annotated TF-IDF technique for dynamic crypto-ransomware preencryption boundary delineation and features extraction. IEEE Access, 8, 140586-140598.

The cryptographic measures used on user files render the consequences of crypto-ransomware assaults irreversible, even post-detection and eradication. Consequently, early detection of such attacks, namely during the pre-encryption phase prior to the initiation of encryption, is essential. Current crypto-ransomware early detection methods use a static time-based thresholding technique to delineate the pre-encryption phase borders. The fixed time thresholding method requires that all samples begin encrypting simultaneously. This assumption does not universally apply to all samples, as the initiation time of the primary sabotage differs among various crypto-ransomware families due to the obfuscation techniques utilized by the malware to alter its attack strategies and evade detection, resulting in diverse attack behaviors. The insufficient data during the first stages of the assault negatively impacts the efficacy of feature extraction approaches in early detection models, hence diminishing detection accuracy. This work offers a Dynamic Pre-

encryption border Delineation and Feature Extraction (DPBD-FE) system that properly identifies the border of the pre-encryption phase for feature extraction and selection. In contrast to the preset thresholding used by existing studies, DPBD-FE monitors the pre-encryption phase for each instance independently, relying on the first appearance of any cryptography-related APIs. An annotated Term Frequency-Inverse Document Frequency (aTF-IDF) method was used to extract characteristics from runtime data produced during the pre-encryption stage of crypto-ransomware assaults. The aTF-IDF addresses the issue of inadequate attack patterns in the first stages of the attack lifecycle. The experimental assessment demonstrates that DPBD-FE effectively identified the pre-encryption borders and extracted characteristics pertinent to this phase with more precision than comparable studies.

5. Alqahtani, A., Gazzan, M., & Sheldon, F. T. (2020, January). A proposed crypto-ransomware early detection (CRED) model using an integrated deep learning and vector space model approach. In 2020 10th Annual Computing and Communication Workshop and Conference (CCWC) (pp. 0275-0279). IEEE.

Ransomware presents a considerable threat by encrypting data or systems and requiring a fee for decryption. Timely identification is crucial to alleviate its effects. This research introduces an Uncertainty-Aware Dynamic Early Stopping (UA-DES) method for enhancing Deep Belief Networks (DBNs) in ransomware detection. UA-DES employs Bayesian methodologies, dropout strategies, and an active learning framework to dynamically modify the number of epochs in the training of the detection model, therefore mitigating overfitting and improving model accuracy and dependability. Our approach utilizes a collection of Application Programming Interfaces (APIs) that depict ransomware activity, referred to as "UA-DES-DBN." The strategy integrates uncertainty and calibration quality metrics, enhancing the training process for improved ransomware detection accuracy. Experiments illustrate the superiority of UA-DES-DBN over traditional models. The suggested model enhanced accuracy from 94% to 98% over diverse input sizes, exceeding the performance of other models. UA-DES-DBN reduced the false positive rate from 0.18 to 0.10, enhancing its applicability in practical cybersecurity scenarios. In the digital era, gadgets are generally interconnected, enabling data transmission and simplifying user communication. This connection presents several security threats to user and corporate data [1]. These threats include malware assaults used by perpetrators to exfiltrate data, disrupt operations, or commandeer systems, resulting in operational disruptions and repercussions for reputation and compliance [2]. Ransomware is a kind of malware used by attackers to encrypt user data via the operating system's inherent cryptographic tools [3,4]. Ransomware poses a substantial risk to companies and people by encrypting data, therefore incapacitating computer systems. A decryption key may be issued subsequent to the payment of a ransom, however this is not guaranteed. The irrevocable consequences of such an assault may be

catastrophic owing to service disruptions, particularly because, in some instances, the decryption key received after ransom payment is ineffective in restoring operations. Early detection of ransomware is essential for mitigating its effects. Numerous studies [7,8,9] underscore the significance of early identification in mitigating the harm inflicted by ransomware attacks. Urooj et al. [10] emphasize the importance of early detection by developing a machine learning strategy for identifying ransomware prior to the encryption process. Furthermore, [11] recommends monitoring external server connections to detect ransomware activity promptly, therefore averting the finalization of encryption procedures. Bold et al. [12] underscore the significance of astute early detection in minimizing false positives, highlighting the benefits of swiftly discovering and eliminating ransomware. Consequently, the prompt identification of ransomware using sophisticated detection methods is crucial to avert data loss, financial damage, and operational interruptions caused by ransomware assaults.

3.EXISTING SYSTEM

Ransomware is a complex and ever advancing menace that may restrict user access to computer systems or encrypt data, requiring a ransom for restoration of access. There are two primary kind of ransomware: locker ransomware, which obstructs users from accessing their machines, and crypto ransomware, which encrypts users' data. Conventional ransomware detection methods, including event-based, statistical-based, and data-centric approaches, are not consistently successful. Consequently, it is essential for the scientific community to devise novel and inventive strategies to counteract ransomware

3.1. DISADVANTAGES OF EXISTING SYSTEM:

- Traditional ransomware detection techniques are not always effective.
- The research community is still developing new and innovative methods to combat ransomware.
- Here are some additional negative points that could be included:
- Ransomware can be very costly for victims. In addition to the ransom payment, victims may also incur costs for data recovery, IT consulting, and legal fees.

3.2. PROPOSED SYSTEM

Ransomware is a kind of malware that encrypts a victim's data and requires a ransom for their decryption. This research provides a feature selection-based framework using numerous machine learning algorithms to categorize security levels for ransomware detection and prevention, demonstrating the efficacy of machine learning in identifying ransomware. The suggested methodology identifies many characteristics for model construction using conventional machine learning classifiers and neural network topologies. The framework is assessed using a ransomware dataset, revealing that random forest classifiers surpass other approaches in accuracy, F-beta, and precision scores. The results indicate that machine learning-based frameworks are useful in ransomware detection. The results indicate that random forest classifiers may be an especially efficient method for ransomware detection. These results may inform the creation of novel

ISSN PRINT 2319 1775 Online 2320 7876
 Journal Volume 14, Iss 04, 2025

ransomware detection technologies to safeguard enterprises against this escalating menace.

3.3. ADVANTAGES OF PROPOSED SYSTEM:

- It is based on transformers, which are a powerful machine learning model that has been shown to be effective for sequence-to-sequence tasks.
- It uses self-attention mechanisms, which allow the model to learn long-range dependencies in the data.
- It is interpretable, which means that the model's predictions can be explained in terms of the features that the model attends to.

4.IMPLEMENTATION

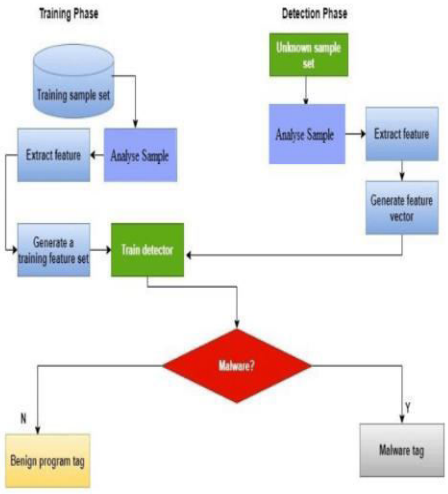


Fig: System Architecure

4.1. MODULES

- User
- Admin
- Data Preprocessing
- Machine Learning

MODULES DESCRIPTION:

User:

The User can register the first. While registering he required a valid User email and mobile for further communications. Once the User register then admin can activate the User. Once admin activated the User then User can login into our system. Here we took a dataset which contains in total 138,047 samples with 54 features and was collected from where 70% are ransomware and remaining 30% are legitimate observations. Using the Machine Learning technique the new data for dataset based on our Django application. User can click the Data Preparations in the web page so that the data cleaning process will be starts. The data and its required values will be displayed.

Admin:

Admin can login with his login details. Admin can activate the registered Users. Once he activate then only the User can login into our system. Admin can view the overall data in the browser. Algorithm execution complete then admin can see the overall accuracy in web page.

Data Preprocessing:

A dataset can be viewed as a collection of data objects, which are often also called as a records, points, vectors, patterns, events, cases, samples, observations, or entities. Data objects are described by a number of features that capture the basic characteristics of an object, such as the mass of a physical object or the time at which an event occurred, etc. Features are often called as variables, characteristics, fields, attributes, or dimensions. The data preprocessing in this forecast uses techniques like removal of noise in the data, the expulsion of missing information,

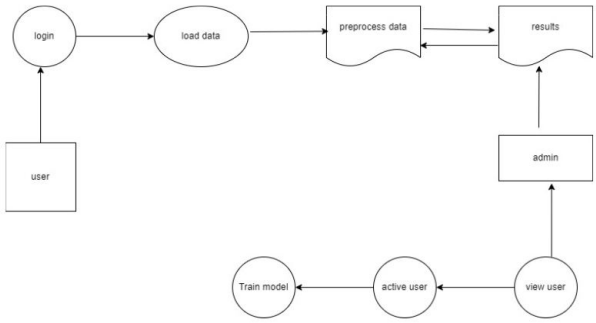
modifying default values if relevant and grouping of attributes for prediction at various levels.

Machine learning:

We applied multiple machine learning algorithms: Decision Tree (DT), Random Forest (RF), Naïve Bayes (NB), Logistic Regression (LR) as well as Neural Network (NN)-based classifiers on a selected number of features for ransomware classification. We performed all the experiments on one ransomware dataset to evaluate our proposed framework. The experimental results demonstrate that RF classifiers outperform other methods in terms of accuracy, F-beta, and precision scores.

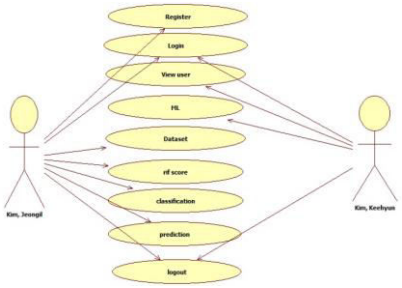
DATA FLOW DIAGRAM

1. The DFD is also called as bubble chart. It is a simple graphical formalism that can be used to represent a system in terms of input data to the system, various processing carried out on this data, and the output data is generated by this system.
2. The data flow diagram (DFD) is one of the most important modeling tools. It is used to model the system components. These components are the system process, the data used by the process, an external entity that interacts with the system and the information flows in the system.
3. DFD shows how the information moves through the system and how it is modified by a series of transformations. It is a graphical technique that depicts information flow and the transformations that are applied as data moves from input to output.
4. DFD is also known as bubble chart. A DFD may be used to represent a system at any level of abstraction. DFD may be partitioned into levels that represent increasing information flow and functional detail.



USE CASE DIAGRAM

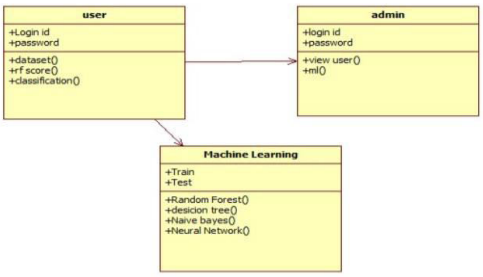
A use case diagram in the Unified Modeling Language (UML) is a type of behavioral diagram defined by and created from a Use-case analysis. Its purpose is to present a graphical overview of the functionality provided by a system in terms of actors, their goals (represented as use cases), and any dependencies between those use cases. The main purpose of a use case diagram is to show what system functions are performed for which actor. Roles of the actors in the system can be depicted.



CLASS DIAGRAM:

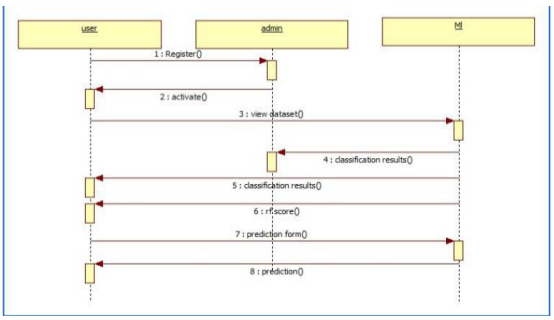
In software engineering, a class diagram in the Unified Modeling Language (UML) is a type of static structure diagram that describes the structure of a system by showing the system's classes, their attributes, operations (or methods), and the relationships among the classes. It explains which class contains information.

ISSN PRINT 2319 1775 Online 2320 7876
 Journal Volume 14, Iss 04, 2025



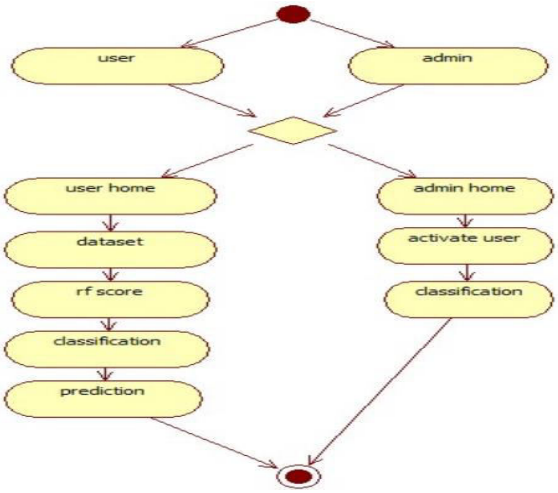
SEQUENCE DIAGRAM:

A sequence diagram in Unified Modeling Language (UML) is a kind of interaction diagram that shows how processes operate with one another and in what order. It is a construct of a Message Sequence Chart. Sequence diagrams are sometimes called event diagrams, event scenarios, and timing diagrams



ACTIVITY DIAGRAM

Activity diagrams are graphical representations of workflows of stepwise activities and actions with support for choice, iteration and concurrency. In the Unified Modeling Language, activity diagrams can be used to describe the business and operational step-by-step workflows of components in a system. An activity diagram shows the overall flow of control.



5.RESULTS

Fig: Index Page

Fig: User Registration Page

Fig: Registered Users

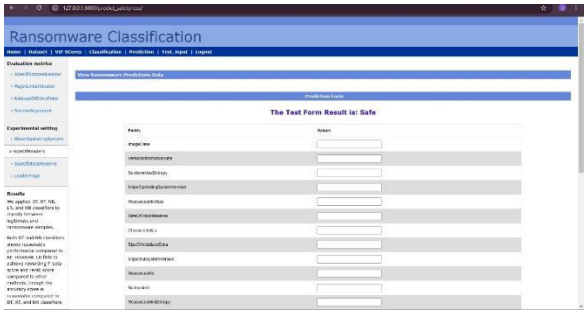


Fig: Detect attack

CONCLUSION

This study's results highlight the crucial need of machine learning in improving ransomware detection systems. The thorough evaluation of many algorithms revealed that Support Vector Machines (SVM) emerged as the most effective classifier, exhibiting a high accuracy rate. The findings underscore the significance of feature engineering, especially with API call attributes, in improving the model's discriminative power. This research enhances cybersecurity measures by using machine learning. Our study intends to enhance the accuracy and flexibility of ransomware detection techniques, hence delivering substantial advantages via more robust and proactive cybersecurity solutions. The thorough examination of several machine learning techniques assesses their efficacy in identifying ransomware trends and provides critical insights to inform the creation of robust solutions against the evolving dangers of ransomware assaults. In the ongoing struggle against cyber enemies, our research equips firms to maintain an advantage via sophisticated algorithms and proactive protection strategies. This study's collection of algorithms establishes a foundation for future progress in ransomware detection, providing a framework for the creation of advanced and robust cybersecurity solutions.

REFERENCES

[1] Kok, S. H., Abdullah, A., & Jhanjhi, N. Z. (2022). Early detection of crypto-ransomware using pre-encryption detection algorithm. Journal of King Saud University-Computer and Information Sciences, 34(5), 1984-1999.

[2] Kok, S. H., Abdullah, A., Jhanjhi, N. Z., & Supramaniam, M. (2019). Prevention of crypto-ransomware using a pre-encryption detection algorithm. Computers, 8(4), 79.

[3] Urooj, U., Maarof, M. A. B., & Al-rimy, B. A. S. (2021, January). A proposed adaptive pre-encryption crypto-ransomware early detection model. In 2021 3rd International Cyber Resilience Conference (CRC) (pp. 1-6). IEEE.

[4] Al-Rimy, B. A. S., Maarof, M. A., Alazab, M., Alsolami, F., Shaid, S. Z. M., Ghaleb, F. A., ... & Ali, A. M. (2020). A pseudo feedback-based annotated TF-IDF technique for dynamic crypto-ransomware preencryption boundary delineation and features extraction. IEEE Access, 8, 140586-140598.

[5] Alqahtani, A., Gazzan, M., & Sheldon, F. T. (2020, January). A proposed crypto-ransomware early detection (CRED) model using an integrated deep learning and vector space model approach. In 2020 10th Annual Computing and Communication Workshop and Conference (CCWC) (pp. 0275-0279). IEEE.

[6] Y Zakaria, W. Z., Abdollah, M. F., Mohd, O., Yassin, S. W. M. S. M., & Ariffin, A. (2022). RENTAKA: A Novel Machine Learning Framework for Crypto-

Ransomware Pre-encryption Detection. International Journal of Advanced Computer Science and Applications, 13(5).

[7] Wang, L., He, R., Wang, H., Xia, P., Li, Y., Wu, L., ... & Xu, G. (2020). Beyond the virus: A first look at coronavirus-themed mobile malware. arXiv preprint arXiv:2005.14619.

[8] Morris, J., Lin, D., & Smith, M. (2021). Fight Virus Like a Virus: A New Defense Method Against File-Encrypting Ransomware. arXiv preprint arXiv:2103.11014.

[9] Wang, Z., Liu, C., Cui, X., Yin, J., & Wang, X. (2022). Evilmodel 2.0: bringing neural network models into malware attacks. Computers & Security, 120, 102807.

[10] Chen, X., Hao, Z., Li, L., Cui, L., Zhu, Y., Ding, Z., & Liu, Y. (2022). Cruparamer: Learning on parameter-augmented api sequences for malware detection. IEEE Transactions on Information Forensics and Security, 17, 788-803.