A COLAB-INTEGRATED HYBRID MODEL FOR EFFECTIVE RANSOMWARE DETECTION VIA VOTING CLASSIFIER TECHNIQUES

Submitted By

Md. Eyashin

Section: A

ID: 211-35-712

Department of Software Engineering

Daffodil International University

Supervised By

Afsana Begum

Assistant Professor & Coordinator M.Sc

Department of Software Engineering

Daffodil International University

Thesis submitted in fulfillment of the requirements for the award of the degree of

Bachelor of Science

Fall - 2024

DAFFODIL INTERNATIONAL UNIVERSITY

DECLARATION OF THESIS AND COPYRIGHT

Author's Full Name	:	MD. EYASHIN
Date of Birth	:	13/04/2001
Title	:	A Colab-Integrated Hybrid Model For Effective Ransomware Detection Via Voting Classifier Techniques
Academic Session	:	2021-2024

I declare that this thesis is classified as:

☐	CONFIDENTIAL	(Contains confidential information under the Official Secret Act 1997)*
☑	RESTRICTED	(Contains restricted information as specified by the organization where research was done)*
☐	OPEN ACCESS	I agree that my thesis to be published as online open access (Full Text)

I acknowledge that Daffodil International University reserves the following rights:

1. The Thesis is the Property of Daffodil International University.
2. The Library of Daffodil International University has the right to make copies of the thesis for the purpose of research only.
3. The Library of Daffodil International University has the right to make copies of the thesis for academic exchange.

Certified by:

Eyashin
(Student's Signature)

211-35-712
Student ID :
Date: 14/01/2025

(Supervisor's Signature)

Afsana Begum
Name of Supervisor
Date: 14/01/2025

NOTE : * If the thesis is CONFIDENTIAL or RESTRICTED, please attach a thesis declaration letter.

APPROVAL

This thesis titled on "**A Colab-Integrated Hybrid Model For Effective Ransomware Detection Via Voting Classifier Techniques**", submitted by **Md. Eyashin (ID: 211-35-712)** to the Department of Software Engineering, Daffodil International University has been accepted as satisfactory for the partial fulfillment of the requirements for the degree of Bachelor of Science in Software Engineering and approval as to its style and contents.

BOARD OF EXAMINERS

Professor Dr. Engr. AKM Masum
Professor
Department of Software Engineering
Faculty of Science and Information Technology
Daffodil International University

Chairman

Md. Shohel Arman
Assistant Professor
Department of Software Engineering
Faculty of Science and Information Technology
Daffodil International University

Internal Examiner 1

Dr. Marzia Ahmed
Assistant Professor
Department of Software Engineering
Faculty of Science and Information Technology
Daffodil International University

Internal Examiner 2

Dr. Md. Monowarul Islam
Associate Professor
Department of Computer Science & Engineering
Jagannath University

External Examiner

SUPERVISOR'S DECLARATION

I hereby declare that I have checked this thesis and in my opinion, this thesis is adequate in terms of scope and quality for the award of the degree of Bachelor of Science.

(Supervisor's Signature)

Full Name : Afsana Begum

Position : Assistant Professor & Coordinator M.Sc

Date : 14/01/2025

STUDENT'S DECLARATION

I hereby declare that the work in this thesis is based on my original work except for quotations and citations which have been duly acknowledged. I also declare that it has not been previously or concurrently submitted for any other degree at Daffodil International University or any other institution.

Eyashin

(Student's Signature)

Full Name : MD. EYASHIN

ID Number : 211-35-712

Date : 14 January 2025

A COLAB-INTEGRATED HYBRID MODEL FOR EFFECTIVE RANSOMWARE DETECTION VIA VOTING CLASSIFIER TECHNIQUES

MD. EYASHIN

Thesis submitted in fulfillment of the requirements
for the award of the degree of
Bachelor of Science

Department of Software Engineering (Major in Cyber Security)

DAFFODIL INTERNATIONAL UNIVERSITY

January 2025

ACKNOWLEDGEMENTS

First and foremost, I am deeply grateful to Almighty Allah, who has given me the strength, wisdom, and perseverance to complete this research. My parents have supported, encouraged, and believed in me from my first day in school to the last book I read, and I'm incredibly thankful for their love. It has always been the fact that they believed in me that was my greatest motivating factor.

I would like to thank my supervisor Afsana Begum, Assistant Professor & Coordinator M.Sc, Department of SWE, Daffodil International University, Dhaka. My supervisor deserves thanks for the valuable advice, support, and guidance the provided throughout the research. Her knowledge and insight have profoundly affected this work. The departmental head, Dr. Imran Mahmud, is also highly appreciated for his support, guidance, and valuable comments which helped me to successfully complete my journey.

Finally, I would like to thank all my friends, colleagues, and all those who helped and encouraged me during this process.

ABSTRACT

Ransomware is a harmful malware that is designed to encrypt a victim's data or lock the victim's system, then demand a ransom for restoration or decrypting the data or unlocking the system, and it often causes significant financial and operational damage. Current ransomware detection methods are struggling to detect ransomware properly because most of the ransomware detection approaches follow dynamic analysis techniques which involve a complicated process, and also use only signature-based features, not use network or behavioral based features. This study proposed a ransomware detection hybrid model that is based on static analysis and uses signature-based features, network, or behavioral features. This study used three ML models for implementing hybrid models, models are Decision Tree, Random Forest, and K-Nearest Neighbors. This study proposed two hybrid models, where the hybrid model achieved highest detection accuracy 97.48% with a low false positive and false negative rate.

Keyword: machine learning, ransomware analysis, ransomware detection, voting classifier, cyber security.

TABLE OF CONTENT

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

DT	Decision Tree
RF	Random Forest
KNN	K-NNeighbors
GBDT	Gradient Boosting Decision Tree
PM	Proposed Model
ML	Machine Learning

CHAPTER 1

INTRODUCTION

1.1 Introduction

In cybersecurity sector rapidly changing threat landscape, technological advancements, cyber defense strategies, and attack techniques. Many people are working in this sector to protect themselves from attackers. Cyber Security infrastructure, more advanced cyber defense strategies, and tools are constantly being developed because always emerging threats are coming in the cybersecurity sector. Malware or malicious software is always dangerous and harmful for individuals or organizations. Ransomware is a type of malware. Ransomware mainly encrypts files on a victim's device and demands a ransom for decrypting files. If the victim pays ransom amount then attackers send a decryption key and victims can restore access to their data, otherwise attackers delete those files or disclose them publicly [1]. And there are some types of ransomware (NotPetya), that only encrypt files or systems, not possible to decrypt [2]. Ransomware is not only an individual threat, it also impacts organizations and government systems or any type of site. It is exploiting vulnerabilities in the victim systems using phishing emails, any type of malicious downloads, or infected USB devices. When victims are infected by a ransomware attack, this time they lose sensitive information, financial losses, operational disruption, and reputational damage. For the first time, ransomware payments crossed $1 billion in 2023 and the United Kingdom(UK) was the most affected country that year [3]. From January to Jun 2024, the most affected industries sectors are healthcare, construction, and manufacturing [4]. The United States(U.S.) is the most targeted country and the business services area is the most targeted sector in 2024 [5]. Ransomware detection approaches struggle to detect threats, and detection model false positive rates are high [6]. Basically, most of the ransomware detection approaches follow dynamic analysis techniques which involve a complicated process, and also use a signature-based detection method, where not use network or behavioral based features that reason detection accuracy is decrease and which is not effective against threats and this type of detection approach struggles to detect threats. Many machine learning algorithms give that solution, but here is main problem is to collect the accurate dataset, and then train the model. First of all collect proper datasets where exist the signature-based features, network, or behavioral features and select the important feature that helps to detect the target feature. Create a hybrid model based on the machine learning algorithms which is performed accurately and model accuracy is high and reduce the false positive. Used StandardScaler function for feature scaling, that is improved model

performance and help to more accurately detect ransomware or anomaly. By focusing on the signature-based feature, network-related features, or behavioral features and implementing a hybrid model, these approaches improve the accuracy of the ransomware detection model, also providing a more effective defense approach against the ransomware threat. This ransomware detection approach improves the detection accuracy, also reduces the false positive rate, and provides a more accurate defense detection approach.

1.2 Motivation

Ransomware attacks are one of the most significant threats that disrupt operations, loss of critical information, and reputational damage to individuals or any type of organization [7]. Current ransomware detection methods are struggling to detect ransomware properly because most of the ransomware detection approaches follow dynamic analysis techniques which involve a complicated process, and also use only signature-based features, not use network or behavioral based features. In this limited analysis, most of the detection approaches fail to capture the anomaly. This reason not possible to improve detection accuracy and reduce false positive rates. This research overcomes these gaps by introducing a hybrid detection model. These machine-learning algorithms proposed an approach that aims to enhance detection accuracy, reduce false positive rates, and provide a scalable solution. This work not only improves model accuracy, also tries to reduce detection model false positive rates and ensure a reliable ransomware detection approach with minimal misclassification.

1.3 Rationale of the Study

Ransomware is becoming a serious issue and it's targeted individuals, groups, any type of business or organization sector, and critical infrastructures. It can disrupt operations, compromise sensitive information, financial losses, and reputational damage. Current ransomware detection methods are struggling to detect ransomware properly because most of the ransomware detection approaches follow dynamic analysis techniques which involve a complicated process, and also use only signature-based features, not use network or behavioral based features. Also used outdated datasets or mainly focused on limited features, that reason detection models are struggling to detect threats and models false positive rates are high. This study overcomes those gaps by introducing a hybrid detection model that combines signature-based features, network, or behavioral features. By using machine learning algorithms possible to improve detection model accuracy, also reduce false positive rates, and create a scalable solution that mitigates the cybersecurity threats. The main purpose is to detect known and unknown variants of ransomware that prevent data breaches, protect critical infrastructure from attackers, and reduce cyber security threats. These ransomware detection approach provide a safe online environment where everyone works smoothly. The use of ransomware detection methods has a significant impact on cybersecurity sector, improving ransomware detection accuracy and reducing known and unknown ransomware threats.

1.4 Research Question

During this study, I faced many types of challenges and successfully overcame all challenges, and finally introduced a hybrid ransomware detection model. Many questions are asked to understand the basic concepts of my research:

- From where I collected the dataset for my research?
- Can a hybrid model, improve detection accuracy and reduce false positives in ransomware detection?
- Which challenges did I face while doing this research?
- Are there any differences between the existing ransomware detection model result and my model result?

1.5 Expected Outcome

The proposed model is expected to achieve significantly higher detection accuracy and reduce false positive rates. In machine-learning-based ransomware detection model, a large dataset was used for training and testing and achieved targeted results. The model utilized signature-based features, network, and behavioral features for effective training and evaluation. After completing all necessary steps, a machine learning based ransomware detection hybrid model will be prepared. Achieved from hybrid model accuracy is 97.48%, false positive rate is 0.93% and false negative rate is 2.12%. Where existing model accuracy is 91.43%.

1.6 Report Layout

Chapter 1, This section discusses research motivation and expected results which is the main goal of the research.

Chapter 2, Reviews the existing research which is mainly focused on the ransomware detection approach, and discusses the scope of problems and challenges.

Chapter 3, Discusses the dataset analysis, proposed hybrid model methodology, and implementation requirements.

Chapter 4, This section discusses the research experiment results and algorithms.

Chapter 5, In this chapter summarizes this study and discusses future study scop.

CHAPTER 2

BACKGROUND

2.1 Introduction

Ransomware is a type of malicious code or software that is designed to block victim's access to the system or any sensitive information file until the victim's ransom amount is paid. In last few years, attackers have attacked many financial institutions, educational institutions, healthcare, critical infrastructure sectors, private agencies, and government agencies using ransomware attack methodology, where attackers or attacker groups disrupt services, steal sensitive data or expose personal information, financial losses, and reputation damage. Many people analyze attack type, methodology, attacker's tactics, and techniques then develop security infrastructure, more advanced cyber defense strategies, and tools for dependent attacks and mitigate stealing sensitive data or exposing personal information, and financial losses.

2.2 Related Works

Michael et al. [6] proposed a ransomware detection methodology using cosine similarity on bytecode, where an overall model detection accuracy rate of 94%. Focuses on bytecode analysis, where missing critical indicators such as network traffic and system behavior. This model is unable to detect emerging ransomware variants. Zhang et al. [8] proposed an opcode-based ransomware detection approach, using several machine learning models and achieving the highest accuracy of 91.43%. Only used static analysis, but not used dynamic analysis. Another limitation is some methods can not properly detect ransomware and sometimes require human intervention in certain N-gram methods. Bingyan et al. [9] worked on the existing GAN model and improved 6% accuracy over existing methods and overall model accuracy rate is 95.2%. Dynamic IRP operation monitoring with cross-validation ensures robustness, but high computational resource requirements limit model applicability. Alhashmi et al. [10] used six machine-learning algorithms and evaluated the ransomware detection, where gain highest model accuracy was 99.48% using XGBoost machine-learning algorithms, and used five-old cross-validation for ensured comprehensive performance evaluation. The limitation is ML models must require continuous updates for evolving ransomware threats and the Naive Bayes ML model produces higher false positive rates. Berardi et al. [11] introduce Data Flooding against Ransomware (DFaR) for detection, mitigation, and restoration. Used three data flooding strategies random, on-the-fly, and shadow. Research limitation is honeypot techniques are focused on rarely-used folders that lead

to false positives, and fail to cover all potential attack surfaces. Ali et al. [12] reviewed 290 papers that were published between 2015 to 2022 and the authors discussed only deep-learning models for malware detection. AE, CNN RNN, LSTM, and DBN are the widely used models for detecting malware. The research limitation is the limited research studies on web-based malware detection and insufficient focus on IoT malware. Hussain et al. [13] proposed a malware detection model for windows operating system and achieved an overall model accuracy rate is 99.44%. Total six machine learning models were applied, model names are Random Forest, SVM, Decision Tree, AdaBoost, GNB, and Gradient Boosting. The system can identify zero-day malware effectively. Used smallest dataset and limited explored in dynamic features and lack of real-time scanning capabilities in existing models. Reshmi [14] reviewed the ransomware detection and prevention techniques were showed the existing machine-learning detection model faces challenges in real-world applications. False positives are high and traditional signature-based solutions struggle to detect new variants of ransomware. Kapoor et al. reviewed existing ransomware detection, avoidance, and mitigation strategies and proposed ML-based solutions [15]. They are using static analysis to detect ransomware and using two tools, CRSTATIC and GreatEatlon. They proposed a solution to counter ransomware attacks but this solution has limited technical solutions. The survey by James and Sabitha provides a comprehensive overview of malware detection techniques, including signature-based, honeypot-based, dynamic, and hybrid approaches [16]. MARTINS et al. concentrated on attack and defensive tactics while primarily investigating adversarial machine learning in malware and intrusion detection systems [17]. The L-BFGS optimization approach is utilized to address non-trivial issues. They used outdated and limited datasets in intrusion scenarios and intrusion scenario is not evaluated for adversarial attacks. And difficulties in identifying ransomware in pictures and compressed data. Zimba et al. [18] analyzed ransomware attack structures and show CAT4 and CAT5 ransomware are difficult to mitigate and also show that how to effective mitigation strategies depend on ransomware generation. Windows operating system users are the primary target for ransomware attacks. The research gap is lack of detailed statistical analysis on financial losses and limited exploration of post-ransomware recovery processes. Maigida et al. analyzed ransomware patterns, attacks, and detection techniques [19]. Then categorized ransomware attack methods and assessed defenses against it. There is a lack of ransomware prediction models because not enough research has been done on dynamic crypto-ransomware attack strategies. The survey proposed by Kok et al., where analyzed the ransomware attack techniques, methodology, attack lifecycle, detection techniques, and emphasized machine learning algorithms [20]. And they recommend using a hybrid algorithm to improve ransomware detection performance. LEE et al. proposed a machine-learning model for detecting ransomware from infected files with high accuracy and low errors [21]. The machine learning model ransomware detects perfectly, and high detection rate with low false positives and negatives. There are some types of methods used for the model, including KNN, linear model, and decision tree. This model has some limitations, it is challenging to detect ransomware when files are compressed and image files. In cloud backup systems, it is also challenging to detect ransomware, and only limited ransomware possible to detect. Poudyal et al. [22] combined assembly-level instructions and dlls dataset feature and achieved the highest model accuracy rate of 97.9532% using the Random Forest ML algorithms, and individual (assembly-level instructions

dataset) highest accuracy rate is 97.8916% using AdaBoost with RF ML Classifier. The limitation is ransomware detects sandbox environments but does not execute them. Alhawi et al. categorized two ransomware classes, Locker and Crypto ransomware, then used static and dynamic approaches to detect ransomware and achieved high true positive rates from ElderRan and UNVEL for ransomware detection [23]. There challenge is a lack of comparable studies that can be utilized for the evaluation of assessment metrics. Need more ransomware family datasets to extend existing datasets, because inability to detect ransomware in real time with cloud-based classifier.

2.3 Comparative Analysis and Summary

The main focus of this study is to improve ransomware detection accuracy, implement a more accurate detection model, reduce model false positives and false negative rates, and provide the best hybrid detection model that helps to minimize the threat in cyberspace and provide a more secure system. The hybrid detection model used a large size of dataset for model training and testing, and the dataset was collected from Kaggle, which is an available online platform. First of all, the dataset preprocessing and split dataset into train data and test data sets then implement all necessary steps and complete the detection model. The full model was implemented using Python and I used five machine-learning classifiers combination to develop a hybrid model. Finally, implemented the best hybrid ransomware detection model which is impactful for cyberspace.

2.4 Scope of the Problem

Ransomware attacks have recently become one of the major cybersecurity issues. These attacks are the main cause of the organizations' downtime, the largest money loss they have to face, and the most serious information violations, which include government, health, finance, and other important sectors. Existing ransomware detection solutions follow dynamic analysis techniques which involve a complicated process, and also use only signature-based features, not use network or behavioral based features. Lack of real-time ransomware datasets or mainly focused on limited features, which reason reduces model training performance and detection model accuracy also reduce. In addition, combining different types of information (such as signature-based, network and behavior features) constitutes a heavy technical challenge, especially when handling a high volume of data while ensuring the required computation speed. Addressing these problems requires innovative approaches that combine machine learning with hybrid feature analysis to provide accurate, and scalable ransomware detection solutions. In this case, the hybrid ransomware detection model performs accurately and provides scalable detection solutions.

2.5 Challenges

Establishing the ransomware detection approach is very difficult because ransomware constantly develops characteristics and highly sophisticated evasion tactics. The lack of zero-day ransomware with labeled data complicates the detection process even more. The way of combining signature-based, network, and behavioral

features into one detection model is a difficult task, which requires the implementation of advanced feature selection and data preprocessing techniques. The imbalanced datasets add more issues as they make the training of the model biased thus leading to more false-positive and false-negative. Also, there are many challenges to this study, challenges are:

- Dataset collection
- Data handling
- Preprocessing
- False positives and negatives minimization
- Scalability
- Maintaining detection high accuracy

CHAPTER 3

RESEARCH METHODOLOGY

3.1 Introduction

In this section, we will discuss the research subject, dataset collection procedure, statistical analysis, proposed methodology, and finally talk about which requirements are needed to implement this hybrid ransomware detection model. This is a main part of my research, here I will explain from where I collected the dataset to step by step show model implementation.

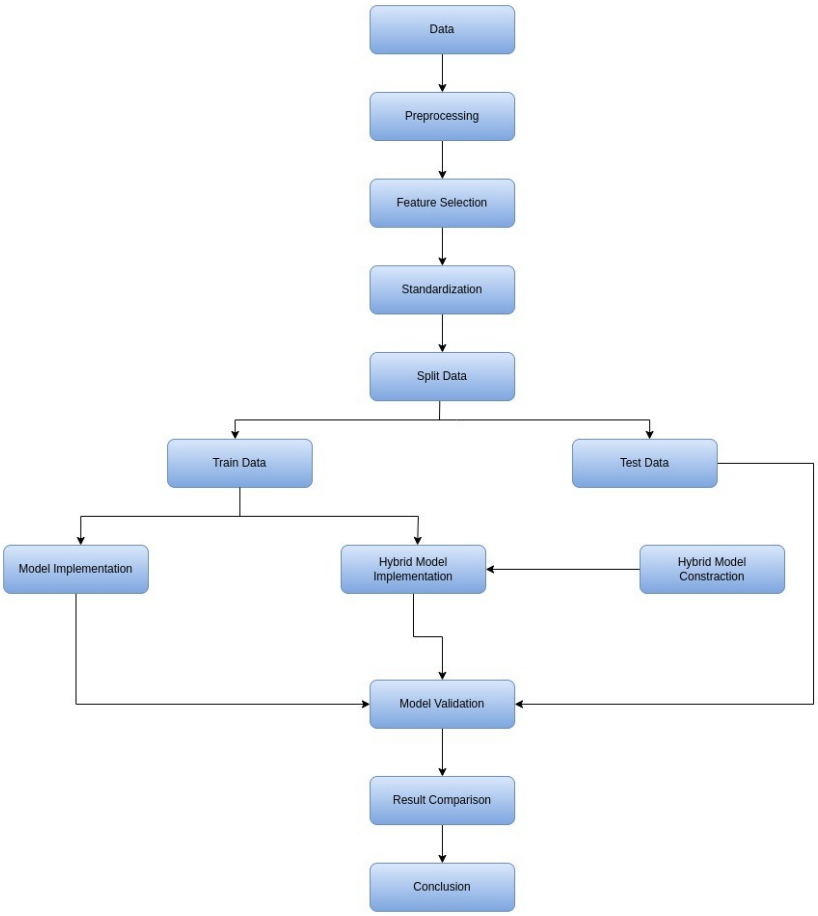

Figure 3.1: Workflow Diagram of Hybrid Model

First of all, we will collect the dataset for this study, then analyze this collected dataset. After collecting the dataset next step is preprocessing the dataset and selecting the future extraction method. Now select the best machine learning algorithms for implementing the hybrid model. In this section, we will select several machine learning algorithms then combine all algorithms and implement a hybrid model. Now split the dataset into three parts, first one is training dataset, second part is validation dataset and third one is testing dataset. After splitting dataset, now train a hybrid machine learning model. Here note that training models are not overfitted or underfitting. When a model is too simple that time is called model is underfitted, and when a model is more complex that time is called model is overfitting [24]. Overcome these two problems and successfully train the machine learning model. After ML model training is completed, collect the model accuracy and try to minimize the model's false positive rates and false negative rates. We will explain step-by-step all processes, which will help to understand easily all processes. Here used more accurate machine learning model, which helps to achieve high model accuracy and reduce the model false positive rates and model false negative rates.

3.2 Research Subject and Instrumentation

For this study, we collected data from Kaggle, which is available online. Based on machine learning studies, datasets are most important or valuable for training machine learning models. In instrument section, we select the Python programming language and use Python environment for implementing the machine learning model. Also, needs to Windows operating system and several Python-based libraries (like Numpy, SkLearn, etc.) to implement the model. And using the Google Colab online platform, where implement the full model using several machine learning algorithms, and train the model then execute the full model. Also need to review the relevant test and analysis of this test. And we need to follow several choices:

- Is the collected dataset trusted?
- From where dataset are collected and how is the data gathered for this project?
- What is the optimal way to organize, preprocess, and manage the dataset?
- Which machine learning algorithms would be most effective for achieving high detection accuracy?

3.2.1 Data Collection Procedure

Data was collected from publicly available repositories and it is direct submission from an organization, where included many types of ransomware family variants of data. It is a trusted source, and many researchers have used same dataset for her research. This dataset was collected from the Kaggle online platform and it is a reputable source. After preparing this dataset, there are two types of data are exist. First one is ransomware variant data and second one is normal data. This dataset split the three sections, model training set, validation set and testing set data. The datasets

included signature-based features, network-related features, and behavioral features. All types of features help to accurately train the model, and when model trains properly, this time we will achieve the best output. Where detection model accuracy rate was achieved high and model false positive rates and negative rates were reduced.

3.3 Correlation Test

The correlation matrix represents relation strength between two variables. It ensures that redundant features don't affect model accuracy. It is calculated to measure linear relationships between features, supporting feature selection and reducing unnecessary dimensions. Analysis of all features and develop a correlation between one feature to another feature, and showed a strong positive correlation matrix. This matrix helps to improve the model accuracy. Now we will illustrate the correlation matrix and show the correlation between all features.

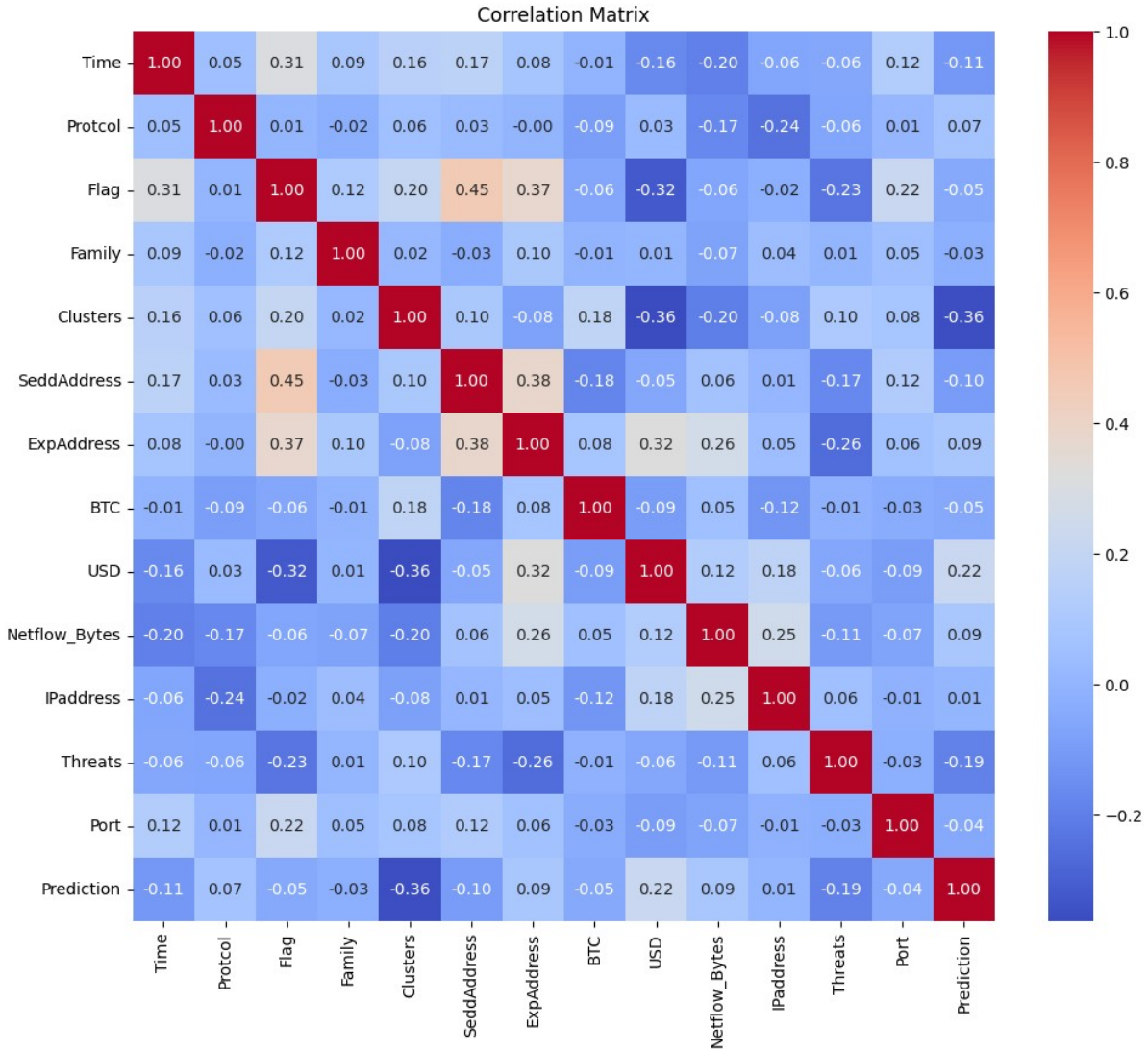

Figure 3.2: Correlation matrix between all features

3.4 Statistical Analysis

There are many types of ransomware variants exist in the dataset, and also have normal data. Dataset is one of the most important parts of model implementation. In hybrid model, we used four machine learning models, models including DT, RF, and KNN. We combine these four ML models and implement a hybrid model for ransomware detection.

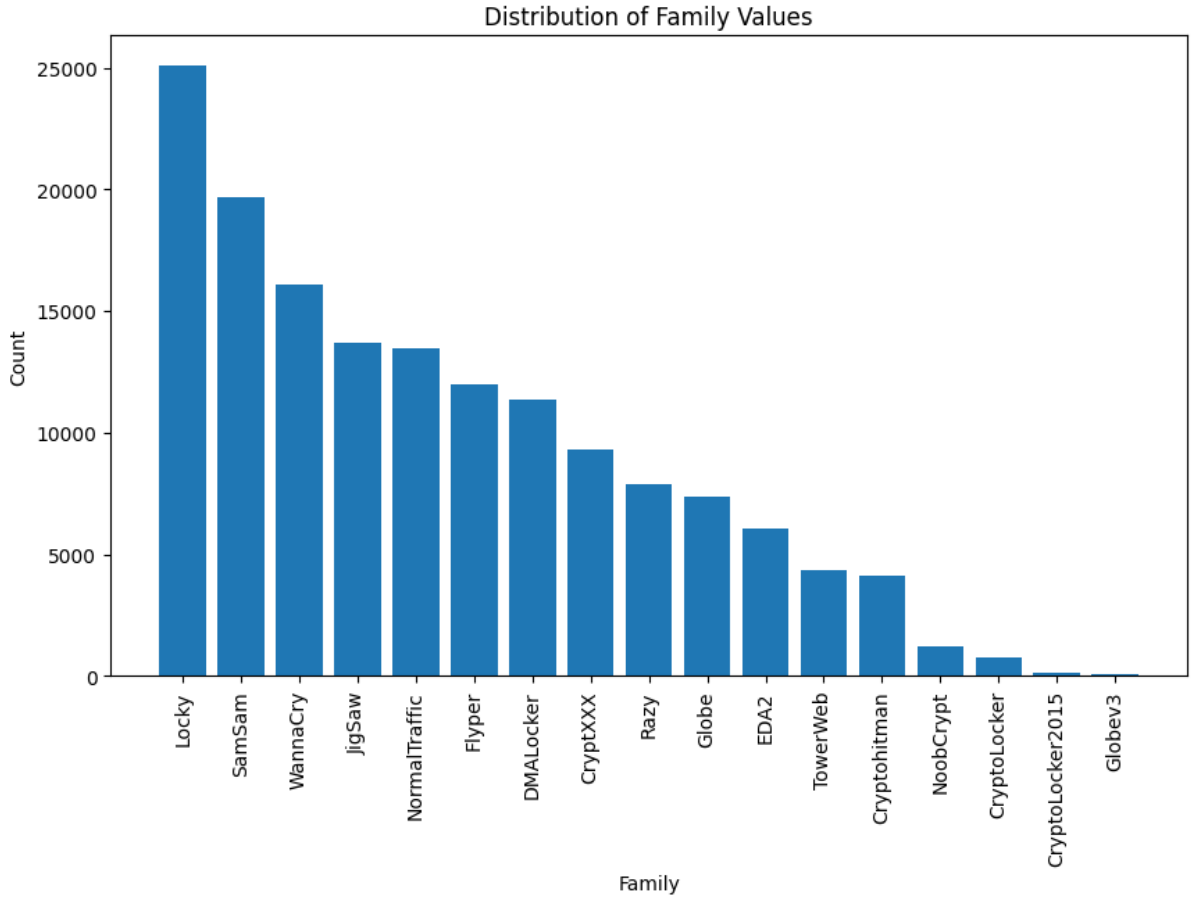

Figure 3.3: Ransomware family variants and normal traffic

In Figure 3.4, the bar graph shows normal traffic, ransomware variants, and the number of data. Explained as follows every variant of ransomware and normal traffic.

Locky: It is a highly destructive ransomware variant that first appeared in 2016 [25]. It typically spreads through email attachments. Encrypt the sensitive information files using strong AES encryption algorithms then demand payment in Bitcoin.

SamSam: SamSam ransomware is developed and operated by BOSS SPIDER [26]. Known for targeting healthcare and government organizations. SamSam ransomware also known as MSIL/Samas.A [27]. SamSam is a manual ransomware that is often delivered via brute-force attacks on weak passwords. It uses a variety of encryption techniques.

WannaCry: WannaCry ransomware variants exploited the Windows Server Message Block (SMB) protocol vulnerability in 2017. Then encrypt files and demand Bitcoin ransom. This time impacted over 200,000 systems globally and disrupted industries like healthcare and finance [28]. This ransomware spreads by itself in the victim's system.

JigSaw: This variant was known for its aggressive tactics, often deleting files progressively if victims didn't pay. It displayed a sadistic countdown, threatening to delete files unless the ransom was paid [29].

Normal Traffic: Normal network traffic refers to the expected flow of data packets across a network during a specific period.

Flyper: It is distributed through malicious email links or cracked software downloads. Flyper encrypts files and demands a Bitcoin payment for decryption. It uses RSA and AES algorithms for file encryption and it is also dangerous because encrypts many files in a short time [30].

DMALocker: It targets mainly enterprises. It encrypts files using AES-256 algorithms and locks users out of their systems, demanding payment to restore access [31]. It's often delivered through phishing attacks.

CryptXXX: CryptXXX was first identified in 2016. It targeted video files and other media files, demanding Bitcoin for decryption. It also used AES-256 algorithms to encrypt the file [32].

Razy: This type of ransomware is distributed via fake installers or malicious websites [33]. It encrypts files and demands a ransom for the decryption key, and often tries to steal personal information as well.

Globe: This ransomware uses spam emails to infect users. Used Blowfish encryption and .purge file extension to encrypt files [34]. The ransom demands in Bitcoin, and given a deadline for payment.

EDA2: It is a Globe family variant ransomware. It encrypts files and displays ransom notes with demands. This type of ransomware targets individual users [35].

TowerWeb: This ransomware targets web servers. It encrypts files on the server, affecting websites and their data. The ransom is demanded in Bitcoin to unlock the files.

Cryptohitman: Cryptohitman usually targets files and demands payment for decryption. It uses .porno and .pornoransom extensions for file encryption [36].

NoobCrypt: NoobCrypt was first identified in July 2016. It encrypts files using AES-256 algorithms and demands a ransom payment.

CryptoLocker: It is one of the most infamous ransomware variants. It was first identified in 2013. It is delivered through malicious email attachments, when victim clicks the link or attachment ransomware installs into the system [37]. It uses an

asymmetric encryption method to encrypt files and demands Bitcoin for a decryption key.

CryptoLocker2015: CryptoLocker is a variant of CryptoLocker. It is also encrypting files and demanding Bitcoin for a decryption key.

Globev3: It was first identified in 2017. It uses AES-256 algorithms to encrypt the files. After encrypting the files they demand a ransom payment. It mainly used .decrypt2017 and .hnumkhotep file extensions [38]. It is delivered via malicious email attachments or links.

3.5 Voting Classifier

The Voting Classifier is an ensemble learning technique that combines the predictions of multiple models to enhance overall accuracy. It integrates a collection of diverse base models, such as DT, RF, or KNN, trained on the same dataset. The architecture processes input features through these models and aggregates their predictions to produce a final output [39]. This collaborative approach leverages the strengths of individual models while minimizing their weaknesses, making the Voting Classifier a powerful method for improving prediction performance.

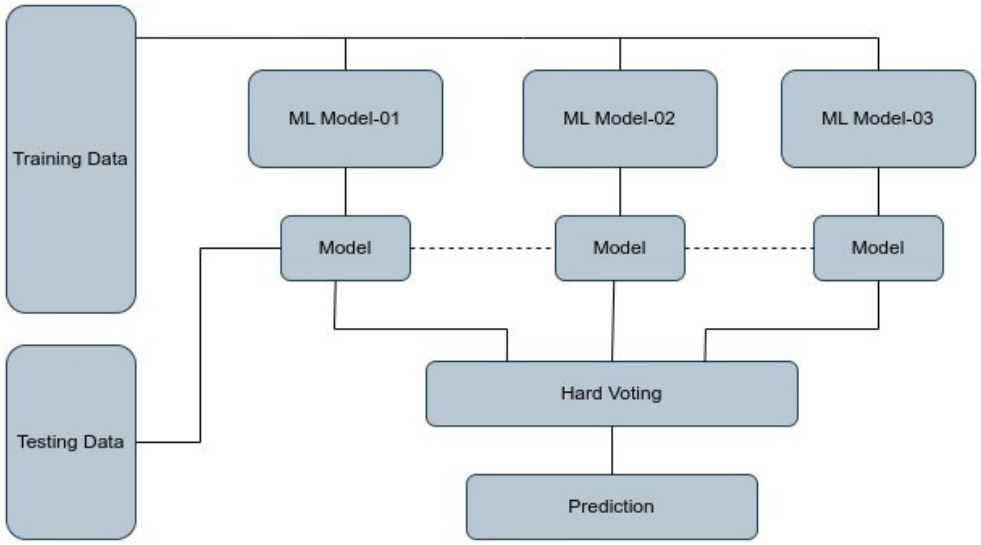

Figure 3.4: Voting classifier architecture

In voting classification two type of voting modes: hard voting and soft voting. In hybrid model implementation we used hard voting mode. Hard voting method combining predictions from multiple classifiers. Each classifier first makes its own prediction, and the final decision is determined by the majority vote among them [40]. For example, if

three classifiers predict the output classes as (X, Y, X), the majority vote is for class X. As a result, X will be the final prediction.

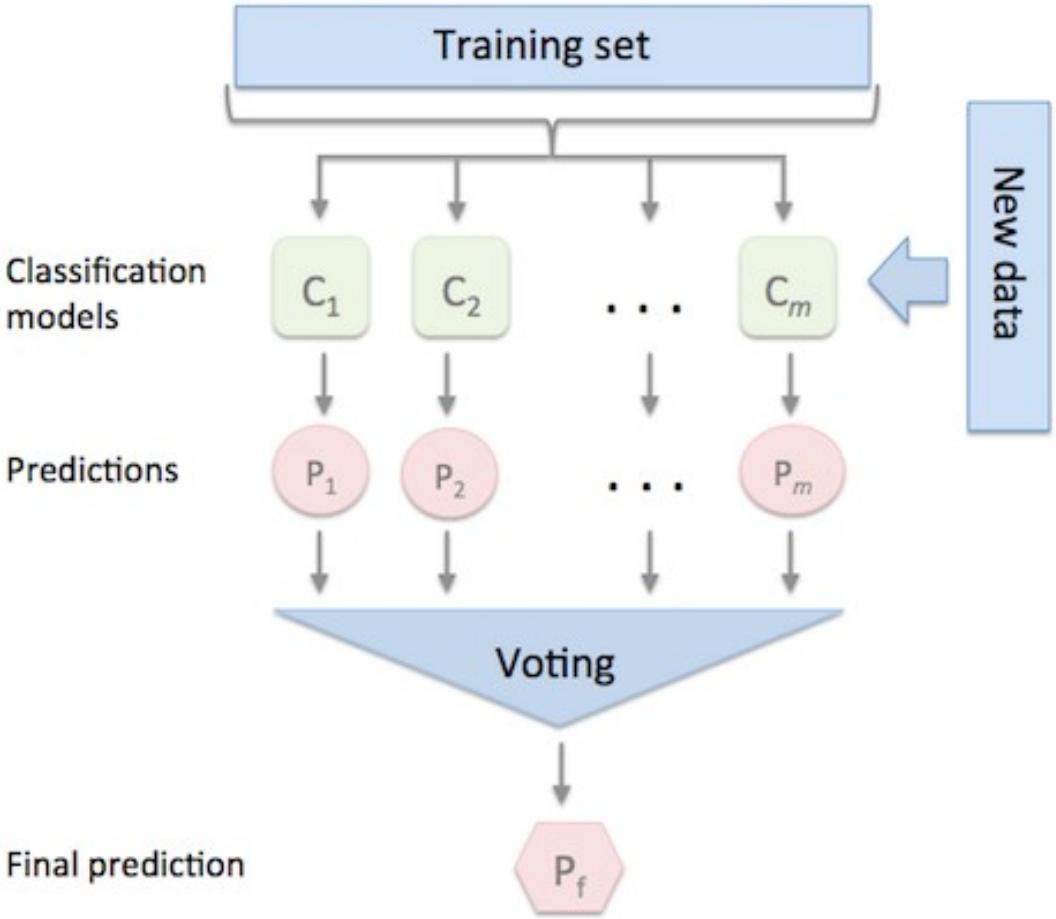

Figure 3.5: Hard voting architecture

3.6 Proposed Methodology

Several methods or techniques were used in this research and achieve the high detection accuracy model. Here we will explain every step of our proposed methodology.

- Data Collection: We collected the dataset from online resources. It is a trustable resource. After collecting the dataset from online resources, first of all preprocess the dataset.
- Data Processing: Analyzed the dataset and handled the missing value. Remove all duplicate values in the data processing time.

- Feature selection: Select all features which is mostly related to the target feature.
- Standardization: Used StandardScaler preprocessing technique to standardize all features that help to improve algorithm compatibility, model performance, and training speed.
- Data Split: After standardization of the dataset, now prepare the dataset for model training, validation, and testing. Entire dataset split the three sections, first one is training dataset, second one is validation dataset and another is testing dataset.
- Model Selection: In this case, we will select the best machine learning model for implementing a hybrid ransomware detection model.
- Voting Classifier: Now use the voting classifier and implement the hybrid model. After implement the hybrid model then model train and test.
- Performance Evaluation: Now we will evaluate the proposed model result. After completing the all implementation steps then execute the hybrid model. Collect the model result and compare this result between existing model and proposed model. Analyze the model accuracy, precision, recall, and f1 score for training dataset, validation dataset and testing dataset. Also, analyze the model false positive rates and false negative rates. Finally generated a confusion matrix that helped to the understand dataset correlation of every feature.

3.7 Implementation Requirements

Require software and hardware to implement the hybrid ransomware detection model. In this case, we will use Python programming language to implement the machine learning based model.

Python 3.13.0: At current time Python latest version is 3.13.0. It is the most popular programming language for implementing the AI or machine learning based model. This programming language has a large ecosystem of libraries. For dataset processing using Pandas and NumPy libraries, also used Scikit-learn or TensorFlow libraries for training models, and matplotlib was used for result visualization.

Google Collab: It is an open-source and free online based platform. It supports the Python programming language and also supports all Python libraries. It also provides free access to powerful hardware accelerators like GPUs and TPUs. It also provides a Jupyter Notebook environment and it is user friendly interface.

Hardware and Software Requirements: We need hardware and software to implement and execute this project.

- Windows Operating System (OS 8 or higher)
- Web browser (chrome, Firefox, etc.)
- RAM(at least 4 GB)
- SSD (minimum 120 GB)

CHAPTER 4

RESULTS AND DISCUSSION

4.1 Introduction

This section explain the hybrid ransomware detection model result, discusses also which algorithms are used and finally compare between existing detection model accuracy and proposed model accuracy. The entire model has several steps and completes every step, then executes the machine learning model and achieves the final output. Hybrid ransomware detection model results are explained step by step below.

4.2 Experimental Results & Analysis

In the cybersecurity area ML model or any type of model can't provide perfect results because threats are continuously changing and attackers use advanced attack techniques and tactics. In the cybersecurity area emerging threats are continuously coming. It is challenging to handle the emerging threats, also more difficult to detect every threat. But it is possible to mitigate the threats and reduce the incident impact. I develop two hybrid detection models for ransomware detection. In the hybrid model, I used several advanced machine learning models to identify known ransomware patterns and compare the behavioral patterns of ransomware. I used a total three machine learning models to implement the hybrid model, three models are DT, RF, and KNN. After executing the hybrid model, I found the model highest accuracy is 97.48%, precision is 98%, recall is 98% and f1-score is 98%. Also, I achieved another goal is to reduce the model's false positive and false negative rates. The hybrid model's false positive rate is 0.93% and false negative rate is 2.12%. The second ransomware detection hybrid model accuracy achieved 97.17%.

4.2.1 Algorithms

Hybrid model implementation time i was used several advanced machine learning model combinations including DT, RM, and KNN. Combining these three models helps to detect ransomware more accurately and achieve our goal. We implemented two hybrid models, for first hybrid model implementation time used DT and RF machine learning model, and second hybrid model implementation time used

DT and KNN machine learning model. Now shown two hybrid model classification reports and confusion matrix below:

Hybrid Model-01 Accuracy: 0.9748

Classification Report:

	precision	recall	f1-score	support
0	0.96	0.97	0.96	12813
1	1.00	1.00	1.00	4057
2	0.98	0.98	0.98	19847
3	0.98	0.98	0.98	12029
accuracy			0.97	48746
macro avg	0.98	0.98	0.98	48746
weighted avg	0.97	0.97	0.97	48746

Figure 4.1: Classification Report of Hybrid Model-01

Hybrid Model-02 Accuracy: 0.9717

Classification Report:

	precision	recall	f1-score	support
0	0.95	0.97	0.96	12813
1	1.00	1.00	1.00	4057
2	0.98	0.97	0.97	19847
3	0.98	0.97	0.97	12029
accuracy			0.97	48746
macro avg	0.98	0.98	0.98	48746
weighted avg	0.97	0.97	0.97	48746

Figure 4.2: Classification Report of Hybrid Model-02

A confusion matrix is a table that shows the performance of a machine learning model by comparing predicted and actual values. Here mainly focus on four key points, for example, true positive, true negative, false positive, and false negative.

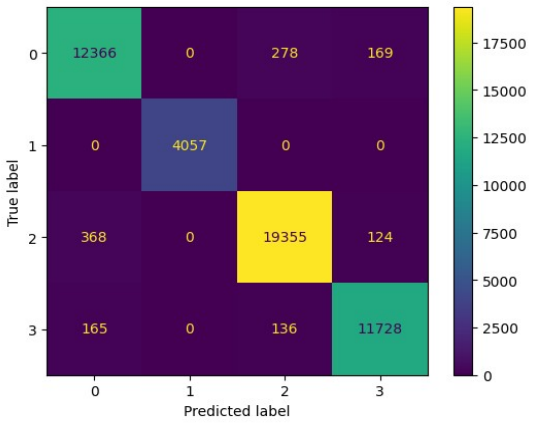

Figure 4.3: Confusion matrix of Model-01

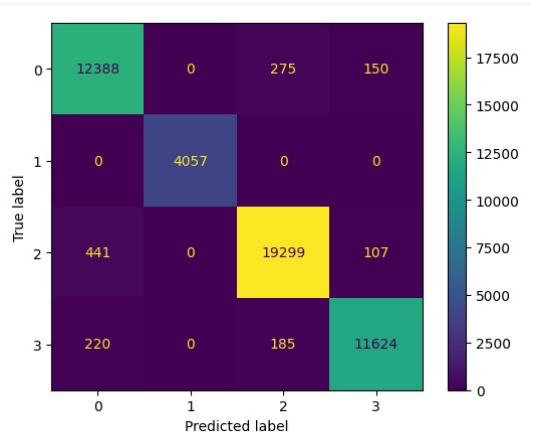

Figure 4.4: Confusion matrix of Model-02

4.3 Model Accuracy Compare

Now show the comparison of all model and Zhang et al. [8] model:

Model	Training Execution Time	Testing Execution Time	Accuracy From Zhang et al. [8]	Accuracy From This Research	F1-Score	Precision	Recall
DT	0.20	0.09	86.57%	91.41%	93.00%	93.00%	93.00%
RM	13	1.09	91.43%	91.98%	93.00%	94.00%	93.00%
KNN	0.50	5	88.19%	92.38%	93.00%	93.00%	93.00%
GBDT	51.82	0.58	89.98%	94.13%	95.00%	95.00%	95.00%
PM-01	4	0.53	N/A	97.48%	98.00%	98.00%	98.00%
PM-02	0.39	4	N/A	97.17%	98.00%	98.00%	98.00%

Table 4.3.1: Comparison of all model results

Here existing ransomware detection model accuracy is 91.43% and the proposed hybrid ransomware model accuracy is 97.48%.

4.4 Discussion

Developed the hybrid model using four machine-learning techniques. This hybrid model detects ransomware threats and reduces threats in cyberspace. The main goal of this study, reduce the ransomware threat in cybersecurity sector and provide a more secure digital environment. Many machine-learning algorithm combinations are used to implement this hybrid model. I trained this model accurately and tested the model performance. Finally achieved high detection model accuracy, and low model false positive rates and low false negative rates.

CHAPTER 5

CONCLUSION

5.1 Summary of the Study

The study focused on developing a hybrid ransomware detection model that provides high detection accuracy. It also minimizes the model false positives and false negatives rates and finally provides a scalable detection model. Into the dataset, a total 17 types of ransomware family variants data exist, and this large size of the dataset is used to model training and testing, this dataset mainly focused on signature-based features, network, and behavioral features. After successfully implementing the hybrid detection model, this detects known and unknown variants of ransomware and ensures a reliable ransomware detection model with minimal misclassification. Existing ransomware detection approaches have many serious drawbacks, and hacker groups use those vulnerabilities. When a hacker group compromises any system that time it is most dangerous and harmful for individuals or any type of organization. There are a number of challenges in the existing ransomware detection model such as the issue of dealing with imbalanced data, difficulties in incorporation of complex features, problems with accurate detection in a large-scale environment, and high rates of false positives and negatives. The study solves those challenges and provides a more robust, hybrid, and scalable approach. The research contributes to the cybersecurity field and provides an efficient solution for ransomware detection.

5.2 Conclusions

Ransomware is a major threat in cybersecurity field and existing ransomware detection models struggle to detect ransomware accurately. Overcome this challange proposed a hybrid ransomware detection approach. In the ransomware detection model used advanced machine-learning algorithms and improved ransomware detection accuracy, minimized the model false positive and false negative rates, and provided accurate and scalable ransomware detection solutions. The hybrid ransomware detection model analyzes the signature-based features, network, or behavioral features and detects ransomware. Proposed machine-learning model successfully integrated hybrid features and achieved enhanced detection accuracy. This study provides a scalable and efficient solution. These hybrid detection model strengthen defenses against ransomware and enhance system security.

5.3 Implication for Further Study

Cybersecurity is a large sector and here emerging threats are continuously coming every moment. That reason it is more difficult to detect every threat, but it is possible to reduce threats and impacts. Ransomware attacks are one of the most dangerous and harmful attacks in cybersecurity sector. Ransomware always upgrades her characteristics and changes attack tactics and techniques. That reason it is more difficult to detect accurately. This study has limitations, the primary limitation is real-time ransomware variants are not detected accurately. It is the future study scop, where work with dynamic datasets, which datasets continuously update with new ransomware samples and deploy ransomware detection model that model performs real-time ransomware detection in large-scale environments, and also effective against the latest ransomware threats. Another limitation is lack of a real-time ransomware dataset. Dataset is one of the most important parts of model training and testing. If those limitations can be overcome, the ransomware detection model will work more accurately in real-time, and is possible to identify emerging ransomware threats.

REFERENCES

1. Cen, M., Jiang, F., Qin, X., Jiang, Q., & Doss, R. (2024). Ransomware early detection: A survey. Computer Networks, 239, 110138.
2. Petya Ransomware. Cybersecurity and Infrastructure Security Agency CISA. (2018, February 15). https://www.cisa.gov/news-events/alerts/2017/07/01/petya-ransomware#:~:text=Solution,encrypted%20files%20will%20be%20released.
3. ThreatDown Newsletter. (2024, September 20). 2024 State of Ransomware Report. ThreatDown. https://www.threatdown.com/dl-state-of-ransomware-2024/
4. Tanner, A., & Bleich, K. (2024, August 9). Ransomware review: First half of 2024. Unit 42. https://unit42.paloaltonetworks.com/unit-42-ransomware-leak-site-data-analysis/
5. Gihon, S. (2024, October 13). *Ransomware groups report 2024 - Q3*. Cyberint. https://cyberint.com/blog/research/ransomware-trends-2024-report/
6. Argene, M., Ravenscroft, C., & Kingswell, I. (2024). Ransomware detection via cosine similarity-based machine learning on bytecode representations.
7. Federal Bureau of Investigation. (2024). Ransomware. FBI. https://www.fbi.gov/how-we-can-help-you/scams-and-safety/common-frauds-and-scams/ransomware
8. Zhang, H., Xiao, X., Mercaldo, F., Ni, S., Martinelli, F., & Sangaiah, A. K. (2019). Classification of ransomware families with machine learning based onN-gram of opcodes. Future Generation Computer Systems, 90, 211-221.
9. Xu, B., & Wang, S. (2024). Examining windows file system irp operations with machine learning for ransomware detection.
10. Alhashmi, A. A., Darem, A. A., Alshammari, A. B., Darem, L. A., Sheatah, H. K., & Effghi, R. (2024). Ransomware Early Detection Techniques. Engineering, Technology & Applied Science Research, 14(3), 14497-14503.
11. Berardi, D., Giallorenzo, S., Melis, A., Melloni, S., Onori, L., & Prandini, M. (2023). Data flooding against ransomware: Concepts and implementations. Computers & Security, 131, 103295.
12. Ali, R., Ali, A., Iqbal, F., Hussain, M., & Ullah, F. (2022). Deep learning methods for malware and intrusion detection: A systematic literature review. Security and Communication Networks, 2022(1), 2959222.

13. Hussain, A., Asif, M., Ahmad, M. B., Mahmood, T., & Raza, M. A. (2022, April). Malware detection using machine learning algorithms for windows platform. In Proceedings of International Conference on Information Technology and Applications: ICITA 2021 (pp. 619-632). Singapore: Springer Nature Singapore.
14. Reshmi, T. R. (2021). Information security breaches due to ransomware attacks-a systematic literature review. International Journal of Information Management Data Insights, 1(2), 100013.
15. Kapoor, A., Gupta, A., Gupta, R., Tanwar, S., Sharma, G., & Davidson, I. E. (2021). Ransomware detection, avoidance, and mitigation scheme: a review and future directions. Sustainability, 14(1), 8.
16. James, A. V., & Sabitha, S. (2021). Malware attacks: A survey on mitigation measures. In Second International Conference on Networks and Advances in Computational Technologies: NetACT 19 (pp. 1-11). Springer International Publishing.
17. Martins, N., Cruz, J. M., Cruz, T., & Abreu, P. H. (2020). Adversarial machine learning applied to intrusion and malware scenarios: a systematic review. IEEE Access, 8, 35403-35419.
18. Zimba, A., & Chishimba, M. (2019). Understanding the evolution of ransomware: paradigm shifts in attack structures. International Journal of computer network and information security, 11(1), 26.
19. Maigida, A. M., Abdulhamid, S. I. M., Olalere, M., Alhassan, J. K., Chiroma, H., & Dada, E. G. (2019). Systematic literature review and metadata analysis of ransomware attacks and detection mechanisms. Journal of Reliable Intelligent Environments, 5, 67-89.
20. Kok, S., Abdullah, A., Jhanjhi, N., & Supramaniam, M. (2019). Ransomware, threat and detection techniques: A review. Int. J. Comput. Sci. Netw. Secur, 19(2), 136.
21. Lee, K., Lee, S. Y., & Yim, K. (2019). Machine learning based file entropy analysis for ransomware detection in backup systems. IEEE access, 7, 110205-110215.
22. Poudyal, S., Subedi, K. P., & Dasgupta, D. (2018, November). A framework for analyzing ransomware using machine learning. In 2018 IEEE symposium series on computational intelligence (SSCI) (pp. 1692-1699). IEEE.

23. Alhawi, O. M., Baldwin, J., & Dehghantanha, A. (2018). Leveraging machine learning techniques for windows ransomware network traffic detection. Cyber threat intelligence, 93-106.
24. Amazon Web Services. (2024, January 25). Model Fit: Underfitting vs. Overfitting. AWS. https://docs.aws.amazon.com/machine-learning/latest/dg/model-fit-underfitting-vs-overfitting.html
25. CISA.gov. (2016, September 29). Ransomware and Recent Variants. Cybersecurity and Infrastructure Security Agency. https://www.cisa.gov/news-events/alerts/2016/03/31/ransomware-and-recent-variants
26. karansood. (2018, May 21). An In-Depth Analysis of Samsam Ransomware and BOSS SPIDER. CrowdStrike. https://www.crowdstrike.com/en-us/blog/an-in-depth-analysis-of-samsam-ransomware-and-boss-spider/
27. CISA.gov. (2018, December 3). SamSam Ransomware. Cybersecurity and Infrastructure Security Agency. https://www.cisa.gov/news-events/cybersecurity-advisories/aa18-337a
28. Cloudflare. (2017, May 12). What was the WannaCry ransomware attack?. Cloudflare. https://www.cloudflare.com/learning/security/ransomware/wannacry-ransomware/
29. SonicWall. (2019, December 21). Jigsaw ransomware variant: Melka, easily reveals decryption key. Sonicwall. https://www.sonicwall.com/blog/jigsaw-ransomware-variant-melka-easily-reveals-decryption-key
30. Glushko, B. (2023, April 11). Flyper ransomware data recovery. SalvageData. https://www.salvagedata.com/flyper-ransomware-data-recovery/
31. Hasherezade, H. (2016, May 23). DMA Locker 4.0: Known ransomware preparing for a massive distribution. Malwarebytes Labs. https://www.malwarebytes.com/blog/news/2016/05/dma-locker-4-0-known-ransomware-preparing-for-a-massive-distribution
32. Wang, D., & Xu, H. (2016, August 22). CryptXXX Ransomware Emerges For a Slice of the Pie. Fortinet. https://www.fortinet.com/blog/threat-research/cryptxxx-ransomware-emerges-for-a-slice-of-the-pie
33. Bisson, D. (2019, January 28). Razy Trojan Installs Malicious Browser Extensions to Steal Cryptocurrency. Security Intelligence.

https://securityintelligence.com/news/razy-trojan-installs-malicious-browser-extensions-to-steal-cryptocurrency/

34. Abrams, L. (2016, August 24). The Globe Ransomware wants to Purge your Files. BleepingComputer. https://www.bleepingcomputer.com/news/security/the-globe-ransomware-wants-to-purge-your-files/
35. News, S. (2016, March 15). New EDA2-Based Ransomware Easily Neutralized. https://www.securityweek.com/new-eda2-based-ransomware-easily-neutralized/
36. Meskauskas, T. (2021, December 27). Cryptohitman ransomware. PCrisk. https://www.pcrisk.com/removal-guides/10018-cryptohitman-ransomware
37. Stouffer, C. (2022, October 12). What is CryptoLocker? an overview + prevention tips. Norton. https://us.norton.com/blog/malware/cryptolocker
38. Emsisoft. (2017, June 4). Globe3 Decryptor. Emsisoft. https://www.emsisoft.com/en/ransomware-decryption/globe3/
39. Awan, F. M., Saleem, Y., Minerva, R., & Crespi, N. (2020). A comparative analysis of machine/deep learning models for parking space availability prediction. Sensors, 20(1), 322.
40. Rutecki, M. (2023, February 26). Voting classifier for better results. Kaggle. https://www.kaggle.com/code/marcinrutecki/voting-classifier-for-better-results

e

ORIGINALITY REPORT

23%	18%	13%	16%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	Submitted to Midlands State University Student Paper	2%
2	dspace.daffodilvarsity.edu.bd:8080 Internet Source	1%
3	Submitted to University of North Carolina, Greensboro Student Paper	1%
4	Submitted to Bowie State University Student Paper	1%
5	Submitted to Champlain College Student Paper	1%
6	"The New Normal and Its Impact on Society", Springer Science and Business Media LLC, 2024 Publication	1%
7	Submitted to University of Central Lancashire Student Paper	1%
8	umpir.ump.edu.my Internet Source	1%

9	journals.stmjournals.com Internet Source	1 %
10	insights2techinfo.com Internet Source	<1 %
11	Daksh, Mohit Sharma, N. Gayathri. "lIoT enabled Covid Prevention System with YOLOv4", 2022 2nd International Conference on Advance Computing and Innovative Technologies in Engineering (ICACITE), 2022 Publication	<1 %
12	jisis.org Internet Source	<1 %
13	journals.riverpublishers.com Internet Source	<1 %
14	Submitted to University of Gloucestershire Student Paper	<1 %
15	Submitted to Edith Cowan University Student Paper	<1 %
16	www.etasr.com Internet Source	<1 %
17	Submitted to Aspen University Student Paper	<1 %
18	Submitted to Study Group Australia Student Paper	<1 %

19	Submitted to University of Oklahoma Student Paper	<1 %
20	Submitted to Daffodil International University Student Paper	<1 %
21	dergipark.org.tr Internet Source	<1 %
22	ir.knust.edu.gh Internet Source	<1 %
23	sciencebibliographies.strategian.com Internet Source	<1 %
24	Submitted to American Public University System Student Paper	<1 %
25	air.unimi.it Internet Source	<1 %
26	www2.mdpi.com Internet Source	<1 %
27	Manabu Hirano, Ryotaro Kobayashi. "RanSMAP: Open dataset of Ransomware Storage and Memory Access Patterns for creating deep learning based ransomware detectors", Computers & Security, 2024 Publication	<1 %
28	Submitted to Johns Hopkins Unversity Student Paper	<1 %

29	Submitted to Southern New Hampshire University - Continuing Education Student Paper	<1 %
30	Submitted to University of Central Florida Student Paper	<1 %
31	eprints.nottingham.ac.uk Internet Source	<1 %
32	ouci.dntb.gov.ua Internet Source	<1 %
33	Submitted to Queen Mary and Westfield College Student Paper	<1 %
34	Submitted to Napier University Student Paper	<1 %
35	arxiv.org Internet Source	<1 %
36	Submitted to University of Arizona Student Paper	<1 %
37	Submitted to TechKnowledge Student Paper	<1 %
38	Submitted to University of Essex Student Paper	<1 %
39	Submitted to University of Queensland Student Paper	<1 %

40	di.univ-blida.dz Internet Source	<1 %
41	ebin.pub Internet Source	<1 %
42	www.researchgate.net Internet Source	<1 %
43	Mohiuddin Ahmed. "Ransomware Evolution", CRC Press, 2024 Publication	<1 %
44	Submitted to University of Hertfordshire Student Paper	<1 %
45	Submitted to University of Westminster Student Paper	<1 %
46	assets-eu.researchsquare.com Internet Source	<1 %
47	Eton Blue, Gregory Campbell, Andrew Stokes, Lawrence Thompson, James Clarke. "Ransomware Detection on Linux Operating System Using Recurrent Neural Networks with Binary Opcode Analysis", Open Science Framework, 2024 Publication	<1 %
48	Submitted to Georgia Institute of Technology Main Campus Student Paper	<1 %

49	Submitted to University of East London Student Paper	<1%
50	Kyungroul Lee, Sun-Young Lee, Kangbin Yim. "Machine Learning Based File Entropy Analysis for Ransomware Detection in Backup Systems", IEEE Access, 2019 Publication	<1%
51	Samsul Ariffin Abdul Karim, Anand J. Kulkarni, Chin Kim On, Mohd Hanafi Ahmad Hijazi. "Intelligent Systems of Computing and Informatics", CRC Press, 2024 Publication	<1%
52	Thomas Lowev, Charlotte Fisher, James Collins. "Advanced Ransomware Detection and Classification via Semantic Analysis of Memory Opcode Patterns", Open Science Framework, 2024 Publication	<1%
53	Submitted to De La Salle University - Manila Student Paper	<1%
54	da Silva Moura, João Carlos Zêzere. "Smart Techniques and Tools to Detect Steganography a Viable Practice to Security Office Department", Universidade NOVA de Lisboa (Portugal), 2024 Publication	<1%

55	William Labone, Nicholas Brown, Stephen Bellini, Catherine Williams, Timothy Flores, Patrick Johansson. "Unidirectional and Bidirectional Machine Learning Models for Ransomware Detection via Malicious Opcode Discovery", Open Science Framework, 2024 Publication	<1 %
56	s-space.snu.ac.kr Internet Source	<1 %
57	Ibrahim Bello, Haruna Chiroma, Usman A. Abdullahi, Abdulsalam Ya'u Gital et al. "Detecting ransomware attacks using intelligent algorithms: recent development and next direction from deep learning and big data perspectives", Journal of Ambient Intelligence and Humanized Computing, 2020 Publication	<1 %
58	e-archivo.uc3m.es Internet Source	<1 %
59	repository.sustech.edu Internet Source	<1 %
60	www.misp.software Internet Source	<1 %
61	Eric Landril, Samuel Valente, Gregory Andersen, Christopher Schneider. "Ransomware Detection through Dynamic	<1 %

Behavior-Based Profiling Using Real-Time Crypto-Anomaly Filtering", Open Science Framework, 2024
Publication

---

62 Kelley, Joseph. "Multi-step Prediction With Neural Networks", Oklahoma State University, 2024 <1%
Publication

---

63 M. Affan Badar, Ruchika Gupta, Priyank Srivastava, Imran Ali, Elizabeth A. Cudney. "Handbook of Digital Innovation, Transformation, and Sustainable Development in a Post-Pandemic Era", CRC Press, 2024 <1%
Publication

---

64 Oliver Anka, Annabelle Clarke, Benjamin Dixon, James Hall. "Quantum-Lattice Feature Extraction for Ransomware Detection Using Multi-Dimensional Cryptographic Signatures", Open Science Framework, 2024 <1%
Publication

---

65 Xianwei Gao, Changzhen Hu, Chun Shan, Weijie Han. "MaliCage: A packed malware family classification framework based on DNN and GAN", Journal of Information Security and Applications, 2022 <1%
Publication

---

66 acikerisim.karabuk.edu.tr:8080

	Internet Source	<1%
67	dokumen.pub Internet Source	<1%
68	mdpi-res.com Internet Source	<1%
69	peerj.com Internet Source	<1%
70	repository.stcloudstate.edu Internet Source	<1%
71	tailieuso.udn.vn Internet Source	<1%
72	vulners.com Internet Source	<1%
73	www.mdpi.com Internet Source	<1%
74	www.techtarget.com Internet Source	<1%
75	Elvis Bennett, Jasper Ellington, Gideon Blackstone, Hugo Whitfield, Leon Ashcroft. "Enhanced Vectorized Ransomware Detection: A Novel Spectral Segmentation Approach Using Nonlinear Frequency Patterns", Open Science Framework, 2024 Publication	<1%