CYBER FRAUD - DETECTION AND ANALYSIS OF THE CRYPTO-RANSOMWARE

A report submitted in partial fulfillment of the requirements for the Degree of

Bachelor of Technology

In

COMPUTER SCIENCE ENGINEERING (Cybersecurity)

BY

K.L. GEETESH	2011CS040035
K. KEDARI NEHA	2011CS040034
D. VINEETH KUMAR	2011CS040020
A. CHANDAN	2011CS040001

Under the esteemed guidance of

P. SHANMUKHA KUMAR

Assistant Professor

Department of Computer Science & Engineering (Cyber Security)

School of Engineering

MALLA REDDY UNIVERSITY

Maisammaguda, Dulapally, Hyderabad, Telangana 500100

2024

CYBER FRAUD - DETECTION AND ANALYSIS OF THE CRYPTO-RANSOMWARE

A report submitted in partial fulfillment of the requirements for the Degree of

Bachelor of Technology

In

COMPUTER SCIENCE ENGINEERING (Cybersecurity)

BY

K.L. GEETESH	2011CS040035
K. KEDARI NEHA	2011CS040034
D.VINEETH KUMAR	2011CS040020
A. CHANDAN	2011CS040001

Under the esteemed guidance of

P. SHANMUKHA KUMAR

Assistant Professor

Department of Computer Science Engineering (Cybersecurity)

School of Engineering

MALLA REDDY UNIVERSITY

Maisammaguda, Dulapally, Hyderabad, Telangana 500100

2024

MALLA REDDY UNIVERSITY

(Telangana State Private Universities Act No.13 of 2020 and G.O.Ms.No.14, Higher Education (UE) Department)

Department of Computer Science & Engineering (Cybersecurity)

CERTIFICATE

This is to certify that the project report entitled **"CYBER FRAUD - DETECTION AND ANALYSIS OF THE CRYPTO-RANSOMWARE"**, submitted by **K.L.GEETESH (2011CS040035), K.KEDARI NEHA (2011CS040034), D.VINEETH KUMAR (2011CS040020), A.CHANDAN (2011CS040001),** towards the partial fulfillment for the award of Bachelor's Degree in CSE-Cybersecurity from the **Department of Computer Science & Engineering (Cybersecurity), Malla Reddy University,** Hyderabad, is a record of bonafide work done by him/ her. The results embodied in the work are not submitted to any other University or Institute for award of any degree or diploma.

Internal Guide:
P. Shanmukha kumar
Assistant Professor

Head of the Department
Dr. G. Anand Kumar
CSE(Cyber Security & IoT)

External Examiner

DECLARATION

We hereby declare that the project report entitled "**CYBER FRAUD - DETECTION AND ANALYSIS OF THE CRYPTO-RANSOMWARE**" has been carried out by us and this work has been submitted to the **Department of Computer Science & Engineering (Cybersecurity), Malla Reddy University,** Hyderabad in partial fulfillment of the requirements for the award of degree of Bachelor of Technology. We further declare that this project work has not been submitted in full or part for the award of any other degree in any other educational institutions.

Place:

Date:

K.L.GEETESH	2011CS040035
K.KEDARI NEHA	2011CS040034
D.VINEETH KUMAR	2011CS040020
A.CHANDAN	2011CS040001

ACKNOWLEDGEMENT

We extend our sincere gratitude to all those who have contributed to the completion of this project report. Firstly, We would like to extend our gratitude to **Dr. V. S. K Reddy**, **Vice-Chancellor**, for his visionary leadership and unwavering commitment to academic excellence.

We would also like to express my deepest appreciation to our project guide **P. Shanmukha Kumar**, **Assistant Professor,** whose invaluable guidance, insightful feedback, and unwavering support have been instrumental throughout the course of this project for successful outcomes.

We extend our gratitude to our **PRC-convenor**, **Dr. G. Latha**, for giving valuable inputs and timely guidelines to improve the quality of our project through a critical review process.
We thank our project coordinator, **Mr. A. Ramesh Khanna**, for his timely support.

We are also grateful to **Dr. G. Anand Kumar**, **Head of the Department of CSE-Cybersecurity,** for providing us with the necessary resources and facilities to carry out this project.

We would like to thank **Dr. Kasa Ravindra**, **Dean, School of Engineering**, for his encouragement and support throughout my academic pursuit.

My heartfelt thanks also go to **Dr. Harikrishna Kamatham**, **Associate Dean School of Engineering** for his guidance and encouragement.

We are deeply indebted to all of them for their support, encouragement, and guidance, without which this project would not have been possible.

K.L.GEETESH	2011CS040035
K.KEDARI NEHA	2011CS040034
D.VINEETH KUMAR	2011CS040020
A.CHANDAN	2011CS040001

ABSTRACT

Currently as the widespread use of virtual monetary units (like Bitcoin, Ethereum, Ripple, Litecoin) has begun, people with bad intentions have been attracted to this area and have produced and marketed ransomware in order to obtain virtual currency easily. This ransomware infiltrates the victim's system with smartly-designed methods and encrypts the files found in the system. After the encryption process, the attacker leaves a message demanding a ransom in virtual currency to open access to the encrypted files and warns that otherwise the files will not be accessible. This type of ransomware is becoming more popular over time, so currently it is the largest information technology security threat. In the literature, there are many studies about detection and analysis of this cyber-bullying. In this study, we focused on crypto-ransomware and investigated a forensic analysis of a current attack example in detail. In this example, the attack method and behavior of the crypto-ransomware were analyzed and it was identified that information belonging to the attacker was accessible. With this dimension, we think our study will significantly contribute to the struggle against this threat.

TABLE OF CONTENTS

CHAPTERS			PAGE NUMBERS
CHAPTER 1			
Introduction			1 - 3
1.1	Problem Definition and Description		2
1.2	Objective of The Project		3
1.3	Scope of The Project		3
CHAPTER 2			
System Analysis			4 - 14
2.1	Existing System		4
2.1.1		Literature Survey	5
2.1.2		Limitations of Existing System	8
2.2	Proposed System		9
2.3	System Requirements		10
2.3.1		Hardware Requirements	10
2.3.2		Software Requirements	10
2.4	Feasibility Study		11
2.4.1		Technical Feasibility	11
2.4.2		Operational Feasibility	12
2.4.3		Economic Feasibility	14
CHAPTER 3			
Architectural Design			15 - 26
3.1	Modules Design		15
3.2	Project Architecture		18
3.2.1		Architecture Diagram	18

3.2.2	Data Flow Diagram	19
3.2.3	Class Diagram	20
3.2.4	Use Case Diagram (Admin)	21
3.2.5	Use Case Diagram(User)	22
3.2.6	Sequence Diagram(Admin)	23
3.2.7	Sequence Diagram(User)	24
3.2.8	Activity Diagram(Admin)	25
3.2.9	Activity Diagram(User)	26

CHAPTER 4

Implementation and Testing 27-48

4.1	Sample Code	27
4.2	Execution Flow	48

CHAPTER 5

Results 49-65

5.1	Resulting Screens	49
5.2	Resulting Tables	56
5.3	Resulting Graphs	64

CHAPTER 6

Conclusions and Future Scope of Study 66-67

6.1	Conclusions	66
6.2	Future Scope	66

BIBLIOGRAPHY 68

REFERENCES 69 - 70

PAPER PUBLICATION 71 – 78

WEB LINK OF THE PROJECT 79

List of figures:

Figure 1.1.1	Year on year growth of crypto ransomware attacks	2
Figure 2.1.1	Relation between crypto ransomware attacks and price of bitcoin	5
Figure 3.2.1	Architecture diagram of the project	18
Figure 3.2.2	Data flow Diagaram	19
Figure 3.2.3	Class Diagram	20
Figure 3.2.4	Admin Use Case Diagram	21
Figure 3.2.5	User Use Case Diagram	22
Figure 3.2.6	Admin Sequence Diagram	23
Figure 3.2.7	User Sequence Diagram	24
Figure 3.2.8	Admin Activity Diagram	25
Figure 3.2.9	User Activity Diagram	26
Figure 4.2.1	Execution Flow	48
Figure 5.3.1	Ransomware Detection Evaluation Process	64
Figure 5.3.2	Scalability Performance	64
Figure 5.3.3	Statistics of ransomware encryption process	65
Figure 5.3.4	Precision recall curve using the algorithms	65

List of Screenshots:

Figure 5.1.1	Website Home page	49
Figure 5.1.2	User Login Page	49
Figure 5.1.3	User Dashboard	50
Figure 5.1.4	User Data Upload page	50
Figure 5.1.5	Results page	51
Figure 5.1.6	Admin Login page	51
Figure 5.1.7	Admin Dashboard	52
Figure 5.1.8	Static Analysis	52
Figure 5.1.9	Dynamic analysis	53
Figure 5.1.10	File found Ransomware	53
Figure 5.1.11	Safe files data	54

Figure 5.1.12 Malicious files data 54
Figure 5.1.13 Analysis report 55

List of Tables:

Table 5.2.1 Attacker file details 56
Table 5.2.2 Index values of attacker file details 56
Table 5.2.3 Contains information about user groups for authentication purposes. 56
Table 5.2.4 Index values of auth group 57
Table 5.2.5 Manages permissions for user groups. 57
Table 5.2.6 Index values of user groups 57
Table 5.2.7 Stores permissions granted to users or groups. 57
Table 5.2.8 Index values of permission groups 58
Table 5.2.9 Contains information about registered users. 58
Table 5.2.10 Index values of registered users 58
Table 5.2.11 Maps users to their respective groups. 59
Table 5.2.12 Index values of groups respectively 59
Table 5.2.13 Manages individual user permissions. 59
Table 5.2.14 Index values of user permissions 60
Table 5.2.15 Stores details about uploaded files and their statuses. 60
Table 5.2.16 Index values of uploaded flies 60
Table 5.2.17 Logs administrative actions performed in Django admin interface. 61
Table 5.2.18 Holds index data for user IDs in admin logs. 61
Table 5.2.19 Stores content types used in the Django application. 61
Table 5.2.20 Stores session data for user sessions in Django. 62
Table 5.2.21 Tracks migrations applied to the Django application. 62
Table 5.2.22 Index values of Django application 62
Table 5.2.23 Stores session data for user sessions in Django. 62
Table 5.2.24 Index values of user sessions 63
Table 5.2.25 Contains comprehensive details about users 63
Table 5.2.26 Index values of detailed details of user 63

CHAPTER – 1

INTRODUCTION

The digital age has heralded unparalleled advancements in technology, reshaping the landscape of global finance through the advent of virtual currencies like Bitcoin, Ethereum, Ripple, and Litecoin. While these digital currencies promise a new frontier of financial freedom and privacy, they have also given rise to a new form of cyber threat: crypto ransomware. This malicious software, which exploits encryption to hold vital data hostage, has become a formidable challenge in the realm of cybersecurity. Unlike traditional malware, crypto-ransomware attackers demand ransoms in virtual currencies to release encrypted data, leveraging the anonymity provided by these digital assets to elude capture.

The proliferation of crypto ransomware represents not just a technological challenge but a stark reminder of the persistent evolution of cyber threats in the digital era. These attacks not only signify a significant threat to individual and organizational data integrity but also underscore the urgent need for robust cybersecurity measures and forensic analysis capabilities. As these ransomware attacks become increasingly sophisticated, the cybersecurity community faces the daunting task of developing detection, prevention, and analysis strategies that can adapt as quickly as the threats themselves.

This study aims to dissect the phenomenon of crypto ransomware through a detailed forensic analysis of a contemporary attack. By scrutinizing the modus operandi and behavioural patterns of a specific crypto-ransomware incident, this research endeavours to uncover identifiable markers and vulnerabilities within the attack framework. Such insights are critical in crafting more effective defence against crypto ransomware, thereby contributing to the broader struggle against cyber extortion. Through this investigation, the project seeks not only to enhance our understanding of crypto ransomware but also to propose actionable strategies for its mitigation, reflecting a significant step forward in the ongoing battle for cybersecurity.

1.1 PROBLEM DEFINITION AND DESCRIPTION:

As cyber attackers evolve their tactics, ransomware continues to pose a significant challenge to cybersecurity. Victims are often faced with the dilemma of whether to pay the ransom or risk losing access to critical files. This study aims to contribute to the fight against ransomware by conducting a forensic analysis of a recent attack example, shedding light on the attacker's methods and behavior. By understanding the intricacies of crypto-ransomware attacks, organizations and individuals can better prepare and implement proactive measures to mitigate the risk of such threats.

Ransomware has emerged as a significant cybersecurity threat, encrypting victims' files and demanding ransom for decryption. With the rise of virtual currencies, attackers have found new avenues for exploiting individuals and organizations, making it one of the most prevalent cyber threats today. This malicious software infiltrates systems through various means and encrypts files, rendering them inaccessible to the victim until a ransom is paid in virtual currency. The widespread use of virtual currencies complicates efforts to trace transactions, posing challenges in retrieving encrypted files even after payment.

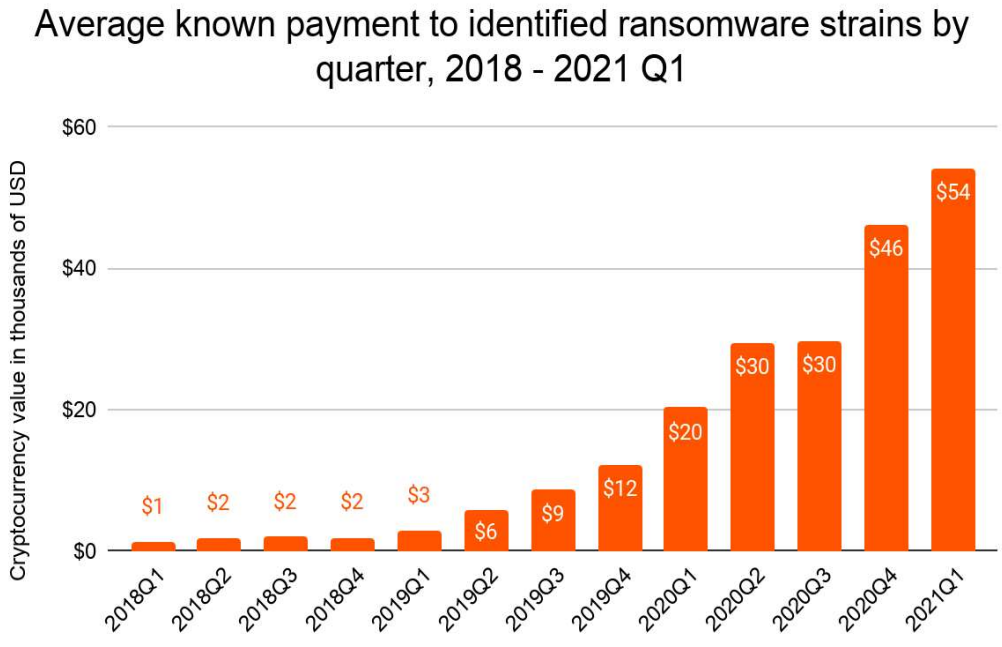


Fig 1.1 Year on year growth of crypto ransomware attacks

1.2 OBJECTIVE OF THE PROJECT:

The overarching objective of this thesis project is to establish a robust framework aimed at effectively identifying, analyzing, and mitigating crypto-ransomware attacks. Through the meticulous application of forensic analysis techniques, the project endeavors to elevate existing cybersecurity measures by providing a comprehensive approach tailored specifically to combat ransomware threats.

This research aims to delve deeply into the intricacies of ransomware incidents, meticulously dissecting their methodologies, propagation techniques, and encryption mechanisms. By doing so, it seeks to unearth critical insights into the modus operandi of ransomware actors, thus empowering cybersecurity professionals with the knowledge necessary to proactively defend against such attacks.

Ultimately, this thesis endeavors to serve as a cornerstone in the ongoing battle against crypto-ransomware, providing a comprehensive framework that amalgamates cutting-edge forensic analysis techniques with robust mitigation strategies. By bridging the gap between theory and practical application, this research aims to bolster the resilience of organizations against the ever-evolving threat landscape of ransomware attacks.

1.3 SCOPE OF THE PROJECT:

The scope of this project encompasses a multifaceted endeavor aimed at bolstering cybersecurity resilience through an exhaustive examination of crypto-ransomware attacks. The primary objective is to develop and deploy advanced techniques tailored for the timely detection and in-depth analysis of ransomware incidents, thereby augmenting existing security measures. This initiative includes the refinement and implementation of robust security protocols designed to mitigate the impact of ransomware attacks and prevent future occurrences. technologies to uncover crucial insights into the modus operandi of ransomware perpetrators. Furthermore, a key aspect of the project involves the dissemination of knowledge and best practices within the cybersecurity community, fostering collaboration and collective efforts in combating ransomware threats. These overarching objectives underpin the project's methodologies and frameworks, with the ultimate goal of malicious exploitation.

CHAPTER – 2

SYSTEM ANALYSIS

2.1 EXISTING SYSTEM:

In the ongoing battle against ransomware, a multitude of strategies have been devised to identify and analyze these insidious threats. Chief among these strategies are those rooted in signature-based detection logic [11]. While historically relied upon, the effectiveness of signature-based approaches is a subject of debate due to their inherent limitations. Traditional signature-based methods falter when confronted with the emergence of new-generation ransomware, particularly the increasingly prevalent fileless variants, which evade detection through conventional means. To overcome these deficiencies, researchers have continuously innovated, exploring novel avenues such as dynamic analysis techniques that delve into the behavioral patterns of ransomware.

One notable advancement in ransomware detection comes from the work of Fatemah et al., who introduced a pioneering method based on graphic mining within a signature-based framework. Their study reported an impressive 96.6% success rate in accurately identifying ransomware instances [12]. Expanding upon this foundation, Daniele et al. devised a dynamic analysis approach harnessing the power of machine learning algorithms to bolster ransomware defense mechanisms [13]. Furthermore, in a groundbreaking initiative back in 2015, Donghyun et al. proposed a digitalized model aimed at preemptively thwarting ransomware attacks while also facilitating prompt identification of crypto-ransomware strains [14].Moreover, the occurrence of false positives and negatives further exacerbates the limitations of signature-based detection systems. False positives occur when benign files or processes are erroneously flagged as ransomware due to similarities in signatures, leading to unnecessary alerts and disruptions within the system. to evade signature detection, slipping past the detection mechanisms undetected. These instances of false positives and negatives not only impede the efficacy of ransomware detection but also erode trust in the reliability of the detection system, Addressing these challenges requires a multifaceted approach that incorporates advanced algorithms, machine learning techniques, and behavioral analysis to enhance the accuracy and effectiveness of ransomware detection while minimizing false positives and negatives.

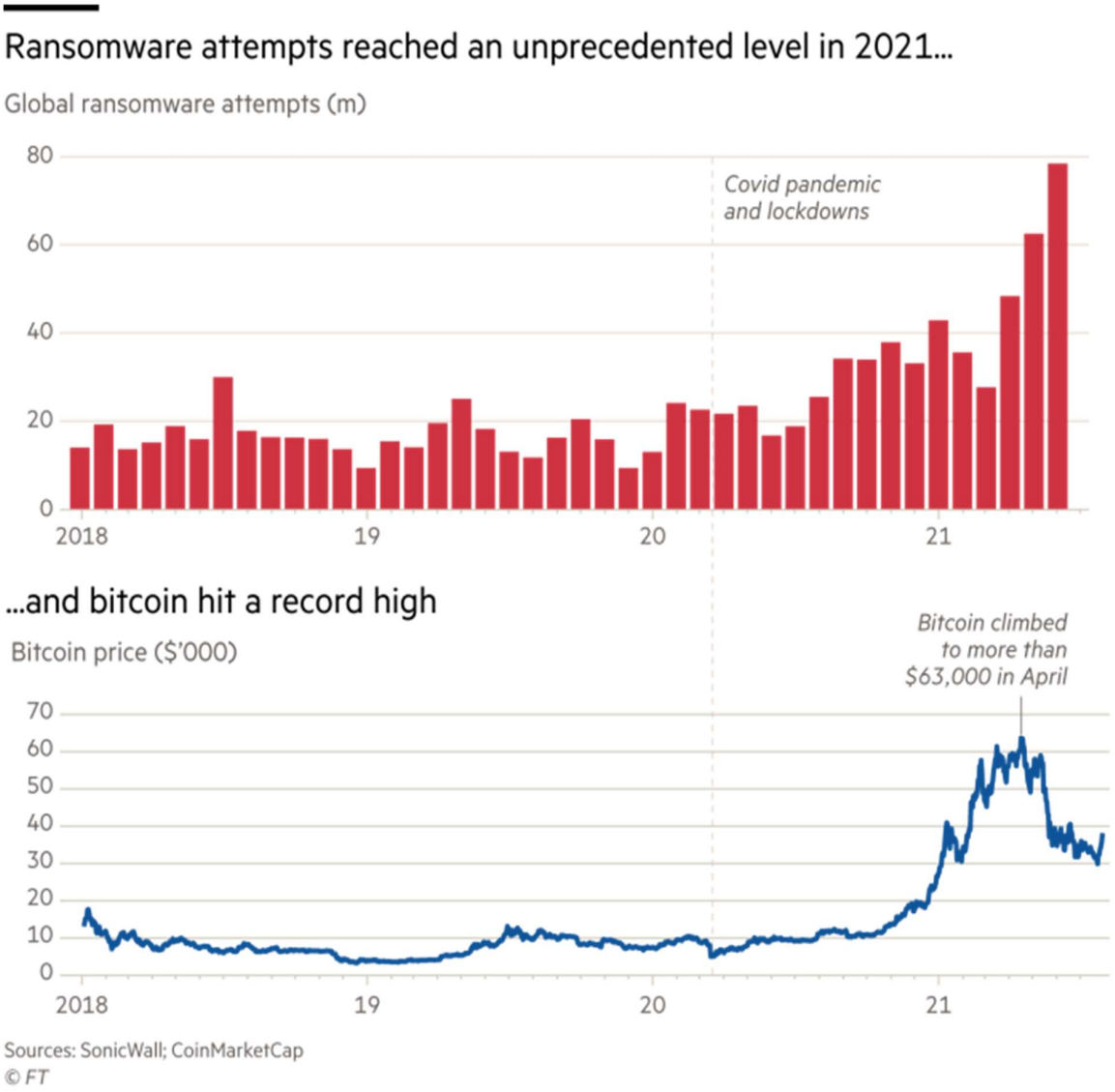


Fig 2.1 Relation between crypto ransomware attacks and price of bitcoin

2.1.1 LITERATURE SURVEY:

The challenge of distinguishing between novel threats and known malware variants is ever-present for antivirus vendors, who grapple with thousands of new malicious samples daily. Despite the reliance on manually created signatures for identifying confirmed threats, the importance of segregating truly novel malware from its known counterparts cannot be overstated. This survey delves into the realm of dynamic analysis techniques and the analysis tools that leverage these methods. Aimed at aiding analysts in timely and accurately identifying samples warranting further manual examination, this work sheds light on the mechanisms for assessing potentially malicious behavior [1].

The surge in smartphone utilization, propelled by the accessibility of cost-effective, cutting-edge technology, has concurrently heightened the vulnerability to personal data breaches. This article presents a sophisticated dual-phase attack detection framework specifically designed for the Android operating system, meticulously crafted to proactively pinpoint and thwart malware intrusions. Leveraging an attack tree methodology, the framework classifies prospective threats into three distinct categories: interception, modification, and system damage, facilitating the interpretation of malicious intent. By conducting a comprehensive comparative assessment of both pre-attack and real-time data, the system strives to proficiently fortify user information, thereby enhancing overall cybersecurity resilience [2].

Recognizing the intricate interplay between technological advancements and human behavior in shaping the effectiveness of malware defense mechanisms, this research embarks on a groundbreaking journey to dissect the real-world dynamics among users, antivirus software, and malware. Drawing parallels with the methodologies employed in clinical trials, the study meticulously assesses antivirus efficacy while shedding light on human-related risk factors. Over the span of four months, with the active participation of 50 individuals, the research scrutinizes the evolving landscape of cybersecurity. The unveiled findings not only offer valuable insights into the performance of antivirus software but also pave the way for more robust field studies aimed at comprehensively evaluating and refining cybersecurity solutions [3].

The looming threat posed by ransomware, epitomized by the relentless Cerber variant, highlights the urgency for a thorough exploration of its intricate technical and operational intricacies. In response, this study delves into the depths of an actual Cerber ransomware assault, employing a meticulous blend of static and dynamic analytical approaches. Through this comprehensive examination, the research illuminates the pathways for potentially tracing the origins of the attack, thereby underscoring the pivotal significance of technical analysis in both understanding and effectively mitigating ransomware threats [4].

Responding to the urgent demand for privacy in data outsourcing, this paper explores advancements in searchable symmetric encryption (SSE), proposing enhanced security definitions and showcasing two efficient constructions. Extending SSE to accommodate queries from multiple users, this work lays the groundwork for more secure and practical data searchability solutions [5].

Moreover, this study delves into the feasibility of executing keyword searches on publicly encrypted data without necessitating full decryption. It introduces a pioneering mechanism designed to safeguard privacy while empowering specific keyword searches. This innovative approach finds practical utility in various applications, including email routing and server-side message filtering. By leveraging this mechanism, the searchability of encrypted data is significantly enhanced, all the while maintaining stringent confidentiality standards [6].

In the realm of cloud storage, where searchable encryption endeavors to harmonize privacy with functionality, this paper undertakes a critical examination of the implications arising from information leakage inherent in efficient yet potentially vulnerable schemes. The research shines a spotlight on the tangible consequences of such compromises, shedding light on the pressing need for a nuanced comprehension of privacy dynamics within the context of searchable encryption. Through its scrutiny, the paper aims to contribute to a more robust understanding of privacy preservation strategies in the digital age [7].

Exploring the consistency and application scope of public-key encryption with keyword search (PEKS), this paper introduces refined consistency metrics and a novel, statistically consistent scheme. Additionally, it explores extensions such as anonymous hierarchical identity-based encryption (HIBE) and multi-user search capabilities, broadening the horizons of searchable encryption [8].

Furthermore, this paper presents an order-preserving encryption scheme tailored for numeric data, facilitating direct comparison operations on encrypted values while preserving query soundness and completeness. Engineered for seamless integration with existing database systems, this scheme tackles the challenges of data querying and updates within encrypted databases [9].

Initiating an in-depth exploration of order-preserving symmetric encryption (OPE), this study challenges conventional security paradigms and introduces a new model emphasizing pseudo-randomness within the order-preserving framework. By elucidating a connection between OPE and the hypergeometric distribution, the paper unveils an efficient encryption scheme promising enhanced security and practicality [12].

2.1.2 LIMITATIONS OF EXISTING SYSTEM:

Ineffectiveness against New-Generation Ransomware:

One of the primary shortcomings of existing ransomware detection systems, particularly those reliant on signature-based logic, is their ineffectiveness against new-generation ransomware strains. Signature-based approaches hinge on the identification of specific patterns or signatures associated with known ransomware variants. However, the emergence of fileless ransomware presents a significant challenge, as these variants operate without leaving traditional signatures or identifiable patterns. Consequently, signature-based detection mechanisms often fall short in effectively identifying and mitigating the threat posed by these evasive ransomware strains.

Limited Coverage:

Another critical limitation of signature-based detection methods is their constrained coverage. These systems can only detect ransomware for which signatures have been previously identified and incorporated into their databases. As a result, they may fail to detect newly developed ransomware variants until their signatures are identified and added to detection databases. This delay in updating signatures leaves systems vulnerable to emerging threats during the interim period, potentially exposing organizations to significant security risks.

False Positives and Negatives:

Moreover, signature-based detection systems are susceptible to generating false positives and negatives, further undermining their reliability. False positives occur when benign files or processes are erroneously identified as ransomware due to similarities in signatures, leading to unnecessary alerts and disruptions. Conversely, false negatives occur when ransomware undergoes modifications or obfuscation to evade signature detection, slipping past the detection mechanisms undetected. These instances of false positives and negatives not only impede the efficacy of ransomware detection but also erode trust in the reliability of the detection system, potentially leading to complacency or distrust among users and administrators.

2.2 PROPOSED SYSTEM:

In this section, we explain our proposed architectural system. In the study, the proposed approach model was designed in order to implement identification and analysis of crypto ransomware specifically. Our approach comprises three modules. These are;

- **Module 1 : Secure Imaging and Preservation**

An image (forensic copy) is taken of the computer attacked by the crypto-ransomware. An image is the name given to a one-to-one copy of the data storage unit of the material to be investigated. All analyses are performed on this image in a safe environment (on a workstation). Thus, the aim is to prevent possible harm to the live system.

- **Module 2 : Ransomware Identification and Analysis**

After creating the analysis environment, investigations of the image begin. In this step, analyses are completed from simple towards complicated methods. The first step is identification of possible ransomware. If there is no threat identified on the computer, the process ends at this step. If ransomware is identified, the first stage is to collect information about the ransomware without executing it. Later the ransomware is executed and characteristic behavior (file-array movements, code architecture) analysis is performed. In the final step, the possibility of contacting the ransomware attacker is investigated in an attempt to obtain contact information.

- **Module 3 : Advanced Feature Extraction and Machine Learning**

Central to the system's approach is the identification of ransomware characteristics through rigorous feature extraction and selection. Features crucial for accurate analysis, including file-array movements and code architecture, are meticulously extracted and prioritized. This process optimizes analysis methods, enhancing detection accuracy and efficiency. Furthermore, the system employs advanced machine learning algorithms to continuously refine feature extraction techniques based on evolving ransomware behaviors and attack patterns.

2.3 SYSTEM REQUIREMENTS

2.3.1 HARDWARE REQUIREMENTS:

- PROCESSOR : Intel i3
- RAM : 2 GB
- ROM : 20 GB

2.3.2 SOFTWARE REQUIREMENTS:

- Operating System : Windows 10/11
- Development Software : Python 3.10
- Programming Language : Python
- Integrated Development Environment : Virtual Studio Code
- Front End Technologies : HTML5,CSS3,Java Script
- Back End Technology : Django
- Database Language : SQL

2.4 FEASIBILITY STUDY:

A feasibility study assesses the operational, technical and economic merits of the proposed project. The feasibility study is intended to be a preliminary review of the facts to see if it is worthy of proceeding to the analysis phase. From the systems analyst perspective, the feasibility analysis is the primary The feasibility study is a management-oriented activity. The objective of a feasibility study is to find out if an information system project can be done and to suggest possible alternative solutions.

Projects are initiated for two broad reasons:
1. Problems that lend themselves to systems solutions
2. Opportunities for improving through:
(a) upgrading systems
(b) altering systems
(c) installing new systems

A feasibility study should provide management with enough information to decide:

- Whether the project can be done
- Whether the final product will benefit its intended users and organization
- What are the alternatives among which a solution will be chosen
- Is there a preferred alternative?

2.4.1 TECHNICAL FEASIBILITY:

A large part of determining resources has to do with assessing technical feasibility. It considers the technical requirements of the proposed project. The technical requirements are then compared to the technical capability of the organization. The systems project is considered technically feasible if the internal technical capability is sufficient to support the project requirements.

The analyst must find out whether current technical resources can be upgraded or added to in a manner that fulfils the request under consideration. This is where the expertise of system analysts is beneficial, since using their own experience and their contact with vendors they will be able to answer the question of technical feasibility.

The essential questions that help in testing the operational feasibility of a system include the following:

- Is the project feasible within the limits of current technology?
- Does the technology exist at all?
- Is it available within given resource constraints?
- Is it a practical proposition?
- Manpower- programmers, testers & debuggers
- Software and hardware
- Are the current technical resources sufficient for the new system?
- Can they be upgraded to provide the level of technology necessary for the system?
- Do we possess the necessary technical expertise, and is the schedule reasonable?
- Can the technology be easily applied to current problems?

2.4.2 OPERATIONAL FEASIBILITY:

Operational feasibility is dependent on human resources available for the project and involves projecting whether the system will be used if it is developed and implemented. Operational feasibility is a measure of how well a proposed system solves the problems, and takes advantage of the opportunities identified during scope definition and how it satisfies the requirements identified in the requirements analysis phase of system development.

Operational feasibility reviews the willingness of the organization to support the proposed system. This is probably the most difficult of the feasibilities to gauge. In order to determine this feasibility, it is important to understand the management commitment to the proposed project. If the request was initiated by management, it is likely that there is management support and the system will be accepted and used. However, it is also important that the employee base will be accepting of the change.

The essential questions that help in testing the operational feasibility of a system include the following:

- Does current mode of operation provide adequate throughput and response time?
- Does current mode provide end users and managers with timely, pertinent, accurate and useful formatted information?

- Does current mode of operation provide cost-effective information services to the business?
- Could there be a reduction in cost and or an increase in benefits?
- Does current mode of operation offer effective controls to protect against fraud and to guarantee accuracy and security of data and information?
- Does current mode of operation make maximum use of available resources, including people, time, and flow of forms?
- Does current mode of operation provide reliable services
- Are the services flexible and expandable?
- Are the current work practices and procedures adequate to support the new system?
- If the system is developed, will it be used?
- Manpower problems
- Labour objections
- Manager resistance
- Organizational conflicts and policies
- Social acceptability
- Government regulations
- Does management support the project?
- Are the users not happy with current business practices?
- Will it reduce the time (operation) considerably?
- Have the users been involved in the planning and development of the project?
- Will the proposed system really benefit the organization?
- Does the overall response increase?
- Will accessibility of information be lost?
- Will the system affect the customers in considerable way?
- Legal aspects
- How do the end-users feel about their role in the new system?
- What end-users or managers may resist or not use the system?
- Does current mode of operation provide adequate throughput and response time?
- Are the current work practices and procedures adequate to support the new system?
- Could there be a reduction in cost and or an increase in benefits?
- Does current mode provide end users and managers with timely, pertinent, accurate and useful formatted information?

2.4.3 ECONOMIC FEASIBILITY:

Economic analysis could also be referred to as cost/benefit analysis. It is the most frequently used method for evaluating the effectiveness of a new system. In economic analysis the procedure is to determine the benefits and savings that are expected from a candidate system and compare them with costs. If benefits outweigh costs, then the decision is made to design and implement the system. An entrepreneur must accurately weigh the cost versus benefits before taking an action.

Possible questions raised in economic analysis are:

- Is the system cost effective?
- Do benefits outweigh costs?
- The cost of doing full system study
- The cost of business employee time
- Estimated cost of hardware
- Estimated cost of software/software development
- Is the project possible, given the resource constraints?
- What are the savings that will result from the system?
- Cost of employees' time for study

The concerned business must be able to see the value of the investment it is pondering before committing to an entire system study. If short-term costs are not overshadowed by long-term gains or produce no immediate reduction in operating costs, then the system is not economically feasible, and the project should not proceed any further. If the expected benefits equal or exceed costs, the system can be judged to be economically feasible. Economic analysis is used for evaluating the effectiveness of the proposed system.

The economic feasibility will review the expected costs to see if they are in-line with the projected budget or if the project has an acceptable return on investment. At this point, the projected costs will only be a rough estimate. The exact costs are not required to determine economic feasibility. It is only required to determine if it is feasible that the project costs will fall within the target budget or return on investment. A rough estimate of the project schedule is required to determine if it would be feasible to complete the systems project within a required timeframe. The required timeframe would need to be set by the organization.

CHAPTER – 3

ARCHETECTURAL DESIGN

In response to the escalating threat posed by crypto-ransomware attacks, the architectural design of this thesis project aims to develop a robust and efficient system for the identification and analysis of such cyber threats. With the proliferation of virtual currencies and the increasing sophistication of malicious actors. This architectural design lays the groundwork for a comprehensive solution that integrates image acquisition, dynamic analysis, and reporting functionalities to empower organizations and individuals in their fight against ransomware.

The design of this system is guided by the recognition that traditional security measures are often inadequate in detecting and mitigating the impact of crypto-ransomware attacks. As these attacks evolve in complexity and scale, it is imperative to adopt a proactive approach that leverages advanced technologies and methodologies. By combining state-of-the-art image acquisition techniques with dynamic analysis capabilities, the proposed system aims to provide actionable insights into the behavior and characteristics of ransomware strains, enabling timely response and effective containment strategies.

3.1 MODULES DESIGN:

1. User Interface Module:

The User Interface Module serves as the primary interaction point for administrators and users with the system. It offers a seamless and intuitive interface for accessing various functionalities and features. The module encompasses the following components:

- **User Authentication:** Enables users to securely log in to the system using their credentials, ensuring authorized access to functionalities based on user roles and permissions.
- **File Upload:** Facilitates the uploading of files or forensic images acquired from computers affected by ransomware attacks. Users can securely upload files through the interface for subsequent analysis.

- **Analysis Request Submission:** Allows users to submit analysis requests for uploaded files. Users can provide specific instructions or preferences regarding the analysis process, such as prioritizing certain types of analysis or requesting expedited processing.
- **Access to Analysis Reports:** Provides users with access to analysis reports generated by the system. Users can view detailed findings, insights, and recommendations resulting from the analysis of uploaded files.
- **User Profile Management:** Enables users to manage their profiles, including updating personal information, modifying preferences, and viewing past activities and interactions within the system.

2. Image Acquisition Module:

The Image Acquisition Module is responsible for acquiring forensic images of computers or devices that have been compromised by crypto-ransomware attacks. It employs advanced techniques to ensure the comprehensive capture of relevant data while preserving the integrity of the original systems. The module includes the following functionalities:

- **Physical and Logical Image Acquisition:** Utilizes both physical and logical methods to capture forensic images of affected computers. Physical acquisition involves creating bit-by-bit copies of storage media, while logical acquisition focuses on capturing specific files or data structures.
- **Data Integrity Preservation:** Ensures the integrity of acquired images by employing cryptographic hashing techniques and verification mechanisms. This guarantees that the acquired data remains unchanged and tamper-proof throughout the acquisition process. actionable recommendations offer actionable recommendations for response and mitigation strategies based on the identified ransomware characteristics and observed behaviors. Recommendations may include preventive measures, containment strategies, and recovery procedures to minimize the impact of ransomware incidents.

- **Live System Protection:** Minimizes the risk of further damage to live systems during the acquisition process by employing non-intrusive and non-destructive techniques. This prevents potential data loss or disruption caused by aggressive acquisition methods.

3. Dynamic Analysis Module:

The Dynamic Analysis Module conducts in-depth analysis of acquired images to identify and

understand the behavior of crypto-ransomware strains. It employs a combination of reverse engineering techniques, machine learning algorithms, and sandbox environments to uncover patterns, characteristics, and potential communication channels associated with ransomware attacks. The module encompasses the following components:

- **Reverse Engineering:** Utilizes reverse engineering techniques to dissect ransomware binaries and understand their underlying code structures, execution flows, and encryption mechanisms. report generation automatically generates detailed reports documenting the analysis procedures, methodologies, and outcomes. Reports include information on ransomware characteristics, behavioral patterns, identified threats, and recommended actions.
- **Machine Learning Analysis:** Applies machine learning algorithms to analyze behavioral patterns and anomalies exhibited by ransomware strains. This enables the identification of signature behaviors and the classification of ransomware variants based on their characteristics.
- **Sandbox Environment:** Executes ransomware samples in controlled sandbox environments to observe their behavior in a safe and isolated setting. This allows for the detection of malicious activities, such as file encryption, network communication, and system modifications, without risking further harm to the analysis environment.

4. Reporting Module:

The Reporting Module generates comprehensive reports summarizing the findings, insights, and recommendations resulting from the analysis of ransomware incidents. The module includes the following functionalities:

- **Report Generation:** Automatically generates detailed reports documenting the analysis procedures, methodologies, and outcomes. Reports include information on ransomware characteristics, behavioral patterns, identified threats, and recommended actions.
- **Insightful Analysis:** Provides insightful analysis and interpretation of ransomware behaviors, enabling stakeholders to understand the nature and severity of the threats posed by specific ransomware strains.
- **Actionable Recommendations:** Offers actionable recommendations for response and mitigation strategies based on the identified ransomware characteristics and observed

3.2 PROJECT ARCHETECTURE

3.2.1 ARCHETECTURE DIAGRAM:

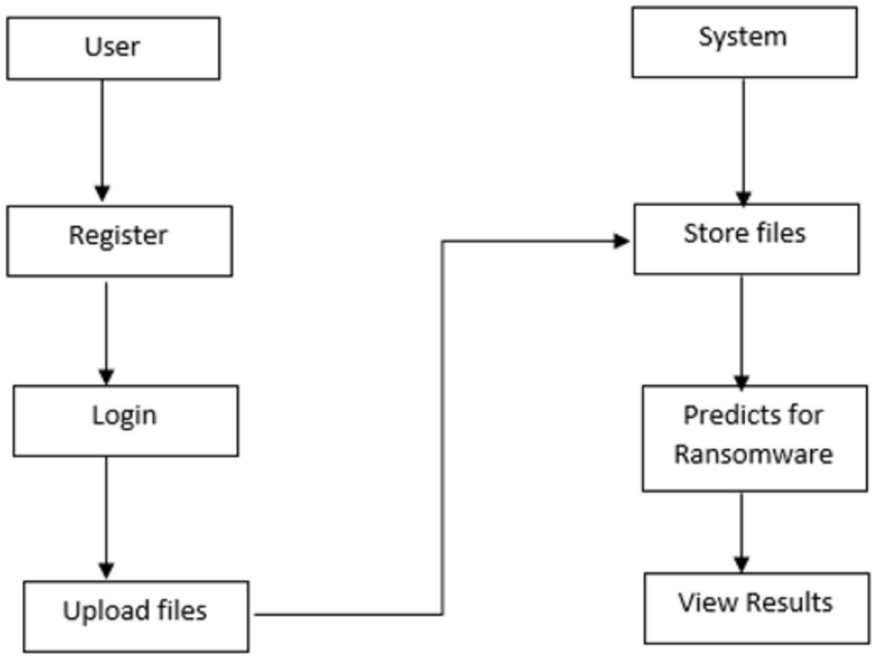


Fig: 3.2.1 Architecture diagram of the project

The above figure 3.2.1 represent the architecture of the project . The architecture diagram for ransomware detection typically includes data sources (endpoints, network traffic), data collection mechanisms, processing for anomaly detection and pattern recognition, a detection engine utilizing signatures and behavioral analysis, alerting/notification systems, response mechanisms like isolating affected systems, logging/reporting for auditing, integration points with other security tools, a user interface for monitoring, and potentially external services for threat intelligence. This diagram showcases how these components work together to detect and respond to ransomware threats effectively. The architecture diagram serves as a blueprint for understanding how data flows through the system, how ransomware threats are identified, and how responses are triggered. Integration with external services enhances the system's capabilities.

3.2.2 DATA FLOW DIAGRAM:

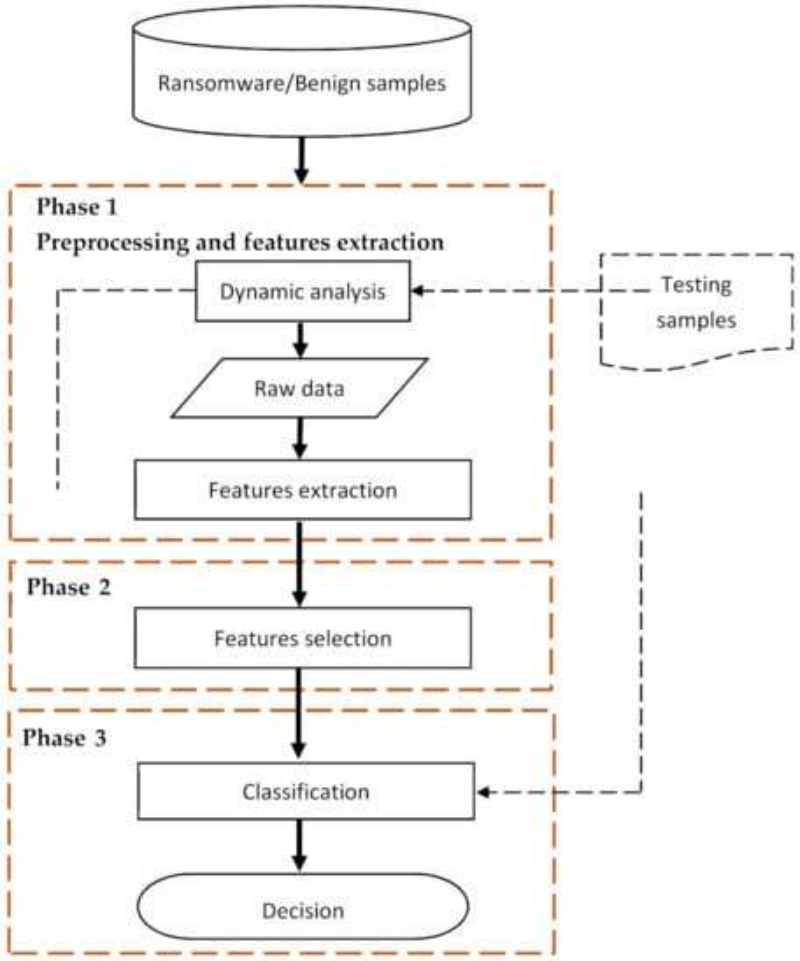


Fig 3.2.2: Data flow Diagaram

In a data flow diagram for your project, we illustrate the movement of data through various processes and systems. It typically consists of entities, processes, data stores, and data flows. Entities represent external entities interacting with the system, processes depict the activities performed on the data, data stores signify where data is stored, and data flows depict the movement of data between these components. This diagram provides a visual representation of how data is input, processed, and output within your project, facilitating understanding and analysis of its data flow architecture. It aids in understanding the interactions between different components, guiding system design, development, and optimization efforts.

3.2.3 CLASS DIAGRAM:

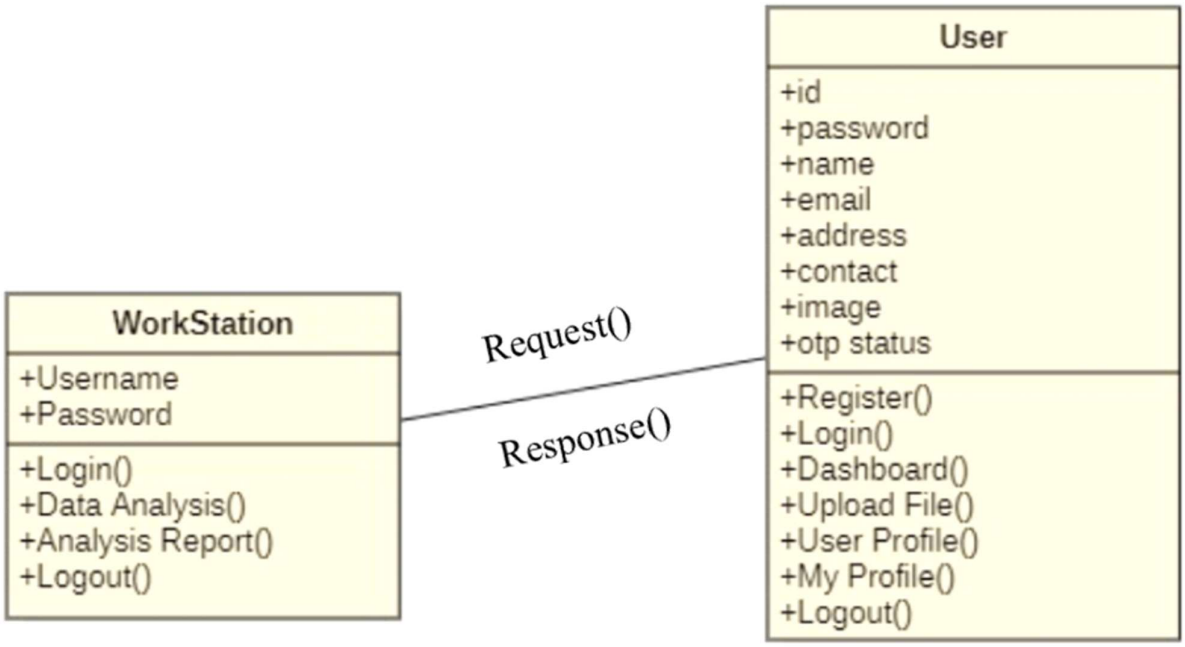


Fig 3.2.3 Class Diagram

A class diagram for your project illustrates the structure of your software system by depicting classes, their attributes, methods, and relationships. Classes represent the key entities or objects in your system, while attributes describe their properties, and methods define their behaviours. Relationships between classes, such as associations, inheritances, aiding in the planning and organization of code development. It helps developers understand the and dependencies, are also depicted. This diagram provides a clear overview of the system's object-oriented design, facilitating communication among developers and guiding the implementation process. The class diagram serves as a blueprint for the software's architecture, aiding in the planning and organization of code development. It helps developers understand the system's design principles, promoting modularity, encapsulation, and reusability. By visually representing the relationships between classes and their interactions, the diagram guides the implementation of features, ensuring cohesion and maintainability throughout the development lifecycle. Additionally, it can serve as documentation for future reference and as a basis for testing and troubleshooting.

3.2.4 USE CASE DIAGRAM (ADMIN) :

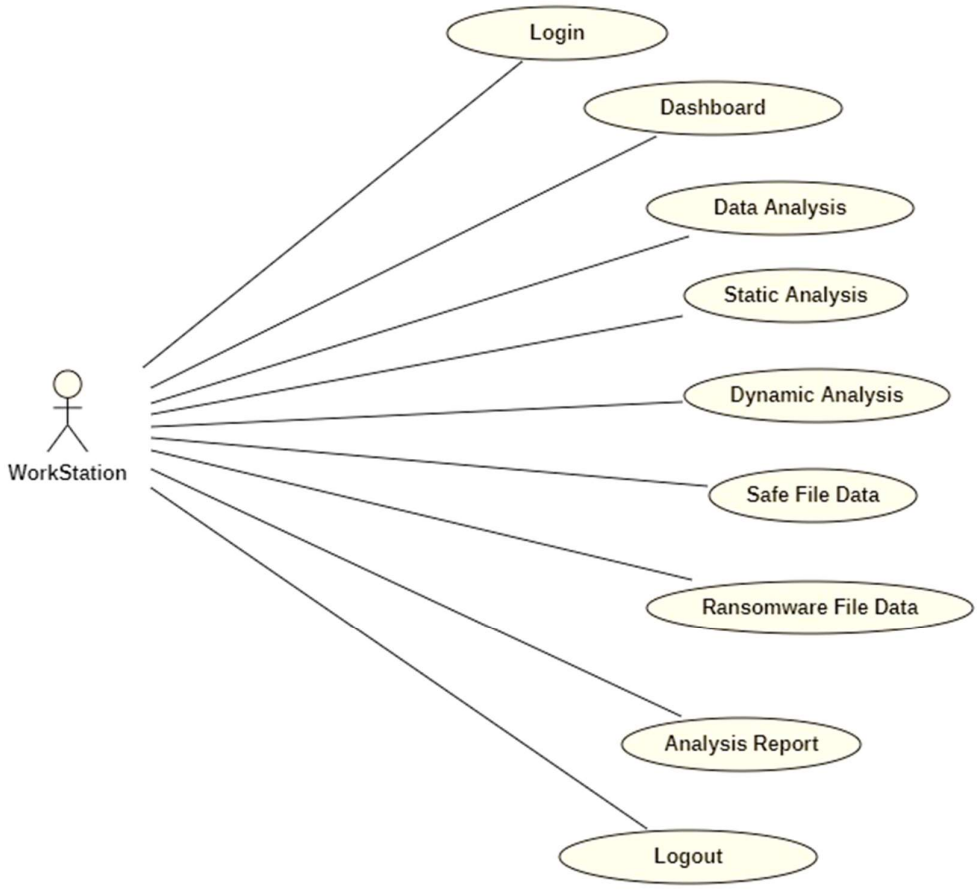


Fig 3.2.4 Admin Use Case Diagram

A Use Case Diagram (Admin) for your project depicts the various interactions and functionalities available to the admin user. It typically includes actors such as the admin and the system, along with use cases representing actions the admin can perform, such as user management, content moderation, system configuration, and reporting. Relationships between the admin and these use cases illustrate the admin's roles and responsibilities within the system. This diagram provides a high and system testing. The Use Case Diagram (Admin) serves as a visual representation of the system's behavior from the admin's perspective, facilitating communication between stakeholders and developers. It helps ensure that all necessary functionalities are identified and understood, guiding the development process to meet the requirements.

3.2.5 USE CASE DIAGRAM(USER) :

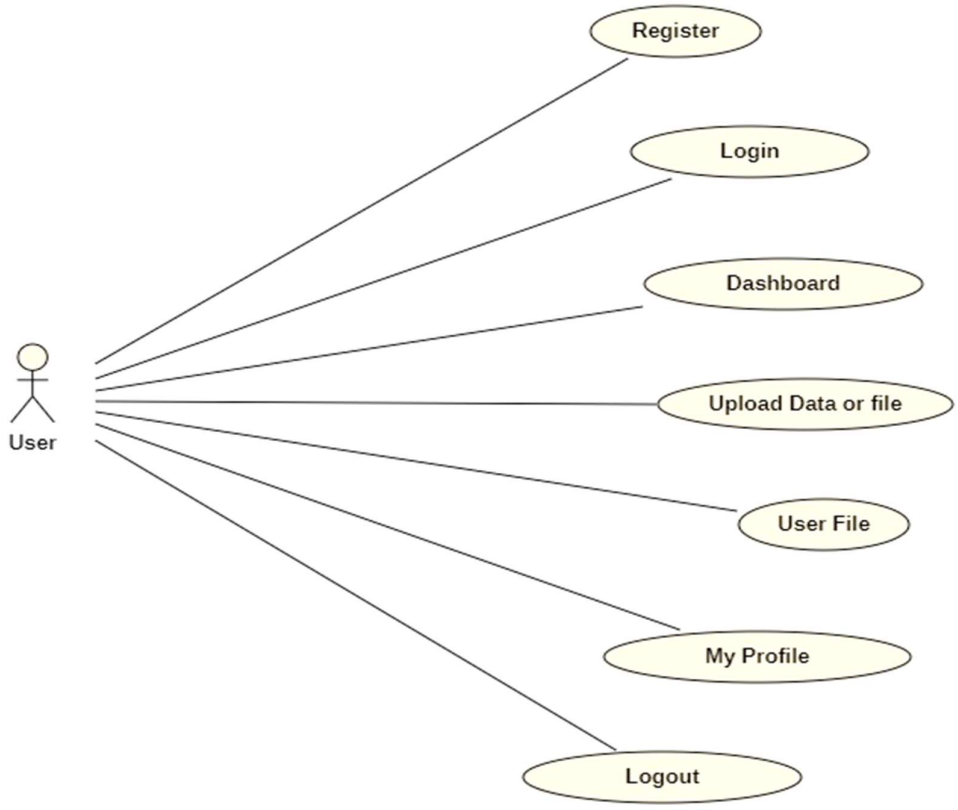


Fig 3.2.5 User Use Case Diagram

A Use Case Diagram (User) for your project illustrates the interactions and functionalities available to the users of the system. It typically includes actors such as the user and the system, along with use cases representing actions the user can perform, such as leaving reviews. This diagram provides a clear overview of the user's journey and available functionalities, aiding in requirements analysis, user interface design, and system testing. The Use Case Diagram (User) serves as a valuable tool for understanding the system's functionality from the user's perspective. It helps ensure that the system aligns with user needs and expectations, guiding the development process to create a user-friendly and intuitive interface. Additionally, by outlining user interactions and scenarios, the diagram assists in identifying usability issues and refining user workflows, contributing to the overall user experience and satisfaction with the system.

3.2.6 SEQUENCE DIAGRAM(ADMIN) :

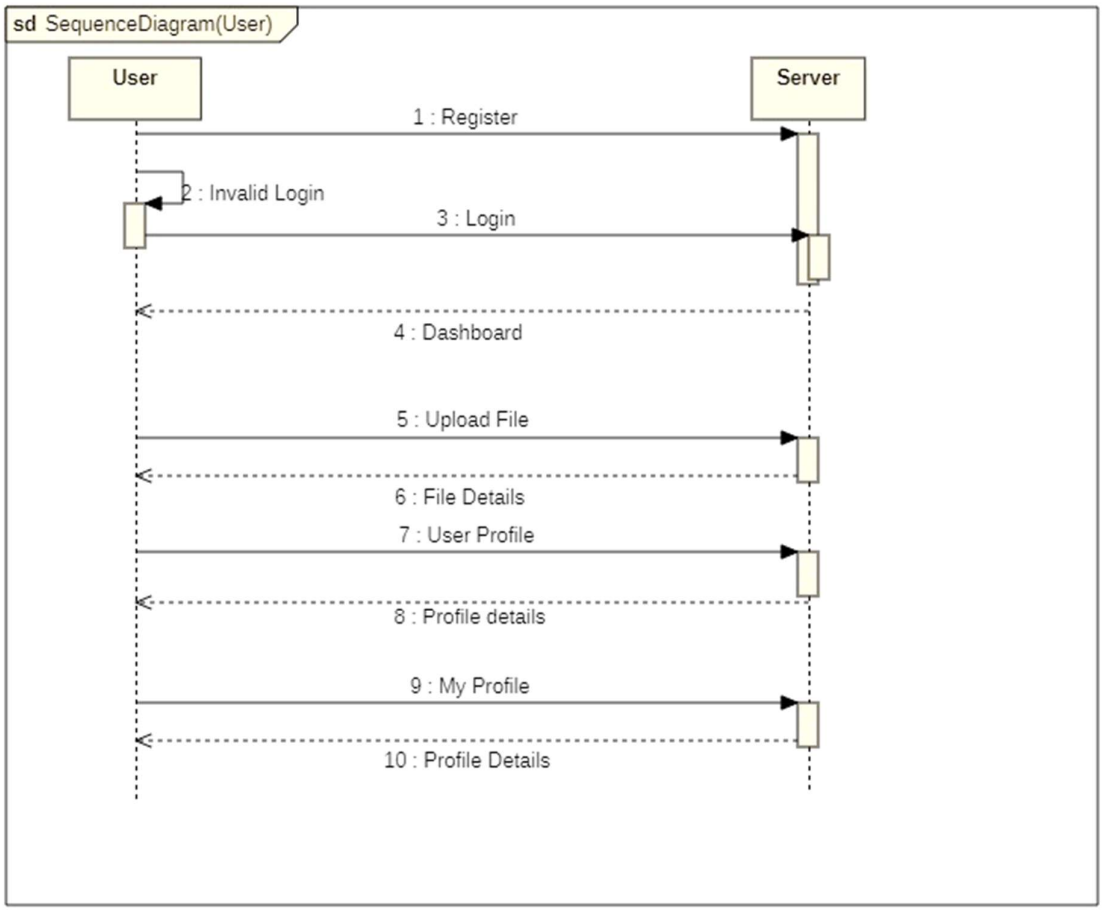


Fig 3.2.6 Admin Sequence Diagram

A Sequence Diagram (Admin) for your project illustrates the chronological sequence of interactions between the admin user and the system components. It typically depicts the flow of messages exchanged between objects over time, showing how the admin initiates actions and how the system responds. The diagram may include scenarios such as user management, content moderation, or system configuration, detailing the specific steps and the order in which they occur. This diagram provides a dynamic view of the admin's interactions with the system, helping to understand the runtime behavior and communication patterns, aiding in system design, implementation, and debugging. The Sequence Diagram (Admin) offers a detailed view of the admin's interactions with the system, including the sequence of method calls, parameter passing, and system responses. It helps in identifying potential bottlenecks, concurrency issues, and dependencies within the system.

3.2.7 SEQUENCE DIAGRAM(USER) :

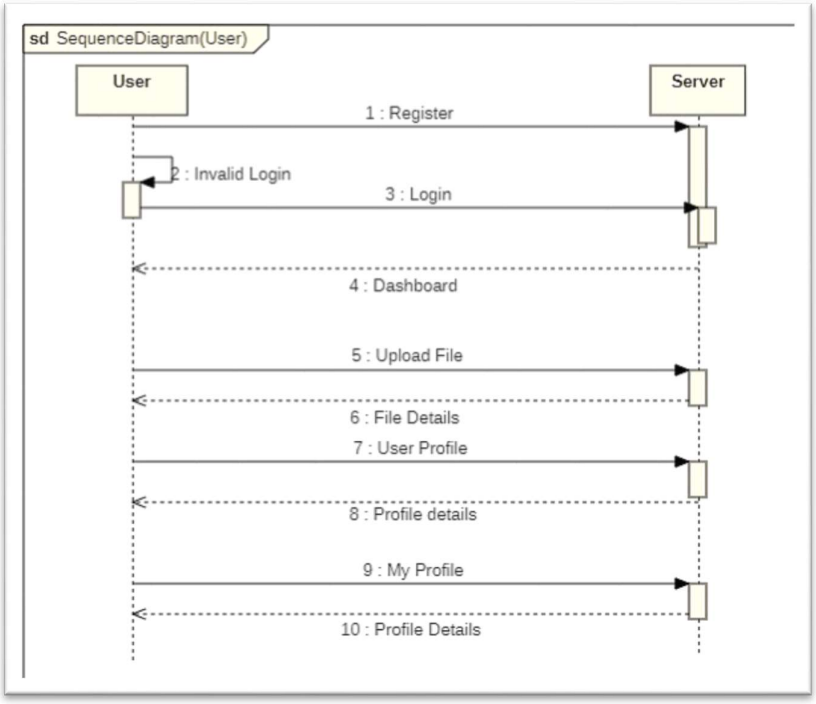


Fig 3.2.7 User Sequence Diagram

A Sequence Diagram (User) for your project illustrates the sequential interactions between a user and the system components. It typically shows the flow of messages exchanged between the user and the system objects over time, depicting actions such as user authentication, browsing content, making purchases, and accessing account settings. The diagram provides a dynamic view of the user's interactions with the system, detailing the order of activities and the communication between objects. This visualization aids in understanding the runtime behavior of the system, guiding the development process, and ensuring that user interactions are handled effectively. Additionally, it facilitates communication between developers and stakeholders, fostering collaboration and alignment on system functionality and requirements. By visualizing these interactions, developers can better understand user workflows and refine system design to enhance user experience. Moreover, stakeholders gain a clearer understanding of system functionality and behavior, fostering effective communication and decision-making throughout the development process. This ensures that the final system meets user needs and expectations while maintaining efficiency and reliability.

3.2.8 ACTIVITY DIAGRAM(ADMIN) :

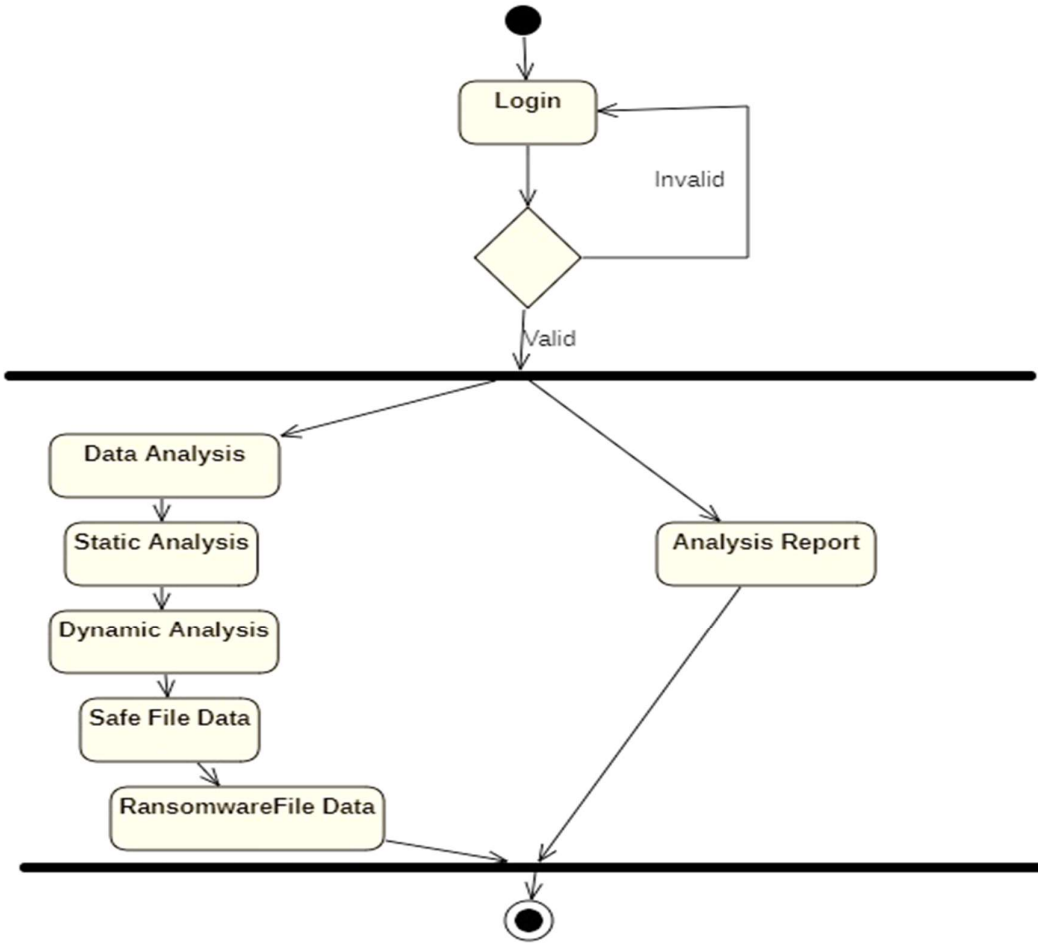


Fig 3.2.8 Admin Activity Diagram

An Activity Diagram (Admin) for your project illustrates the workflow and activities performed by the admin user within the system. It typically outlines the sequence of actions and decisions involved in admin-specific tasks such as user management, content moderation, or system configuration. The diagram uses nodes to represent activities and arrows to depict the flow of control between them, detailing decision points, loops, and parallel activities as necessary. This visual representation aids in understanding the logical flow of admin operations, helping to identify potential bottlenecks, optimize processes, and ensure efficient system administration. Additionally, it serves as a tool for documentation and communication, facilitating collaboration between developers and stakeholders in refining admin workflows and system functionality.

3.2.9 ACTIVITY DIAGRAM(USER) :

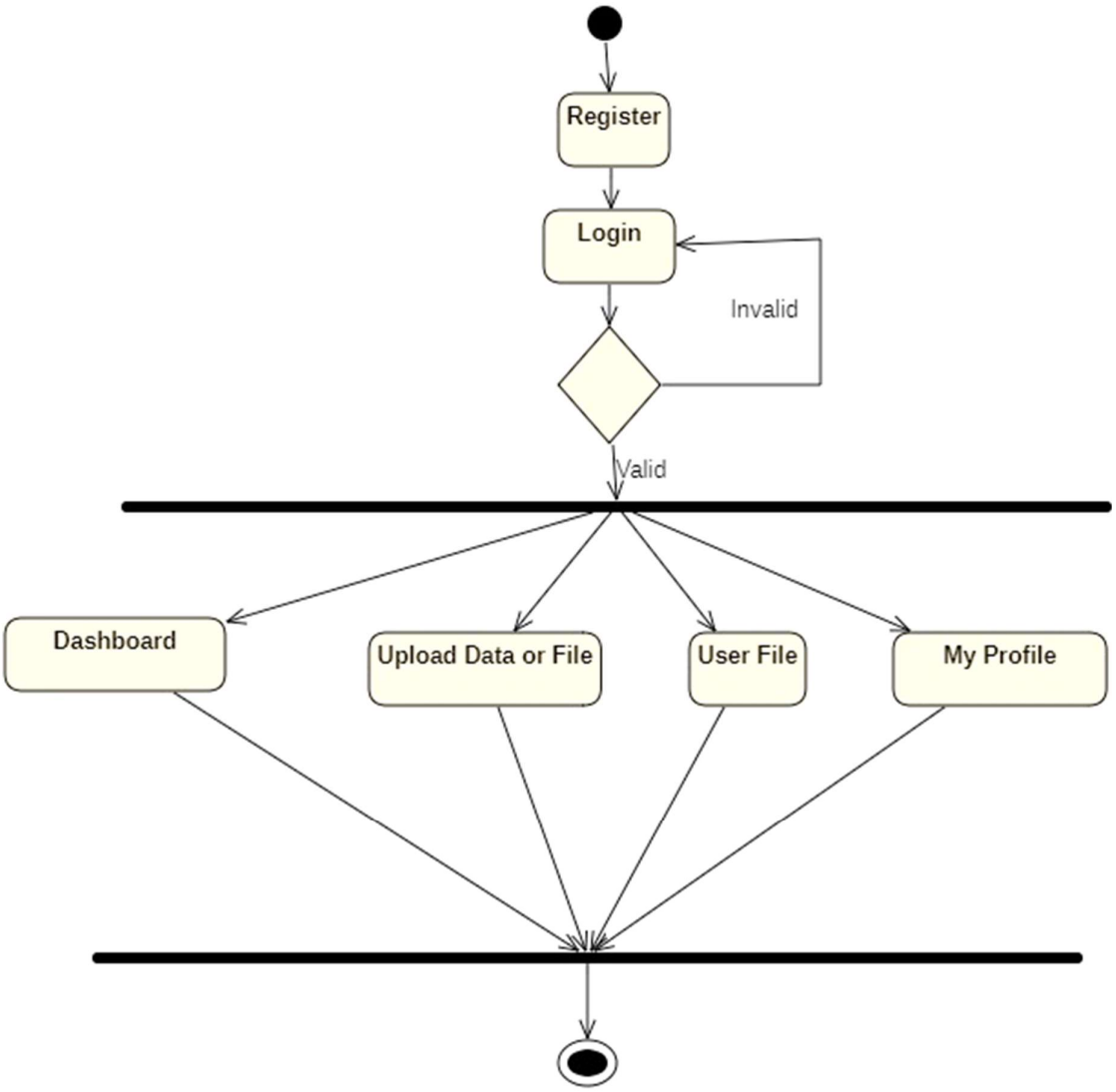


Fig 3.2.9 User Activity Diagram

An Activity Diagram (User) for your project illustrates the sequential flow of activities performed by users within the system. It typically outlines user interactions such as account registration, browsing content, making purchases, and managing settings. Using nodes to represent activities and arrows to indicate transitions between them, the diagram visualizes the user's journey through various tasks, including decision points and loops. This visualization helps to understand the logical of user, identify potential inefficiencies. Additionally, it serves as a communication for stakeholders, facilitating on user design and system functionality.

CHAPTER 4

IMPLEMENTATION AND TESTING

4.1 SAMPLE CODE:

manage.py

```
#!/usr/bin/env python
"""Django's command-line utility for administrative tasks."""
import os
import sys
def main():
    """Run administrative tasks."""
    os.environ.setdefault('DJANGO_SETTINGS_MODULE', 'cyberfraudproject.settings')
    try:
        from django.core.management import execute_from_command_line
    except ImportError as exc:
        raise ImportError(
            "Couldn't import Django. Are you sure it's installed and "
            "available on your PYTHONPATH environment variable? Did you "
            "forget to activate a virtual environment?"
        ) from exc
    execute_from_command_line(sys.argv)
if __name__ == '__main__':
    main()
```

settings.py

```
from pathlib import Path
import os
# Build paths inside the project like this: BASE_DIR / 'subdir'.
BASE_DIR = Path(__file__).resolve().parent.parent
SECRET_KEY = 'django-insecure-n(rv1w=3j79=7_a3u4ueuaj&hudzk)-m--c=!h%^tc(vd(tm&+'
DEBUG = True
```

```
ALLOWED_HOSTS = []
INSTALLED_APPS = [
    'django.contrib.admin',
    'django.contrib.auth',
    'django.contrib.contenttypes',
    'django.contrib.sessions',
    'django.contrib.messages',
    'django.contrib.staticfiles',
    'usersapp',
    'workstationapp',
    'mainapp',
    # 'django_user_agents',
]
MIDDLEWARE = [
    'django.middleware.security.SecurityMiddleware',
    'django.middleware.common.CommonMiddleware',
    'django.middleware.csrf.CsrfViewMiddleware',
    'django.contrib.auth.middleware.AuthenticationMiddleware',
    'django.contrib.messages.middleware.MessageMiddleware',
    'django.middleware.clickjacking.XFrameOptionsMiddleware',
    # 'django_user_agents.middleware.UserAgentMiddleware',
]
ROOT_URLCONF = 'cyberfraudproject.urls'
TEMPLATES = [
    {
        'BACKEND': 'django.template.backends.django.DjangoTemplates',
        'DIRS': [os.path.join(BASE_DIR,'assets/templates')],
        'APP_DIRS': True,
        'OPTIONS': {
            'context_processors': [
                'django.template.context_processors.debug',
                'django.template.context_processors.request',
                'django.contrib.auth.context_processors.auth',
                'django.contrib.messages.context_processors.messages',
```

```
            ],
        },
    },
]
WSGI_APPLICATION = 'cyberfraudproject.wsgi.application'
DATABASES = {
    'default': {
        'ENGINE': 'django.db.backends.mysql',
        'NAME': 'cyber_fraud_projects',
        'HOST':'127.0.0.1',
        'USER':'root',
        'password':'',
        'PORT':'3306',
        'OPTION':{'init_command':"SET sql-mode='STRKT-TRAINS_TABLES'"}
    }
}
AUTH_PASSWORD_VALIDATORS = [
    {
        'NAME': 'django.contrib.auth.password_validation.UserAttributeSimilarityValidator',
    },
    {
        'NAME': 'django.contrib.auth.password_validation.MinimumLengthValidator',
    },
    {
        'NAME': 'django.contrib.auth.password_validation.CommonPasswordValidator',
    },
    {
        'NAME': 'django.contrib.auth.password_validation.NumericPasswordValidator',
    },
]
LANGUAGE_CODE = 'en-us'
TIME_ZONE = 'UTC'
USE_I18N = True
```

```
USE_TZ = True
STATIC_URL = 'static/'
STATICFILES_DIRS=os.path.join(BASE_DIR,'assets/static'),
DEFAULT_AUTO_FIELD = 'django.db.models.BigAutoField'
MEDIA_URL = '/media/'
MEDIA_ROOT=os.path.join(BASE_DIR,'media')
```

Users side

views.py

```
from django.shortcuts import render,redirect
from usersapp.models import *
from django.contrib import messages
import pathlib
from django.core.files.storage import FileSystemStorage
import socket
from django.core.paginator import Paginator
def main_userregistration(request):
    if request.method=="POST" and request.FILES['image']:
     name=request.POST.get('name')
     email=request.POST.get('email')
     password=request.POST.get('password')
     dob=request.POST.get('dob')
     contact=request.POST.get('contact')
     city=request.POST.get('city')
     image=request.FILES['image']
     hostname=socket.gethostname()
     IPadress=socket.gethostbyname(hostname)
     print(IPadress,'hhhh')
     print(name,email,password,contact,image,city,dob)
      userregistration=UserModel.objects.create(user_name=name,user_dob=dob,user_email=
email,user_password=password,user_contact=contact,user_city=city,user_image=image,user
_ip=IPadress)
          userregistration.save()
     if userregistration:
```

```
            messages.success(request,'successfully login')
            return redirect('main_user_login')
        else:
            messages.error(request,'Invalid Credentials')
            return redirect('main_userregistration')
def main_user_login(request):
    if request.method == "POST":
        email=request.POST.get("email")
        password=request.POST.get("password")
        print(email,password)
        try:
            check = UserModel.objects.get(user_email=email,user_password=password)
            request.session['user_id']=check.user_id
            print(check)
            messages.success(request,'user login successfully')
            return redirect('users_dashboard')
        except:
            messages.info(request,'invalid Credentials')
            return redirect('main_user_login')
    return render(request,"main/main-user-login.html")
# Create your views here.
def users_about(request):
    return render(request,'users/user-about-us.html')
def users_contact(request):
    return render(request,'users/user-contact.html')
def users_features(request):
    return render(request,'users/user-features.html')
def users_index(request):
    return render(request,'users/user-index.html')
def users_portfolio(request):
    return render(request,'users/user-portfolio.html')
def users_services(request):
    return render(request,'users/user-services.html')
def users_testimonials(request):
```

```
    return render(request,'users/user-testimonials.html')
def users_dashboard(request):
    users=UserModel.objects.all().count()
    files=FileModel.objects.all().count()
    return render(request,'users/user-dashboard.html',{'i':users,'x':files})
def users_myfile(request):
    user_id=request.session['user_id']
    user=UserModel.objects.get(user_id=user_id)
    userfile=FileModel.objects.filter(user=user_id)
    print(userfile,'data')
    fPosts=FileModel.objects.filter(user=user_id).order_by("file_id")
    paginator = Paginator(fPosts, 4)
    page_number = request.GET.get('page')
    post = paginator.get_page(page_number)
    return render(request,'users/user-myfile.html',{'userfile':userfile,'post':post})
def users_myprofile(request):
    user_id=request.session['user_id']
    userprofile=UserModel.objects.get(user_id=user_id)
    if request.method=="POST":
        name=request.POST.get('name')
        email=request.POST.get('email')
        password=request.POST.get('password')
        dob=request.POST.get('dob')
        contact=request.POST.get('contact')
        city=request.POST.get('city')
        if len(request.FILES)!=0:
            image=request.FILES['image']
            userprofile.user_name=name
            userprofile.user_email=email
            userprofile.user_password=password
            userprofile.user_dob=dob
            userprofile.user_contact=contact
            userprofile.user_city=city
            userprofile.user_image=image
```

```
        else:
            userprofile.user_name=name
            userprofile.user_email=email
            userprofile.user_password=password
            userprofile.user_dob=dob
            userprofile.user_contact=contact
            userprofile.user_city=city
            userprofile.save()
        messages.success(request,'Updated Successfully')
        return redirect('users_myprofile')
    return render(request,'users/user-myprofile.html',{'userprofile':userprofile})
def users_uploaddata(request):
    context={}
    if request.method == "POST" and request.FILES['file']:
        name=request.POST.get("name")
        filetype=request.POST.get("filetype")
        file=request.FILES["file"]
        f_type=file.name
        a=pathlib.Path(f'{f_type}').suffix
        fs=FileSystemStorage()
        fname=fs.save('media/'+name,file)
        url=fs.url(fname)
        context['url'] =fs.url(name)
        uploaded_file_path=fs.path(fname)
        user_id=request.session['user_id']
        user1=UserModel.objects.get(user_id=user_id)
         useruploaddata=FileModel.objects.create(file_name=name,file_type=a,file_upload=file,u
ser=user1,file_path=uploaded_file_path)
  UserModel.objects.create(user_name=name,user_city=city,user_email=email,user_passwor
d=password,user_dob=dob,user_contact=contact,user_image=image)
        useruploaddata.save()
        if useruploaddata:
            messages.success(request,'successfully uploaded data')
            return redirect('users_uploaddata')
```

```
        else:
            messages.error(request,'Invalid datatype')
            return redirect('users_uploaddata')
    return render(request,'users/user-uploaddata.html',context)
def users_pricing(request):
    return render(request,'users/user-pricing.html'
```

models.py

```
from django.db import models
# Create your models here.
class UserModel(models.Model):
    user_id=models.AutoField(primary_key=True)
    user_name=models.CharField(help_text='user_name',max_length=50,null=True)
    user_email=models.EmailField(help_text='user_email',max_length=50)
    user_password=models.CharField(help_text='user_password',max_length=50,null=True)
    user_contact=models.CharField(help_text='user_contact', max_length=50,null=True)
    user_city=models.CharField(help_text='user_city', max_length=200,null=True)
    user_dob=models.DateField(help_text='user_dob',max_length=50,null=True)
    user_ip=models.CharField(help_text='user_ip',max_length=50,null=True)
    user_image=models.ImageField(upload_to='media/',null=True)
    class Meta:
        db_table='user_complete_details'
class FileModel(models.Model):
    file_id=models.AutoField(primary_key=True)
    file_name=models.CharField(help_text='file_name',max_length=50,null=True)
    file_type=models.CharField(help_text='file_type',max_length=50,null=True)
    file_date=models.DateField(help_text='file_data', auto_now_add=True,null=True)
    file_upload=models.FileField(upload_to='media/',null=True)
     file_status=models.CharField(help_text='file_status',max_length=50,default='verification in
process',null=True)
    attack_status=models.CharField(help_text='attack_status',max_length=50,null=True)
    file_path=models.CharField(help_text='file_path',max_length=500,null=True)
      user=models.ForeignKey(UserModel,on_delete=models.CASCADE,related_name='user_c
omplete_details',null=True)
    class Meta:
```

```
        db_table='data_file_details'
def users_about(request):
    return render(request,'users/user-about-us.html')
def users_contact(request):
    return render(request,'users/user-contact.html')
def users_features(request):
    return render(request,'users/user-features.html')
def users_index(request):
    return render(request,'users/user-index.html')
def users_portfolio(request):
    return render(request,'users/user-portfolio.html')
def users_services(request):
    return render(request,'users/user-services.html')
def users_testimonials(request):
    return render(request,'users/user-testimonials.html')
def users_dashboard(request):
    users=UserModel.objects.all().count()
    files=FileModel.objects.all().count()
    return render(request,'users/user-dashboard.html',{'i':users,'x':files})
def users_myfile(request):
    user_id=request.session['user_id']
    user=UserModel.objects.get(user_id=user_id)
    userfile=FileModel.objects.filter(user=user_id)
    print(userfile,'data')
    fPosts=FileModel.objects.filter(user=user_id).order_by("file_id")
    paginator = Paginator(fPosts, 4)
    page_number = request.GET.get('page')
    post = paginator.get_page(page_number)
    return render(request,'users/user-myfile.html',{'userfile':userfile,'post':post})
```

admin side

views.py

```
from django.shortcuts import render,redirect
from usersapp.models import *
```

```
from mainapp.models import *
from django.contrib import messages
import socket
import pathlib
from django.core.files.storage import FileSystemStorage
from django.core.paginator import Paginator
def workstation_index(request):
    return render(request,'workstation/index.html')
def workstation_analysisreport(request):
    files=AttackerModel.objects.filter(att_status="attacked")
    fPosts=AttackerModel.objects.all().order_by("-file_enc_id")
    paginator = Paginator(fPosts,4)
    page_number = request.GET.get('page')
    post = paginator.get_page(page_number)
    return render(request,'workstation/workstation-analysisreport.html',{'file':files,'post':post})
def workstation_dashboard(request):
    users=UserModel.objects.all().count()
    files=FileModel.objects.all().count()
    attackers=AttackerModel.objects.all().count()
                                        return render(request,'workstation/workstation-
dashboard.html',{'x':files,'i':users,'o':attackers})
def workstation_dynamicanalysis(request):
    hostname=socket.gethostname()
    IPadress=socket.gethostbyname(hostname)
    print(IPadress)
    fPosts=FileModel.objects.filter(file_status='marked as ransomware').order_by("-file_id")
    paginator = Paginator(fPosts, 4)
    page_number = request.GET.get('page')
    post = paginator.get_page(page_number')
    return render(request,'workstation/workstation-dynamicanalysis.html',{'post':post})
def workstation_staticanalysis(request):
    hostname=socket.gethostname()
    IPadress=socket.gethostbyname(hostname)
    print(IPadress)
```

```
    fPosts=FileModel.objects.filter(file_status='verification in process').order_by("-file_id")
    paginator = Paginator(fPosts, 4)
    page_number = request.GET.get('page')
    post = paginator.get_page(page_number)
    return render(request,'workstation/workstation-staticanalysis.html',{'post':post})
def markedassafe(request,id):
    file= FileModel.objects.get(file_id=id)
    file.file_status = "marked as safe"
    file.save()
    return redirect ('workstation_safefile')
def markedasransomware(request,id):
    file= FileModel.objects.get(file_id=id)
    file.file_status = "marked as ransomware"
    file.save()
    return redirect ('workstation_dynamicanalysis')
def workstation_ransomwarefile(request):
    fPosts=FileModel.objects.filter(file_status='ransomware').order_by("-file_id")
    paginator = Paginator(fPosts, 4)
    page_number = request.GET.get('page')
    post = paginator.get_page(page_number)
    return render(request,'workstation/workstation-ransomwarefile.html',{'post':post})
def workstation_safefile(request):
    fPosts=FileModel.objects.filter(file_status='marked as safe').order_by("-file_id")
    paginator = Paginator(fPosts, 4)
    page_number = request.GET.get('page')
    post = paginator.get_page(page_number)
    return render(request,'workstation/workstation-safefile.html',{'post':post})
def execute(request,id):
    file=FileModel.objects.get(file_id=id)
    filename = file.file_type
    filepath=file.file_path
    if "C:" in filepath or '.exe' in filename or '.dll' in filename :
        file.file_status='ransomware'
        file.save()
```

```
            messages.success(request,'file found ransomware')
            return redirect('workstation_ransomwarefile')
        else:
            file.file_status='marked as safe'
            file.save()
            messages.error(request,'File is safe')
            return redirect('workstation_safefile')
        return redirect('workstation_ransomwarefile')
```

urls.py

```
from django.contrib import admin
from django.urls import path,include
from django.conf import settings
from django.conf.urls.static import static
from workstationapp import views as workstationapp_views
from usersapp import views as usersapp_views
from mainapp import views as mainapp_views
urlpatterns = [
    path('admin/', admin.site.urls),
#mainapp views
    path('',mainapp_views.main_home,name='main_home'),
    path('main-about',mainapp_views.main_about,name='main_about'),
    path('main-contact',mainapp_views.main_contact,name='main_contact'),
    path('main-features',mainapp_views.main_features,name='main_features'),
    path('main-portfolio',mainapp_views.main_portfolio,name='main_portfolio'),
    path('main-pricing',mainapp_views.main_pricing,name='main_pricing'),
    path('main-services',mainapp_views.main_services,name='main_services'),
    path('main-testimonials',mainapp_views.main_testimonials,name='main_testimonials'),
    path('main-
userregistration',usersapp_views.main_userregistration,name='main_userregistration'),
    path('main-user-login',usersapp_views.main_user_login,name='main_user_login'),
    path('main-
workstationlogin',mainapp_views.main_workstationlogin,name='main_workstationlogin'),
    path('attacker',mainapp_views.attacker,name='attacker'),
    path('enyc/<int:id>/',mainapp_views.enyc,name='enyc'),
```

```
#workstation views
    path('index',workstationapp_views.workstation_index,name='workstation_index'),
    path('workstation-
analysisreport',workstationapp_views.workstation_analysisreport,name='workstation_analysis
report'),
    path('workstation-
dashboard',workstationapp_views.workstation_dashboard,name='workstation_dashboard'),
    path('workstation-
dynamicanalysis',workstationapp_views.workstation_dynamicanalysis,name='workstation_dynamica
nalysis'),
    path('workstation-
staticanalysis',workstationapp_views.workstation_staticanalysis,name='workstation_staticanal
ysis'),
    path('markedassafe/<int:id>/',workstationapp_views.markedassafe,name='markedassafe'),
    path('markedasransomware/<int:id>/',workstationapp_views.markedasransomware,name='
markedasransomware'),
    path('workstation-
safefile',workstationapp_views.workstation_safefile,name='workstation_safefile'),
    path('workstation-
ransomwarefile',workstationapp_views.workstation_ransomwarefile,name='workstation_ransomw
arefile'),
    path('execute/<int:id>/',workstationapp_views.execute,name='execute'),
#usersapp views
   path('user-about-us',usersapp_views.users_about,name='users_about'),
   path('user-contact',usersapp_views.users_contact,name='users_contact'),
   path('user-dashboard',usersapp_views.users_dashboard,name='users_dashboard'),
   path('user-features',usersapp_views.users_features,name='users_features'),
   path('user-index',usersapp_views.users_index,name='users_index'),
   path('user-myfile',usersapp_views.users_myfile,name='users_myfile'),
   path('user-myprofile',usersapp_views.users_myprofile,name='users_myprofile'),
   path('user-portfolio',usersapp_views.users_portfolio,name='users_portfolio'),
   path('user-pricing',usersapp_views.users_pricing,name='users_pricing'),
   path('user-services',usersapp_views.users_services,name='users_services'),
   path('user-testimonials',usersapp_views.users_testimonials,name='users_testimonials'),
```

```
  path('user-uploaddata',usersapp_views.users_uploaddata,name='users_uploaddata'),
] + static(settings.MEDIA_URL,document_root=settings.MEDIA_ROOT)
```

analysisreport.html

```
</head>
 <body>
  <div class="container-scroller">
   <nav class="sidebar sidebar-offcanvas" id="sidebar">
    <div class="text-center sidebar-brand-wrapper d-flex align-items-center">
     <a class="sidebar-brand brand-logo" href="#"><b><h3 style="color: rgb(90, 2,
243);">CYBER FRAUD ADMIN</h3></b></a>
     <a class="sidebar-brand brand-logo-mini pl-4 pt-3" href="index.html"><img
src="assets/images/logo-mini.svg" alt="logo" /></a>
    </div>
    <ul class="nav">
     <li class="nav-item mt-5">
      <a class="nav-link" href="{% url 'workstation_dashboard' %}">
       <i class="mdi mdi-chart-bar menu-icon"></i>
       <span class="menu-title">Dashboard</span>
      </a>
     </li>
     <li class="nav-item">
      <a class="nav-link" data-toggle="collapse" href="#ui-basic" aria-expanded="false"
aria-controls="ui-basic">
       <i class="mdi mdi-contacts menu-icon"></i>
       <span class="menu-title">Data Analysis</span>
       <i class="menu-arrow"></i>
      </a>
      <div class="collapse" id="ui-basic">
       <ul class="nav flex-column sub-menu">
        <li class="nav-item">
         <a class="nav-link" href="{% url 'workstation_staticanalysis' %}">Static
Analysis</a>
        </li>
        <li class="nav-item">
```

```
            <a class="nav-link" href="{% url 'workstation_dynamicanalysis' %}">Dynamic
Analysis</a>
            </li>
            <li class="nav-item">
              <a class="nav-link" href="{% url 'workstation_safefile' %}">Safe File Data</a>
            </li>
            <li class="nav-item">
              <a class="nav-link" href="{% url 'workstation_ransomwarefile' %}">Ransomware
File Data</a>
            </li>
          </ul>
        </div>
      </li>
      <li class="nav-item">
        <a class="nav-link" href="{% url 'workstation_analysisreport' %}">
          <i class="mdi mdi-file-document-box menu-icon"></i>
          <span class="menu-title">Analysis Report</span>
        </a>
      </li>
    </ul>
  </nav>
  <div class="container-fluid page-body-wrapper">
    <div id="theme-settings" class="settings-panel">
      <i class="settings-close mdi mdi-close"></i>
      <p class="settings-heading">SIDEBAR SKINS</p>
      <div class="sidebar-bg-options selected" id="sidebar-default-theme">
        <div class="img-ss rounded-circle bg-light border mr-3"></div> Default
      </div>
      <div class="sidebar-bg-options" id="sidebar-dark-theme">
        <div class="img-ss rounded-circle bg-dark border mr-3"></div> Dark
      </div>
      <p class="settings-heading mt-2">HEADER SKINS</p>
      <div class="color-tiles mx-0 px-4">
        <div class="tiles light"></div>
```

```
          <div class="tiles dark"></div>
        </div>
      </div>
      <nav class="navbar col-lg-12 col-12 p-lg-0 fixed-top d-flex flex-row">
        <div class="navbar-menu-wrapper d-flex align-items-stretch justify-content-between">
          <a class="navbar-brand brand-logo-mini align-self-center d-lg-none" href="{% url
'workstation_dashboard' %}">
          <button class="navbar-toggler navbar-toggler align-self-center mr-2" type="button"
data-toggle="minimize">
            <i class="mdi mdi-menu"></i>
          </button>
          <ul class="navbar-nav">
            </li>
            <li class="nav-item nav-search border-0 ml-1 ml-md-3 ml-lg-5  d-none  d-md-flex" >
              <form class="nav-link form-inline mt-2 mt-md-0" >
                <div class="input-group" style="width: 400px;" >
                  <input type="text" class="form-control" placeholder="Search"  />
                  <div class="input-group-append">
                    <span class="input-group-text">
                      <i class="mdi mdi-magnify"></i>
                    </span>
                  </div>
                </div>
              </form>
            </li>
          </ul>
          <ul class="navbar-nav navbar-nav-right ml-lg-auto">
            <li class="nav-item nav-profile dropdown border-0">
              <a class="nav-link dropdown-toggle" id="profileDropdown" href="#" data-
toggle="dropdown">
                <img class="nav-profile-img mr-2" alt="" src="https://img.freepik.com/free-
vector/businessman-character-avatar-isolated_24877-
60111.jpg?w=740&t=st=1666949636~exp=1666950236~hmac=143c0414ffc7a238eeae219de
95fabe18e8684409e8a588673f05a7c819e468a" >
```

```
            <span class="profile-name">Admin</span>
          </a>
          <div class="dropdown-menu navbar-dropdown w-100" aria-
labelledby="profileDropdown">
            <a class="dropdown-item" href="{% url 'main_home' %}">
              <i class="mdi mdi-logout mr-2 text-primary"></i> Signout </a>
          </div>
        </li>
      </ul>
      <button class="navbar-toggler navbar-toggler-right d-lg-none align-self-center"
type="button" data-toggle="offcanvas">
        <span class="mdi mdi-menu"></span>
      </button>
    </div>
  </nav>
  <div class="main-panel">
    <div class="">
      <div class="container-fluid">
        <div class="row justify-content-center">
          <div class="col-lg-12 grid-margin stretch-card">
            <div class="card">
              <div class="card-body">
                <h4 class="d-flex card-title">Analysis Report</h4>
                <div class="table-responsive">
                  <table class="table table-striped">
                    <thead>
                      <tr>
                        <th>Date&Time</th>
                        <!-- <th>Time</th> -->
                        <th>Event ID</th><th> Action</th>
                        <!-- <th>Computer</th> -->
                        <th>Target-UserName</th>
                        <th>IP Address</th>
                        <th>Attacker Pc</th>
```

```
                    </tr>
                   </thead>
                   <tbody style="Width:5px;
                   Height:10 px;
                   Overflow-x:scroll;">
                   {% for i in post %}
                   <tr>
                    <td>{{i.att_date}}</td>
                    <td>{{i.file_enc_id}}</td>
                    <td>{{i.att_status}}</td>
                    <td> {{i.file_enc.user.user_name}}</td>
                    <!-- <td>Herman Beck</td> -->
                    <td>{{i.att_ip}}</td>
                    <td>{{i.att_pc}} </td>
                    {% endfor %}
                   </tr>
                   </tbody>
                  </table>
                 <nav aria-label="Page navigation example">
                  <ul class="pagination ml-2">
                     {% if post.has_previous %}
                        <!-- <li class="page-item"><a class="page-link" href="?page=1">&laquo;
First</a></li> -->
                        <li class="page-item"><a class="page-link bg-info text-white"
href="?page={{ post.previous_page_number }}">Previous</a></li>
                     {% endif %}
                     {% if post.has_next %}
                     <li class="page-item"><a class="page-link bg-info text-white"
href="?page={{ post.next_page_number }}">Next</a></li>
                     <!-- <li class="page-item"><a class="page-link" href="?page={{
r.paginator.num_pages }}">Last &raquo;</a></li> -->
                     {% endif %}
                  </ul>
                  Page {{ post.number }} of {{ post.paginator.num_pages }}.
```

```
                </nav>
              </div>
            </div>
          </div>
        </div>
      </div>
    </div>
        <!-- page-body-wrapper ends -->
      </div>
  <!-- container-scroller -->
  <!-- plugins:js -->
  <script src="{% static 'workstation/assets/vendors/js/vendor.bundle.base.js' %}"></script>
  <!-- endinject -->
  <!-- Plugin js for this page -->
  <script src="{% static 'workstation/assets/vendors/chart.js/Chart.min.js' %}"></script>
  <script src="{% static 'workstation/assets/vendors/bootstrap-datepicker/bootstrap-
datepicker.min.js' %}"></script>
  <script src="{% static 'workstation/assets/vendors/flot/jquery.flot.js' %}"></script>
  <script src="{% static 'workstation/assets/vendors/flot/jquery.flot.resize.js' %}"></script>
  <script src="{% static 'workstation/assets/vendors/flot/jquery.flot.categories.js'
%}"></script>
  <script src="{% static 'workstation/assets/vendors/flot/jquery.flot.fillbetween.js'
%}"></script>
  <script src="{% static 'workstation/assets/vendors/flot/jquery.flot.stack.js' %}"></script>
  <script src="{% static 'workstation/assets/vendors/flot/jquery.flot.pie.js' %}"></script>
  <!-- End plugin js for this page -->
  <!-- inject:js -->
  <script src="{% static 'workstation/assets/js/off-canvas.js' %}"></script>
  <script src="{% static 'workstation/assets/js/hoverable-collapse.js' %}"></script>
  <script src="{% static 'workstation/assets/js/misc.js' %}"></script>
  <!-- endinject -->
  <!-- Custom js for this page -->
  <script src="{% static 'workstation/assets/js/dashboard.js' %}"></script>
```

```
    <!-- End custom js for this page -->
  </body>
</html>
```

urls.py

```
from django.contrib import admin
from django.urls import path,include
from django.conf import settings
from django.conf.urls.static import static
from workstationapp import views as workstationapp_views
from usersapp import views as usersapp_views
from mainapp import views as mainapp_views

urlpatterns = [
    path('admin/', admin.site.urls),

#mainapp views
   path('',mainapp_views.main_home,name='main_home'),
   path('main-about',mainapp_views.main_about,name='main_about'),
   path('main-contact',mainapp_views.main_contact,name='main_contact'),
   path('main-features',mainapp_views.main_features,name='main_features'),

   path('main-portfolio',mainapp_views.main_portfolio,name='main_portfolio'),
   path('main-pricing',mainapp_views.main_pricing,name='main_pricing'),
   path('main-services',mainapp_views.main_services,name='main_services'),
   path('main-testimonials',mainapp_views.main_testimonials,name='main_testimonials'),
   path('main-
userregistration',usersapp_views.main_userregistration,name='main_userregistration'),
   path('main-user-login',usersapp_views.main_user_login,name='main_user_login'),
   path('main-
workstationlogin',mainapp_views.main_workstationlogin,name='main_workstationlogin'),
   path('attacker',mainapp_views.attacker,name='attacker'),
   path('enyc/<int:id>/',mainapp_views.enyc,name='enyc'),
#workstation views
    path('index',workstationapp_views.workstation_index,name='workstation_index'),
```

```
    path('workstation-
analysisreport',workstationapp_views.workstation_analysisreport,name='workstation_analysis
report'),
    path('workstation-
dashboard',workstationapp_views.workstation_dashboard,name='workstation_dashboard'),
    path('workstation-
dynamicanalysis',workstationapp_views.workstation_dynamicanalysis,name='workstation_dy
namicanalysis'),
    path('workstation-
staticanalysis',workstationapp_views.workstation_staticanalysis,name='workstation_staticanal
ysis'),
    path('markedassafe/<int:id>/',workstationapp_views.markedassafe,name='markedassafe'),

path('markedasransomware/<int:id>/',workstationapp_views.markedasransomware,name='mar
kedasransomware'),
    path('workstation-
safefile',workstationapp_views.workstation_safefile,name='workstation_safefile'),
    path('workstation-
ransomwarefile',workstationapp_views.workstation_ransomwarefile,name='workstation_ranso
mwarefile'),
    path('execute/<int:id>/',workstationapp_views.execute,name='execute'),
#usersapp views
   path('user-about-us',usersapp_views.users_about,name='users_about'),
   path('user-contact',usersapp_views.users_contact,name='users_contact'),
   path('user-dashboard',usersapp_views.users_dashboard,name='users_dashboard'),
   path('user-features',usersapp_views.users_features,name='users_features'),
   path('user-index',usersapp_views.users_index,name='users_index'),
   path('user-myfile',usersapp_views.users_myfile,name='users_myfile'),
   path('user-myprofile',usersapp_views.users_myprofile,name='users_myprofile'),
   path('user-portfolio',usersapp_views.users_portfolio,name='users_portfolio'),
   path('user-pricing',usersapp_views.users_pricing,name='users_pricing'),
   path('user-services',usersapp_views.users_services,name='users_services'),
   path('user-testimonials',usersapp_views.users_testimonials,name='users_testimonials'),
   path('user-uploaddata',usersapp_views.users_uploaddata,name='users_uploaddata')
```

4.2 EXECUTION FLOW:

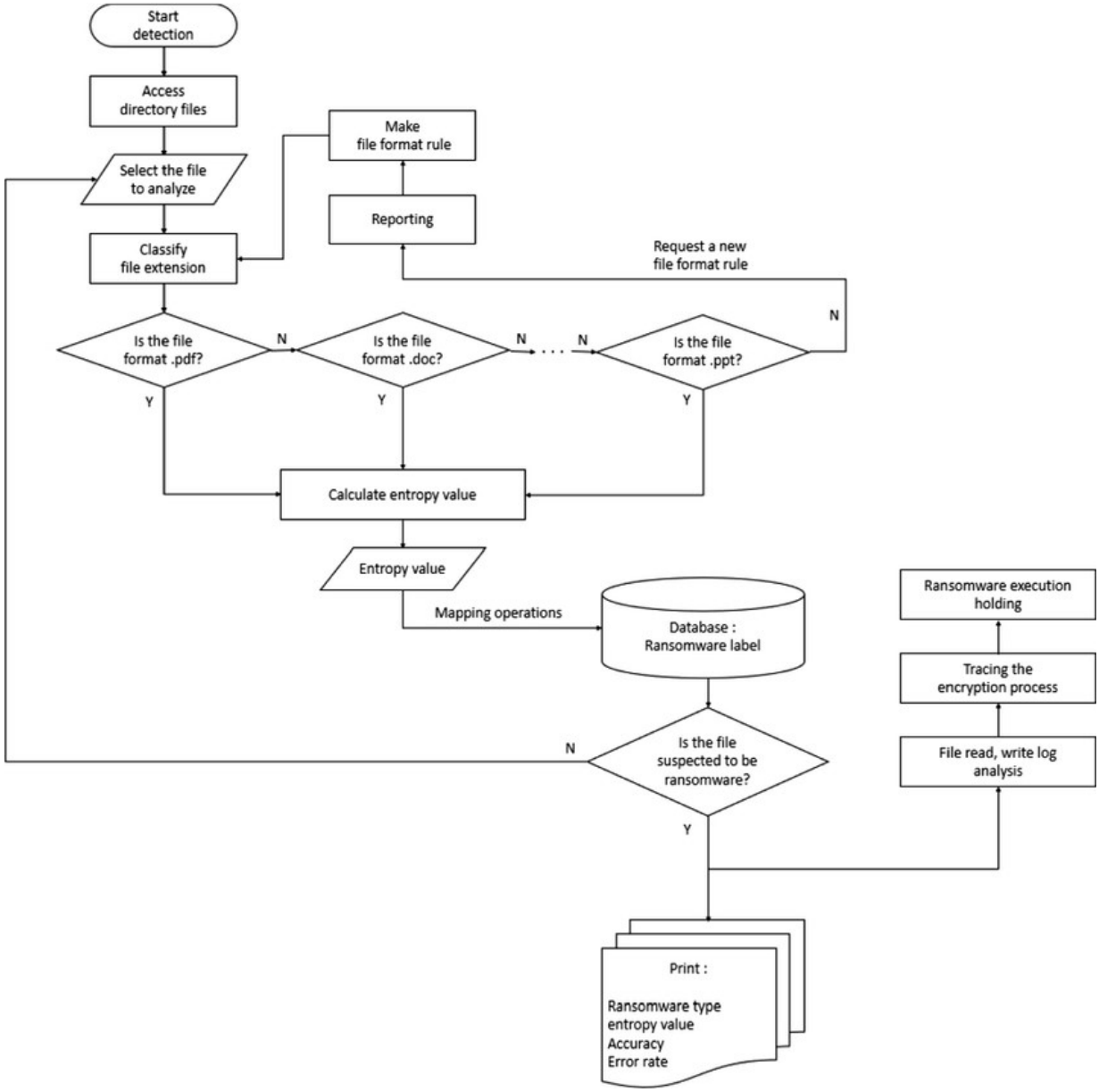


Fig 4.2 Execution Flow

CHAPTER 5

RESULTS

5.1 RESULTING SCREENS:

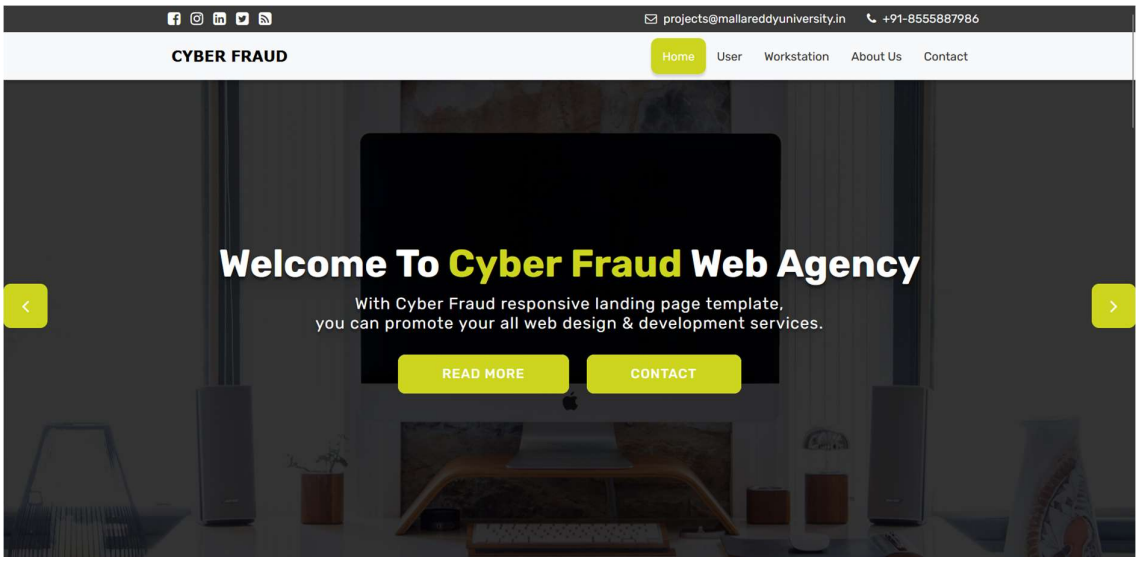


Fig.5.1.1 Website Home page

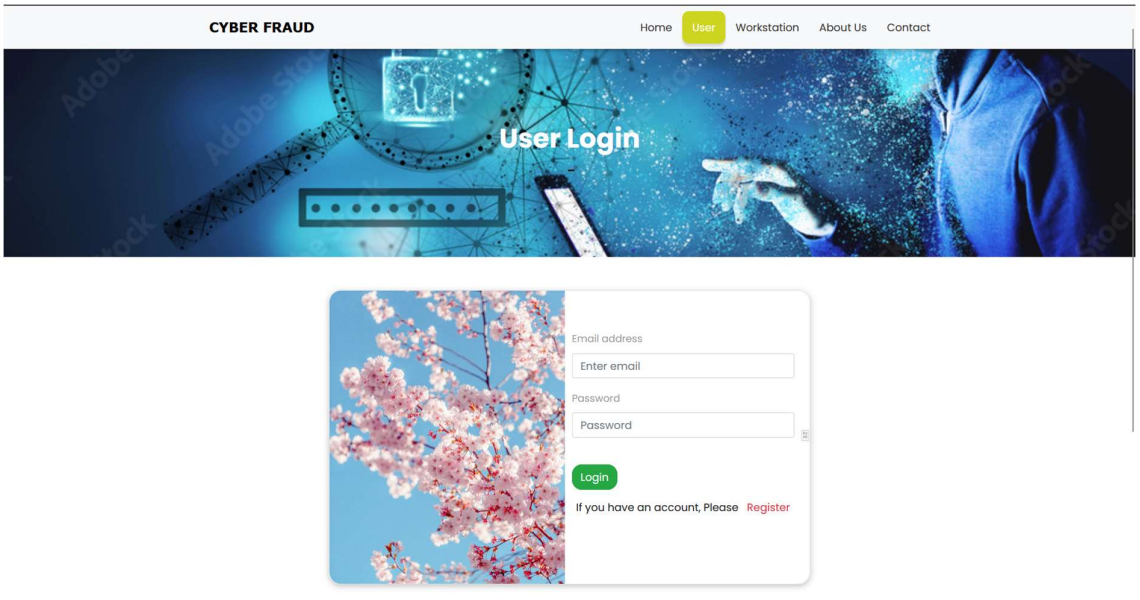


Fig.5.1.2 User Login Page

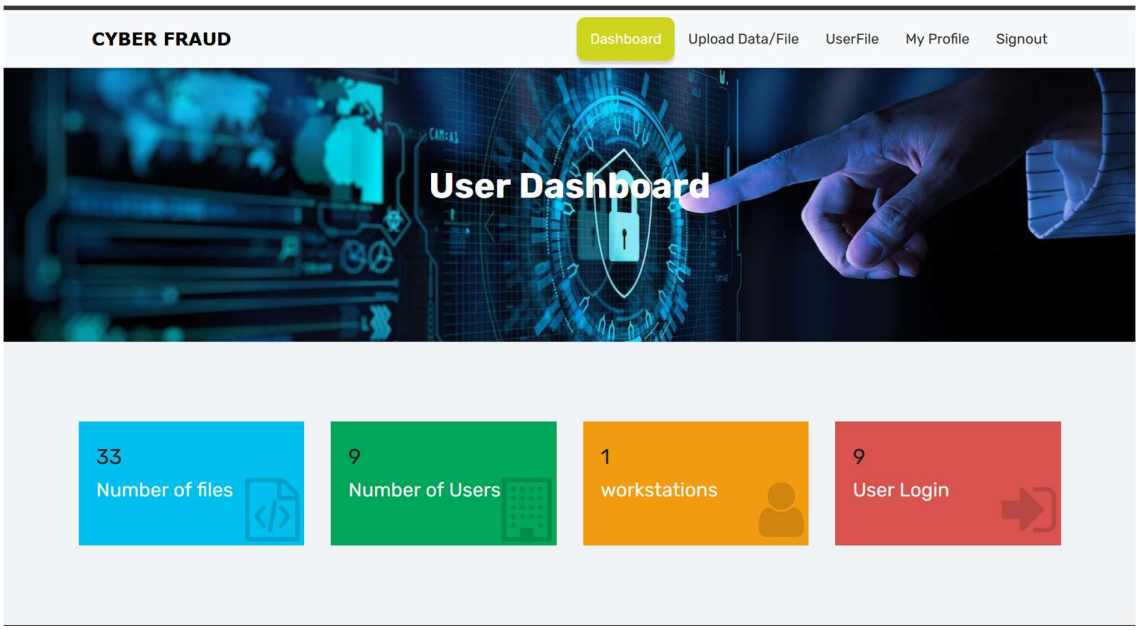


Fig.5.1.3 User Dashboard

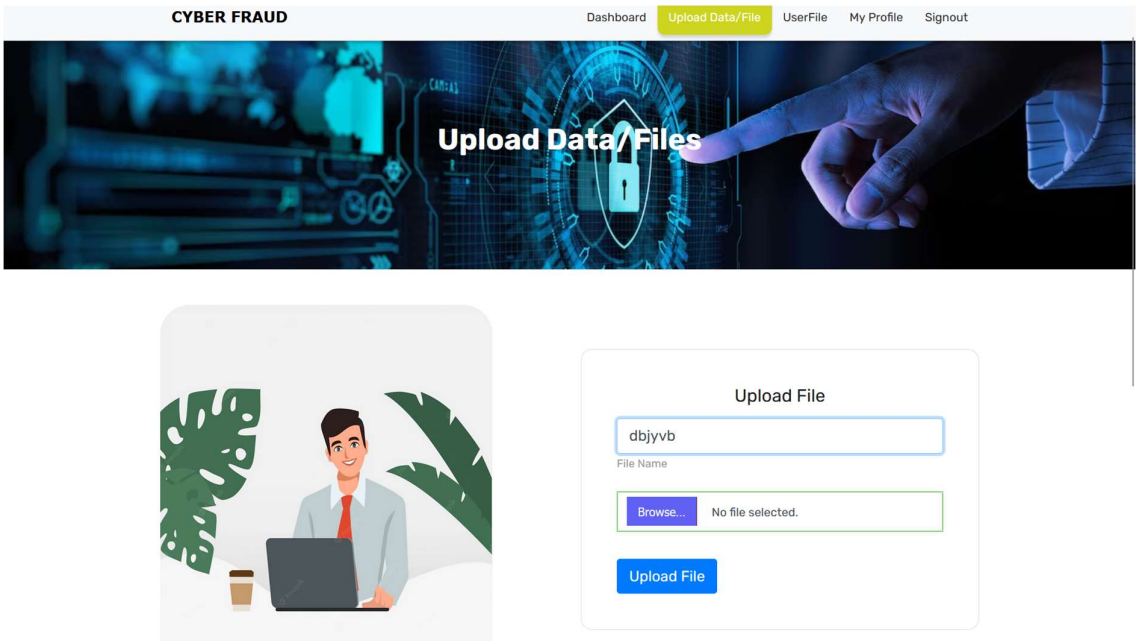


Fig.5.1.4 User Data Upload page

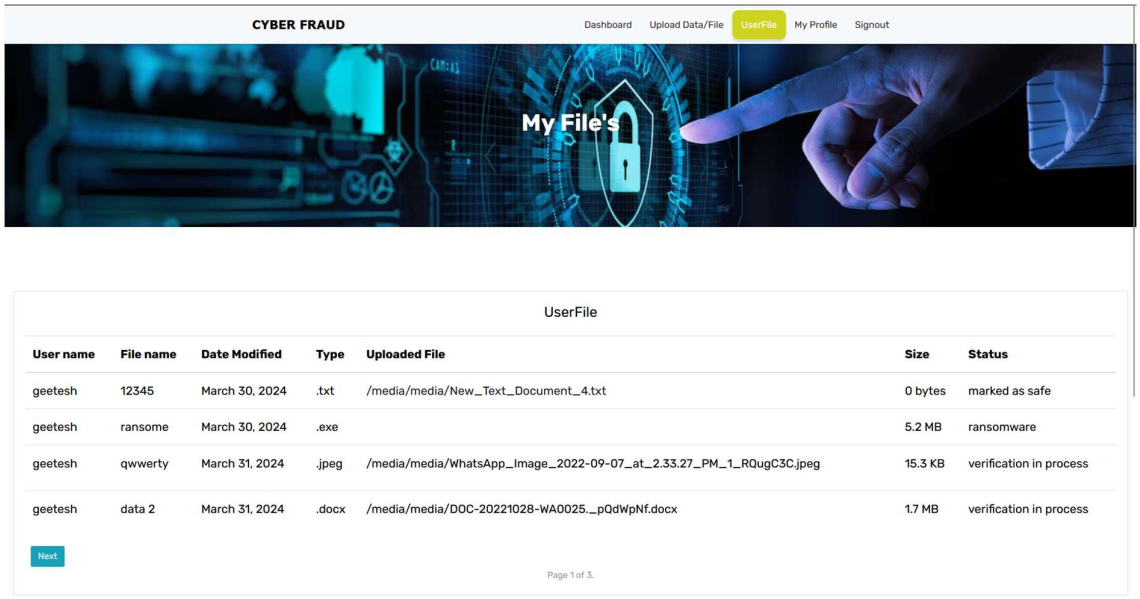


Fig.5.1.5 Results page

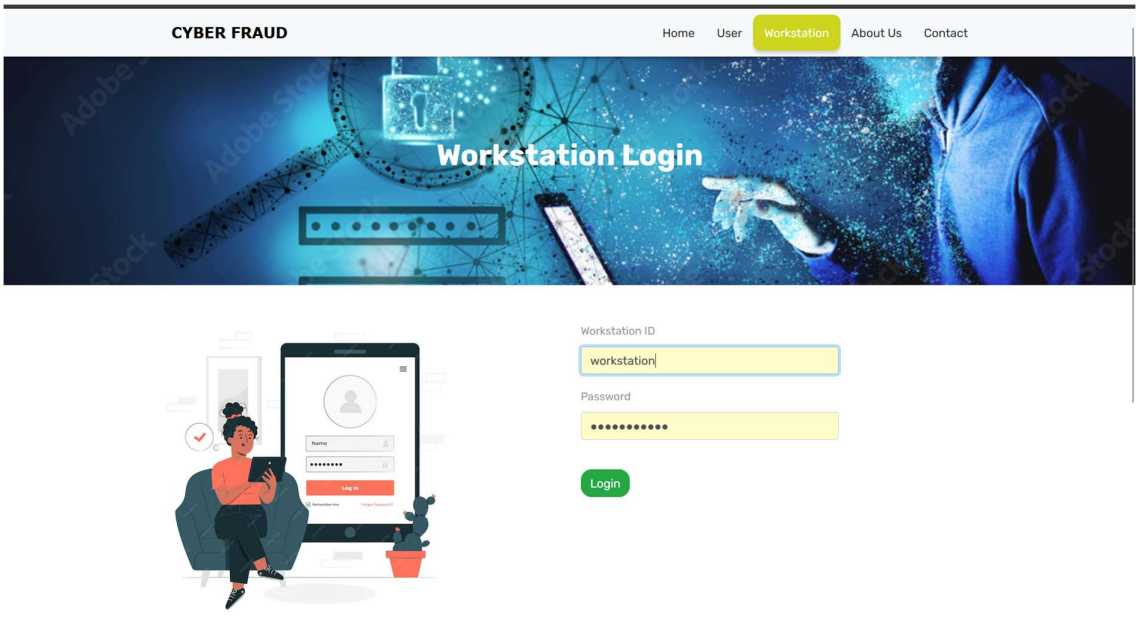


Fig.5.1.6 Admin Login page

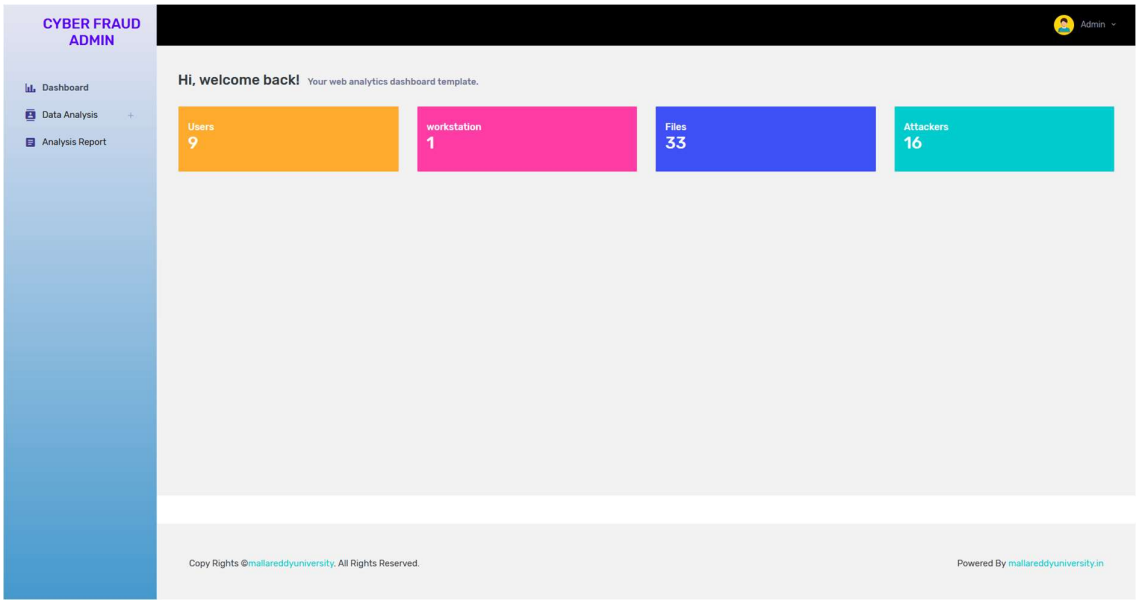


Fig.5.1.7 Admin Dashboard

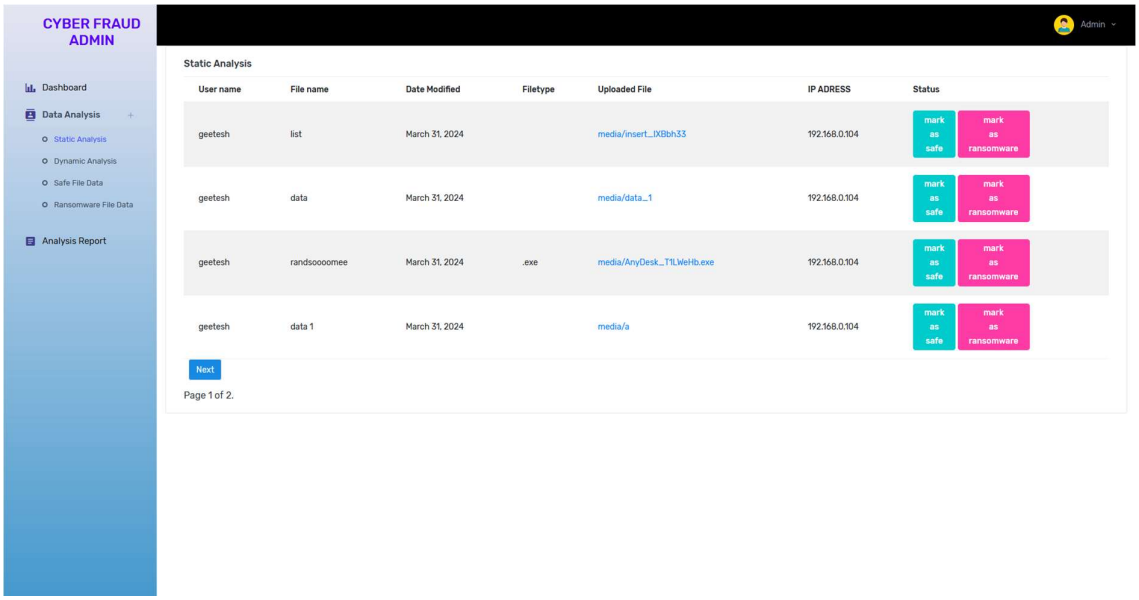


Fig.5.1.8 Static Analysis

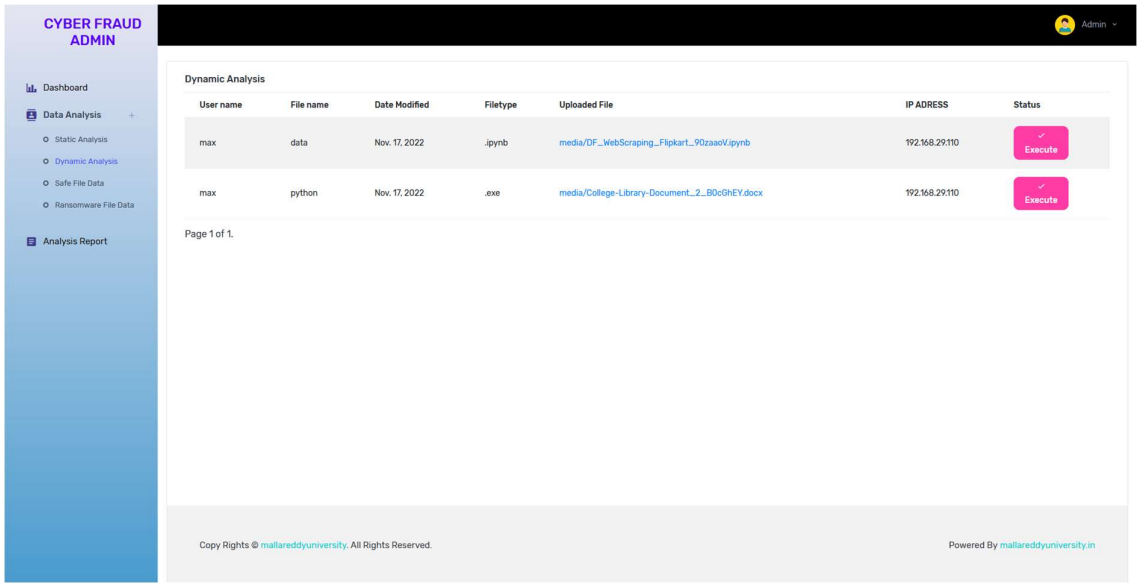


Fig.5.1.9 Dynamic analysis

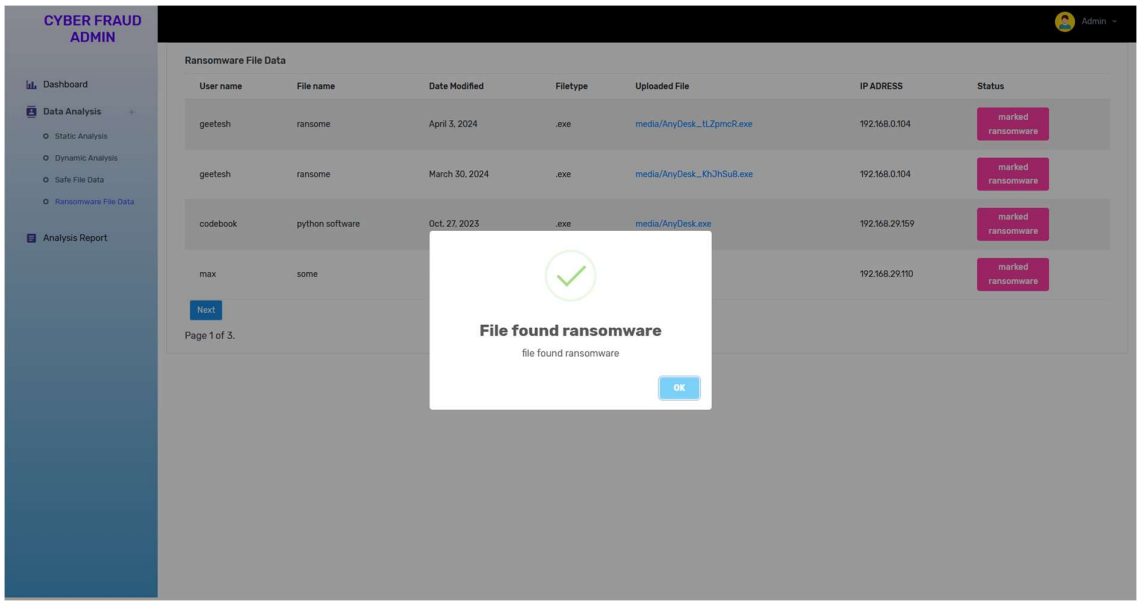


Fig.5.1.10 File found Ransomware

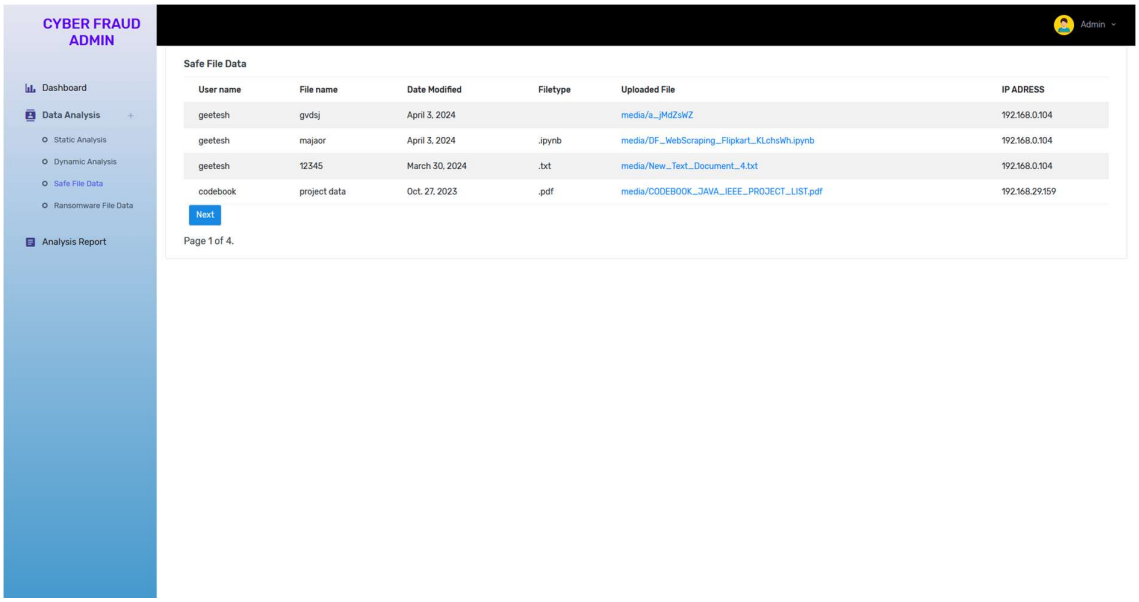


Fig.5.1.11 Safe files data

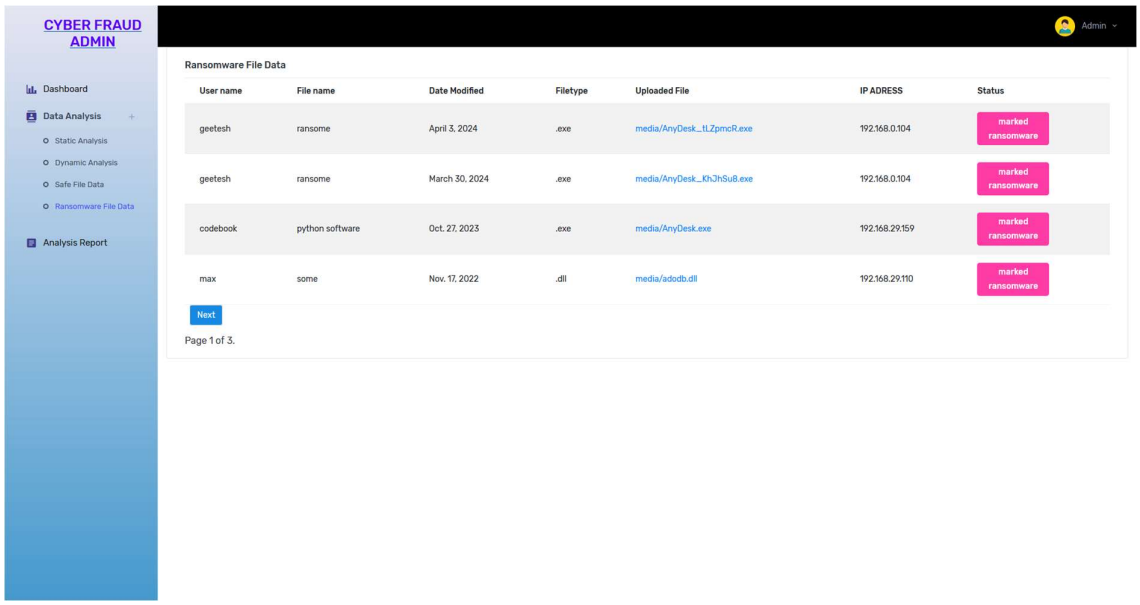


Fig.5.1.12 Malicious files data

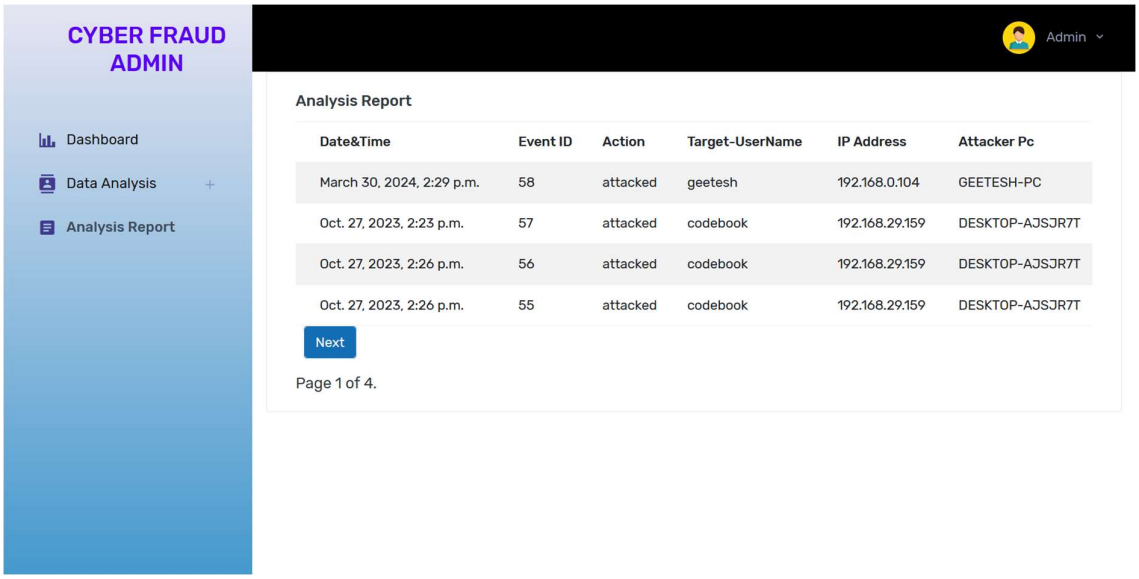


Fig.5.1.13 Analysis report

5.2 RESULTING TABLES:

Attacker_file_details

Table comments: attacker_file_details

Column	Type	Null	Default
id	bigint(20)	No	
file_enc_id	int(11)	No	
file_name	varchar(50)	Yes	*NULL*
file_type	varchar(50)	Yes	*NULL*
user_name	varchar(50)	Yes	*NULL*
att_date	datetime(6)	Yes	*NULL*
att_status	varchar(50)	Yes	*NULL*
att_ip	varchar(50)	Yes	*NULL*
att_url	varchar(100)	Yes	*NULL*
att_pc	longtext	Yes	*NULL*

Table 5.2.1 : Attacker file details

Indexes values of attacker file details

Keyname	Type	Unique	Packed	Column	Cardinality	Collation	Null
PRIMARY	BTREE	Yes	No	id	11	A	No
attacker_file_details_user_id_6d71a0b4	BTREE	No	No	file_enc_id		A	No

Table 5.2.2 : Index values of attacker file details

auth_group

Table comments: auth_group

Column	Type	Null	Default
id	int(11)	No	
name	varchar(150)	No	

Table 5.2.3 : Contains information about user groups for authentication purposes.

Auth group Index values

Keyname	Type	Unique	Packed	Column	Cardinality	Collation	Null
PRIMARY	BTREE	Yes	No	id	0	A	No
name	BTREE	Yes	No	name	0	A	No

Table 5.2.4 : Index valus of auth group

auth_group_permissions

Table comments: auth_group_permissions

Column	Type	Null	Default
id	bigint(20)	No	
group_id	int(11)	No	
permission_id	int(11)	No	

Table 5.2.5 : Manages permissions for user groups.

Permissions of auth group indexes

Keyname	Type	Unique	Packed	Column	Cardinality	Collation	Null
PRIMARY	BTREE	Yes	No	id	0	A	No
auth_group_permissions_group_id_permission_id_0cd325b0_uniq	BTREE	Yes	No	group_id		A	No
				permission_id	0	A	No
auth_group_permissions_group_id_b120cbf9	BTREE	No	No	group_id		A	No
auth_group_permissions_permission_id_84c5c92e	BTREE	No	No	permission_id		A	No

Table 5.2.6 : Attacker file details

auth_permission

Column	Type	Null	Default
id	int(11)	No	
name	varchar(255)	No	
content_type_id	int(11)	No	
codename	varchar(100)	No	

Table 5.2.7 : Stores permissions granted to users or groups.

Keyname	Type	Unique	Packed	Column	Cardinality	Collation	Null
PRIMARY	BTREE	Yes	No	id	36	A	No
auth_permission_content_type_id_codename_01ab375a_uniq	BTREE	Yes	No	content_type_id		A	No
				codename	36	A	No
auth_permission_content_type_id_2f476e4b	BTREE	No	No	content_type_id		A	No

Table 5.2.8 : Attacker file details

auth_user

Table comments: auth_user

Column	Type	Null	Default
id	int(11)	No	
password	varchar(128)	No	
last_login	datetime(6)	Yes	*NULL*
is_superuser	tinyint(1)	No	
username	varchar(150)	No	
first_name	varchar(150)	No	
last_name	varchar(150)	No	
email	varchar(254)	No	
is_staff	tinyint(1)	No	
is_active	tinyint(1)	No	
date_joined	datetime(6)	No	

Table 5.2.9 : Contains information about registered users.

User authentication indexes

Keyname	Type	Unique	Packed	Column	Cardinality	Collation	Null	Comment
PRIMARY	BTREE	Yes	No	id	0	A	No	
username	BTREE	Yes	No	username	0	A	No	

Table 5.2.10 : Attacker file details

auth_user_groups

Table comments: auth_user_groups

Column	Type	Null	Default	Comments
id	bigint(20)	No		
user_id	int(11)	No		
group_id	int(11)	No		

Table 5.2.11 : Maps users to their respective groups.

User group indexes

Keyname	Type	Unique	Packed	Column	Cardinality	Collation	Null	Comment
PRIMARY	BTREE	Yes	No	id	0	A	No	
auth_user_groups_user_id_group_id_94350c0c_uniq	BTREE	Yes	No	user_id		A	No	
				group_id	0	A	No	
auth_user_groups_user_id_6a12ed8b	BTREE	No	No	user_id		A	No	
auth_user_groups_group_id_97559544	BTREE	No	No	group_id		A	No	

Table 5.2.12 : Attacker file details

auth_user_user_permissions

Table comments: auth_user_user_permissions

Column	Type	Null	Default	Comments
id	bigint(20)	No		
user_id	int(11)	No		
permission_id	int(11)	No		

Table 5.2.13 : Manages individual user permissions.

Values of user permissions

Keyname	Type	Unique	Packed	Column	Cardinality	Collation	Null	Comment
PRIMARY	BTREE	Yes	No	id	0	A	No	
auth_user_user_permissions_user_id_permission_id_14a6b632_uniq	BTREE	Yes	No	user_id		A	No	
				permission_id	0	A	No	
auth_user_user_permissions_user_id_a95ead1b	BTREE	No	No	user_id		A	No	
auth_user_user_permissions_permission_id_1fbb5f2c	BTREE	No	No	permission_id		A	No	

Table 5.2.14 : index values of user permissions

data_file_details

Table comments: data_file_details

Column	Type	Null	Default	Comments
file_id	int(11)	No		
file_name	varchar(50)	Yes	*NULL*	
file_type	varchar(50)	Yes	*NULL*	
file_date	date	Yes	*NULL*	
file_upload	varchar(100)	Yes	*NULL*	
user_id	int(11)	Yes	*NULL*	
file_status	varchar(50)	Yes	*NULL*	
attack_status	varchar(50)	Yes	*NULL*	

Table 5.2.15 : Stores details about uploaded files and their statuses.

Indexes of data file details

Keyname	Type	Unique	Packed	Column	Cardinality	Collation	Null	Comment
PRIMARY	BTREE	Yes	No	file_id	19	A	No	
data_file_details_user_id_0fbb8ecd	BTREE	No	No	user_id		A	Yes	

Table 5.2.16 : Stores details about index values in uploaded files.

django_admin_log

Table comments: django_admin_log

Column	Type	Null	Default	Comments
id	int(11)	No		
action_time	datetime(6)	No		
object_id	Longtext	Yes	*NULL*	
object_repr	varchar(200)	No		
action_flag	smallint(5)	No		
change_message	Longtext	No		
content_type_id	int(11)	Yes	*NULL*	
user_id	int(11)	No		

Table 5.2.17 : Logs administrative actions performed in the Django admin interface.

Django admin log indexes

Keyname	Type	Unique	Packed	Column	Cardinality	Collation	Null	Comment
PRIMARY	BTREE	Yes	No	id	0	A	No	
django_admin_log_content_type_id_c4bce8eb	BTREE	No	No	content_type_id		A	Yes	
django_admin_log_user_id_c564eba6	BTREE	No	No	user_id		A	No	

Table 5.2.18 : Holds index data for user IDs in admin logs.

django_content_type

Table comments: django_content_type

Column	Type	Null	Default	Comments
id	int(11)	No		
app_label	varchar(100)	No		
model	varchar(100)	No		

Table 5.2.19 : Stores content types used in the Django application.

Stores session data indexes

Keyname	Type	Unique	Packed	Column	Cardinality	Collation	Null	Comment
PRIMARY	BTREE	Yes	No	id	9	A	No	
django_content_type_app_label_model_76bd3d3b_uniq	BTREE	Yes	No	app_label		A	No	
				model	9	A	No	

Table 5.2.20 : Stores session data for user sessions in Django.

django_migrations

Table comments: django_migrations

Column	Type	Null	Default
id	bigint(20)	No	
app	varchar(255)	No	
name	varchar(255)	No	
applied	datetime(6)	No	

Table 5.2.21 : Tracks migrations applied to the Django application.

Attacker file indexes

Keyname	Type	Unique	Packed	Column	Cardinality	Collation	Null
PRIMARY	BTREE	Yes	No	id	31	A	No

Table 5.2.22 : Attacker file details

django_session

Table comments: django_session

Column	Type	Null	Default
session_key	varchar(40)	No	
session_data	longtext	No	
expire_date	datetime(6)	No	

Table 5.2.23 : Stores session data for user sessions in Django.

Session details

Keyname	Type	Unique	Packed	Column	Cardinality	Collation	Null	Comment
PRIMARY	BTREE	Yes	No	session_key	2	A	No	
django_session_expire_date_a5c62663	BTREE	No	No	expire_date		A	No	

Table 5.2.24 :Index of session details

user_complete_details

Table comments: user_complete_details

Column	Type	Null	Default
user_id	int(11)	No	
user_name	varchar(50)	Yes	*NULL*
user_email	varchar(50)	No	
user_password	varchar(50)	Yes	*NULL*
user_contact	varchar(50)	Yes	*NULL*
user_city	varchar(200)	Yes	*NULL*
user_dob	Date	Yes	*NULL*
user_image	varchar(100)	Yes	*NULL*
user_ip	varchar(50)	Yes	*NULL*

Table 5.2.25 : Contains comprehensive details about users, including personal information and preferences.

Indexes

Keyname	Type	Unique	Packed	Column	Cardinality	Collation	Null
PRIMARY	BTREE	Yes	No	user_id	7	A	No

Table 5.2.26 : Index of user details

5.3 RESULTING GRAPHS:

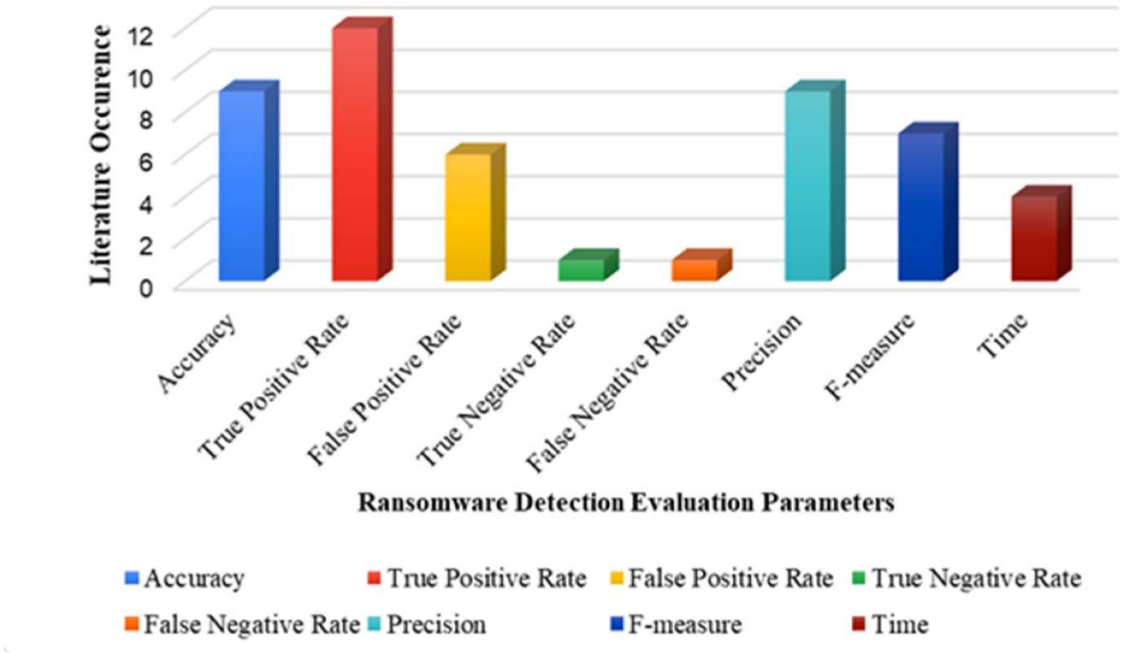


Fig 5.3.1 Ransomware Detection Evaluation Process

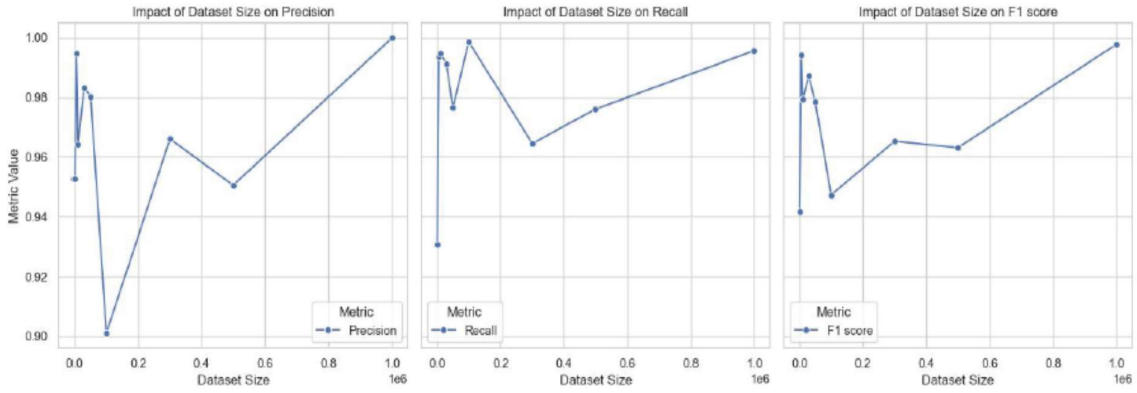


Fig 5.3.2 Scalability Performance

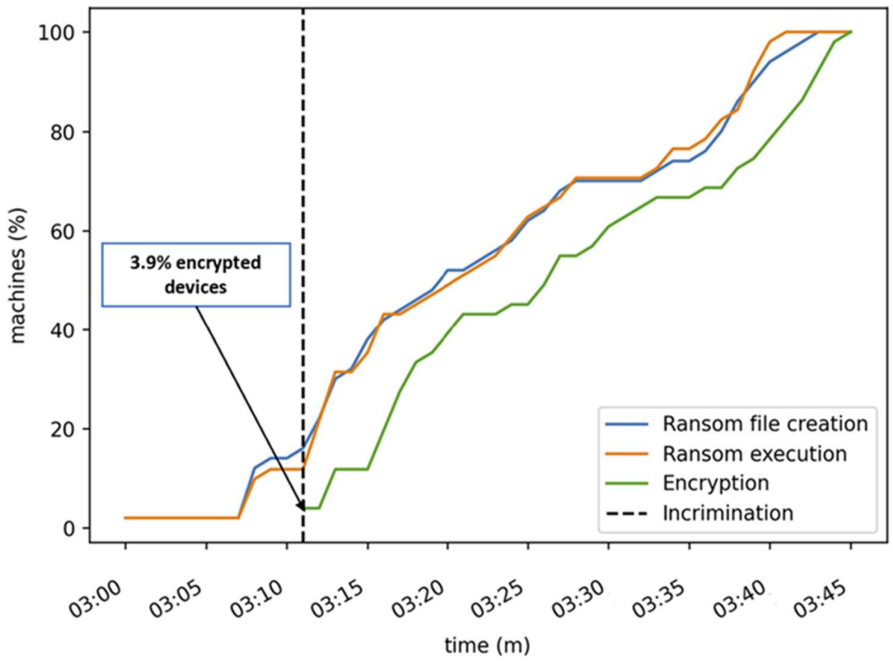


Fig 5.3.3 Statistics of ransomware encryption process

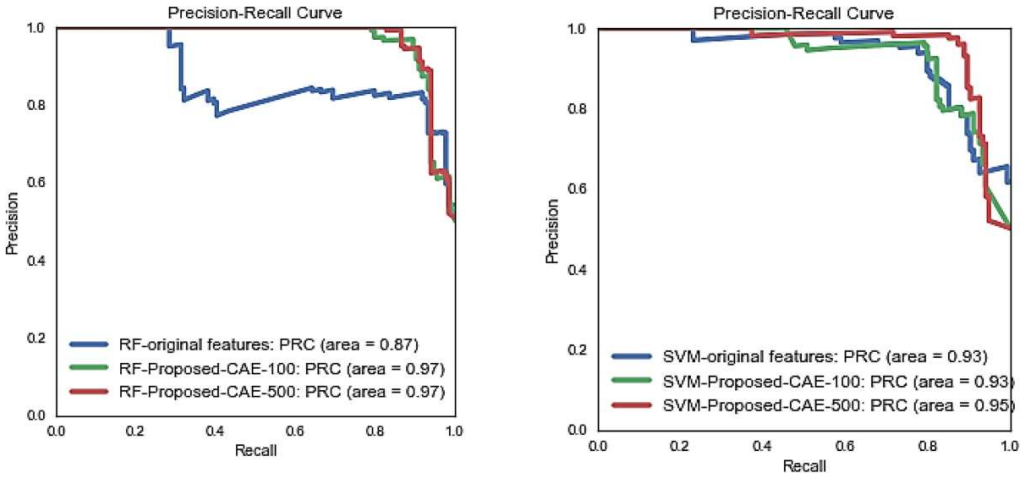


Fig 5.3.4 Precision recall curve using the algorithms

CHAPTER 6

CONCLUSIONS AND FUTURE SCOPE OF STUDY

6.1 CONCLUSIONS:

A large increase in the number crypto-ransomware attacks has been experienced, especially with the popularity of virtual currency. This situation is due to the difficulty in legally tracing virtual currency. Attackers encrypt the victim's files with crypto-ransomware and inform them that they need to buy an encryption key to ensure access to their files again. Due to the encryption type used in ransomware it is nearly impossible to break the encryption through outside intervention and this is accepted as technically impossible. held in a storage area they own. In recent times, attackers have sent a message stating that they will unencrypt a file of the victim's choosing not above 100 MB in order to make sure the victim believes the situation. When the victim agrees, they are successfully given access to the file. However, when the victim pays the desired ransom the attacker has achieved their aim and communication ceases.

Analysis of ransomware encompasses detection of this software, understanding how it works and reaching the attacker. During crypto-ransomware analysis, reverse engineering techniques are used and the structure of the malware and interaction with the system are determined.

6.2 FUTURE SCOPE:

In contemplating the future trajectory of this system, numerous avenues for advancement emerge. Firstly, the integration of cutting-edge machine learning algorithms holds promise for enhancing ransomware detection and analysis capabilities. Techniques like deep learning and anomaly detection could empower the system to dynamically adapt, effectively identifying evolving ransomware variants and sophisticated evasion tactics.

Furthermore, the incorporation of real-time threat intelligence feeds and external data sources could significantly bolster the system's ability to detect and respond swiftly to ransomware threats. By continuously monitoring global threat landscapes and analyzing indicators, the

system could issue proactive alerts and recommendations, facilitating preemptive actions against potential ransomware attacks.

Automation presents another avenue for future development. By integrating automated workflows and orchestration techniques, the system could initiate containment measures, restore affected systems, and mitigate the impact of ransomware incidents rapidly and automatically, thereby minimizing downtime and disruption.

Moreover, exploring the integration of blockchain technology could enhance the security and integrity of the system's data storage and analysis processes. Leveraging blockchain for immutable record-keeping and decentralized consensus mechanisms could fortify data integrity, auditability, and resilience against tampering or manipulation attempts.

Additionally, integrating the system with cloud-based services could offer scalability, flexibility, and accessibility benefits. By leveraging cloud infrastructure for data storage, processing, and analysis, the system could accommodate increasing data volumes and user demands while ensuring high availability and reliability of services.

BIBLIGRAPHY

- W3 School – (https://www.w3schools.com/python/)
- Geek for Geeks – (https://www.geeksforgeeks.org/python-programming-language/learn-python-tutorial/)
- Python Official Documentation – (https://docs.python.org/3/tutorial/)
- Tutorials Point – (https://www.tutorialspoint.com/python/index.htm)
- Real Python – (https://realpython.com/)
- Django for Beginners – (https://djangoforbeginners.com/introduction/)
- Guru99 – (https://www.guru99.com/django-tutorial.html)

REFERENCES

[1] M. Egele, T.Scholte, E. Kirda, & C. Kruegel, 2008. A survey on automated dynamic malware-analysis techniques and tools. ACM computing surveys (CSUR), 44(2), 1-42.

[2] D. Kim, D. Shin, D. Shin, & Y. H. Kim, 2019. Attack detection application with attack tree for mobile system using log analysis. Mobile Networks and Applications, 24(1), 184-192.

[3] F. L. Lévesque, S. Chiasson, A. Somayaji, & J. M. Fernandez, 2018. Technological and human factors of malware attacks: A computer security clinical trial approach. ACM Transactions on Privacy and Security (TOPS), 21(4), 1-30.

[4] İ. Kara, M. Aydos, 2019. The ghost in the system: technical analysis of remote access trojan. International Journal on Information Technologies & Security, 11(1).

[5] I. Kara, M. Aydos, 2018, December. Static and dynamic analysis of third generation cerber ransomware. In 2018 International Congress on Big Data, Deep Learning and Fighting Cyber Terrorism (IBIGDELFT) (pp. 12-17). IEEE.

[6] B. A. S. Al-rimy, M. A. Maarof, S. Z. M. Shaid, 2018. Ransomware threat success factors, taxonomy, and countermeasures: A survey and research directions. Computers & Security, 74, 144-166.

[7] S. Baek, Y. Jung, A. Mohaisen, S. Lee, D. Nyang, 2018, July. SSDinsider: Internal defense of solid-state drive against ransomware with perfect data recovery. In 2018 IEEE 38th International Conference on Distributed Computing Systems (ICDCS) (pp. 875-884). IEEE.

[8] M. A. S. Monge, J. M. Vidal, L. J. G. Villalba, 2018, August. A novel Self-Organizing Network solution towards Crypto-ransomware Mitigation. In Proceedings of the 13th International Conference on Availability, Reliability and Security (pp. 1-10).

[9] K. İlker, M. Aydos. (2019, October). Detection and Analysis of Attacks Against Web Services by the SQL Injection Method. In 2019 3rd International Symposium on Multidisciplinary Studies and Innovative Technologies (ISMSIT) (pp. 1-4). IEEE.on Electronic Crime Research (eCrime) (pp. 1-13). IEEE.

[10] S. Mohurle, M. Patil, 2017. A brief study of wannacry threat: Ransomware attack 2017. International Journal of Advanced Research in Computer Science, 8(5).

[11] F. Karbalaie, A. Sami, and M. Ahmadi. 2012.Semantic malware detection by deploying graph mining. International Journal of Computer Science Issues,9(1):373-379.

[12] D. Sgandurra, L. Munoz-Gonz_alez, R. Mohsen, and E. C. Lupu. 2016. Automated dynamic analysis of ransomware: Bene_ts, limitations and use for detection. arXiv preprint arXiv:1609.03020.

[13] D. Kim and S. Kim. 2015. Design of quanti-cation model for ransom ware prevent. World Journal of Engineering and Technology, 3(03):203.

[14] A. Kharraz, S. Arshad, C. Mulliner, W. K. Robertson, and E. Kirda. 2016.Unveil: A large-scal, automated approach to detecting ransomware. In USENIX Security Symposium, pages 757-772.

[15] https://websitem.karatekin.edu.tr/ilkerkara/paylasimlar/dosya/0f7a100dc f5c42d2

[16] M. Boldt, andB. Carlsson.2006 Analysing privacy-invasive software using computer forensic methods. ICSEA, Papeetee.

[17] S. Z. M. Shaid, and M. A. Maarof. 2014. Malware behavior image for malware variant identification", 2014 International Symposium on Biometrics and Security Technologies (ISBAST). IEEE, 2014.

[18] I. Kara. 2019. A basic malware analysis method. Computer Fraud & Security, 2019(6), 11-19.

[19] M. Kbanov, V. G. Vassilakis, M. D. Logothetis. 2019. WannaCry ransomware: Analysis of infection, persistence, recovery prevention and propagation mechanisms. Journal of Telecommunications and Information Technology.

[20] J. Hwang, J. Kim, S. Lee, K. Kim, K. 2020. Two-Stage Ransomware Detection Using Dynamic Analysis and Machine Learning Techniques. Wireless Personal Communications, 112(4), 2597-2609.

PAPER PUBLICATION

CYBER FRAUD - DETECTION AND ANALYSIS OF THE CRYPTO-RANSOMWARE

Kunchum Lakshmi Geetesh[1], Kaza Kedari Neha[2], Dodda Vineeth[3], Akula Chandan[4], P.Shanmukha Kumar[5]

[1-4]Department Of Cybersecurity, Malla reddy University, Hyderabad, Telangana, India.
[5]Assistant Professor, Department of Cybersecurity, Malla reddy University, Hyderabad, Telangana, India.

2011cs040035@mallareddyuniversity.ac.in[1], 2011cs040034@mallareddyuniversity.ac.in[2], 2011cs040020@mallareddyuniversity.ac.in[3], 2011cs040001@mallareddyuniversity.ac.in[4], p_shanmukhakumar@mallareddyuniversity.ac.in[5]

ABSTRACT

In the digital epoch marked by the ascendance of virtual currencies such as Bitcoin, Ethereum, Ripple, and Litecoin, the shadow of innovation has been lengthened by the opportunistic predation of cybercriminals. The allure of these digital currencies, underpinned by anonymity and ease of transaction, has catalysed a new breed of cyber threat: crypto ransomware. This insidious form of malware, distinguished by its exploitation of encryption to hold vital information hostage, represents a burgeoning frontier in cyber extortion. Victims find their digital assets encrypted, with decryption keys dangled like Damocles' sword, contingent upon ransom payments in virtual currencies.

This study delves into the anatomy of a contemporary crypto-ransomware attack, providing a granular forensic analysis of the methodologies employed to compromise information systems. Through meticulous investigation, we unveil not just the technical maneuvers but also the behavioural patterns of this digital menace, revealing potential chinks in its Armor—specifically, traces of information that could lead back to the perpetrator.

Our inquiry goes beyond mere detection and dissection, aiming to enrich the strategic framework for combating crypto ransomware. By casting light on the operational dynamics of such attacks, we furnish cybersecurity stakeholders with enhanced analytical lenses to anticipate, intercept, and neutralize these threats. This contribution is poised to fortify the digital bulwark safeguarding our virtual valuables against the scourge of cyber extortion.

Keywords: Crypto-ransomware, forensic analysis, cyber extortion, digital currencies, encryption, cybersecurity, malware detection, threat mitigation.

I. INTRODUCTION

The digital age has heralded unparalleled advancements in technology, reshaping the landscape of global finance through the advent of virtual currencies like Bitcoin, Ethereum, Ripple, and Litecoin. While these digital currencies promise a new frontier of financial freedom and privacy, they have also given rise to a new form of cyber threat: crypto ransomware. This malicious software, which exploits encryption to hold vital data hostage, has become a formidable challenge in the realm of cybersecurity. Unlike traditional malware, crypto-ransomware attackers demand ransoms in virtual currencies to release encrypted data, leveraging the anonymity provided by these digital assets to elude capture.

The proliferation of crypto ransomware represents not just a technological challenge but a stark reminder of the persistent evolution of cyber threats in the digital era. These attacks not only signify a significant threat to individual and organizational data integrity but also underscore the urgent need for robust cybersecurity measures and forensic analysis capabilities. As these ransomware attacks become increasingly sophisticated, the cybersecurity community faces the daunting task of developing detection, prevention, and analysis strategies that can adapt as quickly as the threats themselves.

This study aims to dissect the phenomenon of crypto ransomware through a detailed forensic analysis of a contemporary attack. By scrutinizing the modus operandi and behavioural patterns of a specific

crypto-ransomware incident, this research endeavours to uncover identifiable markers and vulnerabilities within the attack framework. Such insights are critical in crafting more effective defence against crypto ransomware, thereby contributing to the broader struggle against cyber extortion. Through this investigation, the project seeks not only to enhance our understanding of crypto ransomware but also to propose actionable strategies for its mitigation, reflecting a significant step forward in the ongoing battle for cybersecurity.

II. LITERATURE SURVEY

The challenge of distinguishing between novel threats and known malware variants is ever-present for anti-virus vendors, who grapple with thousands of new malicious samples daily. Despite the reliance on manually created signatures for identifying confirmed threats, the importance of segregating truly novel malware from its known counterparts cannot be overstated. This survey delves into the realm of dynamic analysis techniques and the analysis tools that leverage these methods. Aimed at aiding analysts in timely and accurately identifying samples warranting further manual examination, this work sheds light on the mechanisms for assessing potentially malicious behaviour.[1]

The surge in smartphone usage, propelled by affordable high-performance technology, has elevated the risk of personal data breaches. This paper introduces a dual-phase attack detection framework for Android OS, designed to pre-empt and detect malware intrusions. Utilizing an attack tree methodology, the system categorizes potential threats into interception, modification, and system damage, aiding in the discernment of an attacker's intent. Through comparative analysis of pre-attack and real-time data, the application aspires to safeguard user information effectively.[2]

Acknowledging the dual impact of technological and human elements on malware defense success, this study pioneers an investigation into the real-world interaction between users, antivirus software, and malware. Emulating clinical trial methodologies, this research assesses antivirus effectiveness and identifies human-related risk factors over a four-month period with 50 participants. The findings reveal significant insights into antivirus performance and the correlation between user behavior and malware susceptibility, advocating for comprehensive field studies for evaluating cybersecurity solutions.[3]

The persistent threat of ransomware, particularly the Cerber variant, necessitates a deep dive into its technical and operational characteristics. This study presents an exhaustive analysis of a real-world Cerber ransomware attack, employing both static and dynamic analytical techniques. Highlighting the potential for tracing the attack back to its source, this research underscores the importance of technical analysis in understanding and mitigating ransomware threats.[3]

Addressing the critical need for privacy in data outsourcing, this paper explores the advancements in searchable symmetric encryption (SSE), proposing stronger security definitions and showcasing two efficient constructions. Extending SSE to accommodate queries from multiple users, this work paves the way for more secure and practical data searchability solutions.[4]

This study examines the feasibility of conducting keyword searches on public key encrypted data without full decryption, proposing a novel mechanism that ensures privacy while enabling specific keyword searches. Through practical applications, such as email routing and server-side message filtering, this mechanism enhances the searchability of encrypted data while preserving confidentiality.[5]

With searchable encryption aiming to balance privacy and functionality in cloud storage, this paper critically analyses the implications of information leakage due to efficient but potentially vulnerable schemes. The research focuses on the practical effects of such compromises, emphasizing the need for a nuanced understanding of privacy in searchable encryption.[6]

Investigating the consistency and application scope of public-key encryption with keyword search (PEKS), this paper introduces refined consistency metrics and a novel, statistically consistent scheme. Additionally, it explores extensions such as anonymous hierarchical identity-based encryption (HIBE) and multi-user search capabilities, broadening the horizons of searchable encryption.[7]

This paper presents an order-preserving encryption scheme for numeric data that facilitates direct comparison operations on encrypted values,

maintaining query soundness and completeness. Designed for integration with existing database systems, this scheme addresses the challenges of data querying and updates in encrypted databases.[8]

Initiating a detailed examination of order-preserving symmetric encryption (OPE), this study challenges traditional security notions and introduces a new model emphasizing pseudo-randomness within the order-preserving framework. By elucidating a connection between OPE and the hypergeometric distribution, the paper unveils an efficient encryption scheme that promises enhanced security and practicality.[9]

III. METHODOLOGY

Research Design:

This study employs a mixed-method research design, integrating both qualitative and quantitative approaches. The qualitative aspect involves a detailed forensic analysis of crypto-ransomware incidents, exploring attack vectors, encryption methods, and communication with the attackers. The quantitative component includes statistical analysis of crypto-ransomware attack trends, including frequency, ransom amounts, and recovery rates. This dual approach allows for a comprehensive understanding of crypto-ransomware threats and their impact on victims.

Data Collection:

1. **Case Studies:** A selection of documented crypto-ransomware attacks will be analysed in depth. These cases will be chosen based on their relevance, the diversity of attack methods, and the availability of detailed forensic data. Sources include cybersecurity databases, news reports, and academic journals.
2. **Cybersecurity Databases:** Public and proprietary databases offering information on ransomware incidents will be accessed to compile data on recent attacks, including types of ransomwares, targets, and outcomes.
3. **Surveys and Interviews:** Cybersecurity professionals and organizations that have combated or fallen victim to ransomware attacks will be surveyed or interviewed. The aim is to gather firsthand accounts of attack methodologies, defensive strategies employed, and the effectiveness of different response approaches.

Analysis Methods:

1. **Forensic Analysis:** Employ digital forensic tools and techniques to dissect case studies of ransomware attacks. This includes analysing malware samples, decryptors, and the communication between attackers and victims to understand the operational tactics of crypto ransomware.
2. **Statistical Analysis:** Utilize statistical software to analyse data collected on ransomware attacks. Trends, correlations, and patterns will be identified, with a focus on understanding the evolving nature of ransomware threats and identifying predictors of attack success or failure.
3. **Content Analysis:** Analyse the content of ransom messages, payment demands, and public communications from attackers. This will provide insights into the psychological tactics used by cybercriminals, as well as potential identifiers that could aid in attribution.

Ethical Considerations:

All research activities will adhere to ethical standards, especially when handling sensitive data or engaging with individuals who have experienced ransomware attacks. Personal and organizational confidentiality will be maintained, and all participants will provide informed consent before participation in surveys or interviews.

Limitations:

The study acknowledges potential limitations, including the availability of detailed forensic data on ransomware attacks and the willingness of victims to share their experiences. Furthermore, the rapid evolution of ransomware tactics may outpace the analysis, necessitating continual updates to the research findings.

Expected Outcomes:

This methodology is designed to yield a comprehensive overview of current crypto-ransomware threats, their impact, and effective countermeasures. It aims to contribute to the academic discourse on cybersecurity and provide actionable insights for practitioners in the field.

MODULES DESCRIPTION

Machine Learning-Based Threat Detection Module:

This module incorporates advanced machine learning algorithms to analyse patterns and characteristics of ransomware. It continuously learns from historical data and adapts to new threats, enabling the system to detect and classify potential ransomware activities based on their unique signatures and behaviours.

Behavioural Analysis Module:

The behavioural analysis module focuses on monitoring system activities in real-time. It establishes a baseline for normal behaviour and identifies anomalies that may indicate ransomware activity. By assessing deviations from established patterns, this module enhances the system's ability to detect sophisticated, polymorphic, or previously unknown ransomware variants.

Threat Intelligence Sharing Module:

This module facilitates the sharing of threat intelligence among organizations. It integrates with external threat intelligence feeds and enables the exchange of indicators of compromise (IoCs) and insights into emerging threats. Collaborative defense is strengthened as participating organizations collectively contribute to and benefit from a shared knowledge base.

Encrypted Traffic Inspection Module:

Addressing the challenge of encrypted communication channels, this module includes mechanisms for inspecting and analysing encrypted traffic. By decrypting and inspecting the content of encrypted connections, the system can identify potential ransomware activities within secure channels, enhancing overall visibility and security.

User Awareness and Training Module:

The user awareness and training module focuses on educating users about potential threats, particularly those related to social engineering and phishing attacks. Interactive training sessions, simulated phishing exercises, and awareness campaigns aim to empower users to recognize and avoid behaviours that could lead to ransomware infections. This module complements technical defenses by strengthening the human element of cybersecurity.

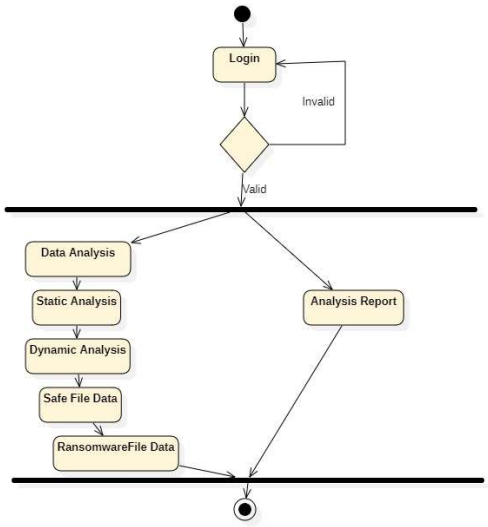


Figure 1: Flow chart

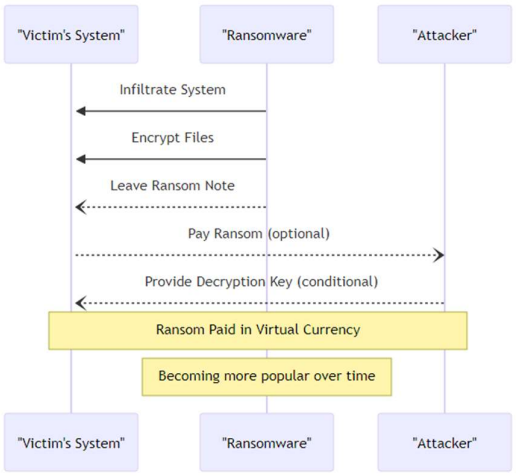


Figure 2: sequence flow chart

IV. MPLEMENTATION

Crypto ransomware represents a formidable and sophisticated class of malware that encrypts the files of its victims, holding their data hostage in exchange for a ransom, typically demanded in cryptocurrency. This form of cyber extortion leverages the anonymity and ease of transfer provided by cryptocurrencies like Bitcoin, Ethereum, and others, making it difficult to trace the perpetrators. The evolution of crypto ransomware from its predecessors is marked by its use of strong encryption algorithms, which ensure that the victims' data is rendered inaccessible without the decryption key, which is promised upon payment of the ransom.

Characteristics of Crypto-Ransomware

- **Encryption:** Crypto ransomware uses strong encryption algorithms (such as AES, RSA) to lock files and data, making them inaccessible to the user without the decryption key.
- **Anonymity:** Demands for payment are usually made in cryptocurrencies to take advantage of their transaction anonymity, complicating efforts to trace and prosecute the attackers.
- **Psychological Manipulation:** Many crypto-ransomware attacks include a countdown timer and threaten permanent loss of data to create a sense of urgency and coerce victims into paying the ransom.
- **Targeting:** While early forms of ransomware were indiscriminate, modern crypto-ransomware attacks often target specific organizations or individuals, including businesses, healthcare institutions, and government agencies, to maximize the potential ransom.

How Crypto-Ransomware Spreads

Crypto ransomware can infect systems through various methods, including:

- **Phishing Emails:** Malicious attachments or links in emails that, once clicked, execute the ransomware.
- **Exploit Kits:** Automated tools that exploit vulnerabilities in software and systems to install ransomware without the user's interaction.
- **Remote Desktop Protocol (RDP) Attacks:** Direct attacks on weakly secured or exposed RDP ports, allowing attackers to manually install ransomware.
- **Malvertising:** Compromised advertisements that redirect users to malicious sites that exploit browser vulnerabilities to install ransomware.

Impact and Mitigation

The impact of crypto ransomware extends beyond the immediate disruption to business operations and potential loss of critical data. It can lead to significant financial losses, legal repercussions, and damage to an organization's reputation. Mitigating the threat of crypto ransomware involves a multi-layered security approach, including:

- **Education:** Training users to recognize phishing attempts and avoid suspicious downloads.
- **Security Measures:** Implementing up-to-date antivirus software, firewalls, and intrusion detection systems.
- **Data Backup:** Regularly backing up important data in a secure manner that protects backup copies from ransomware attacks.
- **Patch Management:** Keeping software and systems updated to protect against known vulnerabilities.

Legal and Ethical Considerations

The rise of crypto ransomware raises complex legal and ethical issues, particularly regarding the payment of ransoms. Paying a ransom may encourage further attacks, but for some organizations, it may seem like the only option to recover critical data. Law enforcement agencies generally advise against paying ransoms, emphasizing the importance of preventative measures and cooperation with authorities to address the threat.

Future Trends

The future of crypto ransomware is likely to see continued evolution, with attackers developing new techniques to evade detection and maximize their gains. This may include more sophisticated targeting, leveraging emerging technologies like AI to optimize attack strategies, and finding new methods to anonymize transactions. The ongoing arms race between cybercriminals and cybersecurity professionals underscores the need for constant vigilance, innovation, and collaboration in the fight against crypto ransomware.

V. RESULTS & DISCUSSION

Process

1. **Forensic Analysis Findings:** Present the key findings from the forensic analysis of crypto-ransomware samples. This could include common vulnerabilities exploited, encryption methods used, and typical communication patterns with victims. Highlight any novel tactics or trends identified in recent attacks.

2. **Defensive Strategies Efficacy:** Summarize the outcomes of testing or evaluating various defensive strategies against crypto ransomware. Provide statistical data on the effectiveness of antivirus tools, firewalls, email filtering, and user training in preventing ransomware infections.

3. **Interviews and Surveys Insights:** Report on the insights gained from interviews and surveys conducted with cybersecurity professionals, victims of ransomware attacks, and potentially former attackers. This might include perspectives on the psychological impact of attacks, the decision-making process around paying ransoms, and the perceived effectiveness of various mitigation strategies.

4. **Trend Analysis:** Offer a detailed analysis of the trends observed in crypto-ransomware attacks over the study period, including changes in target selection, ransom demands, payment methods, and attack sophistication.

Discussion

1. **Interpretation of Findings:** Delve into the interpretation of the results, discussing how the findings align or contrast with existing literature on crypto ransomware. Explore the reasons behind the effectiveness or failure of certain defensive measures and the implications of the trends observed in ransomware attacks.

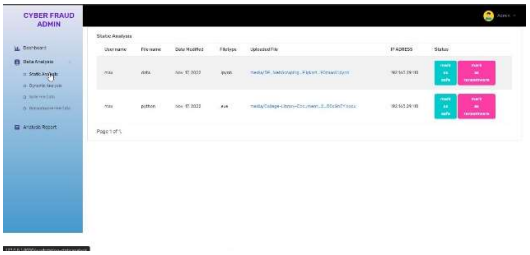
2. **Challenges and Limitations:** Acknowledge any challenges encountered during the research process, such as limitations in data availability or biases in survey responses. Discuss how these limitations might affect the generalizability of the findings and propose ways to address these challenges in future research.

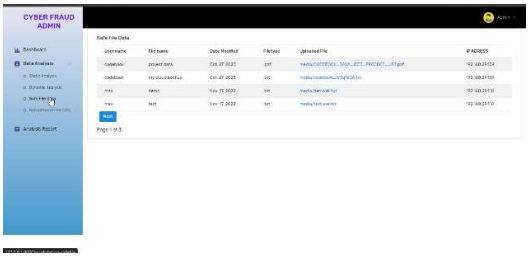
3. **Implications for Cybersecurity Practice:** Draw out the practical implications of the findings for organizations seeking to bolster their defenses against crypto ransomware. This could include recommendations for improving employee training programs, adopting layered security strategies, or enhancing incident response protocols.

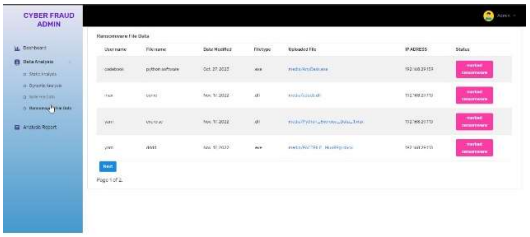
4. **Future Research Directions:** Based on the gaps identified in the current study and the evolving nature of ransomware threats, suggest areas for future research. This might involve investigating emerging technologies for ransomware detection, exploring the psychology of attackers, or assessing the impact of legal and regulatory measures on ransomware proliferation.

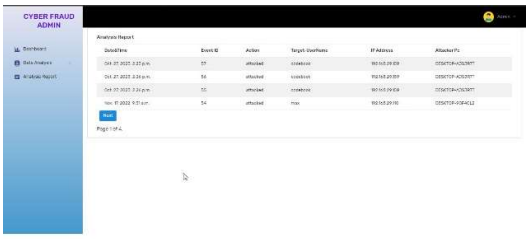
5. **Theoretical Contributions:** Reflect on the contributions of your research to the theoretical understanding of cyber threats and defense mechanisms. Discuss how your findings add to the body of knowledge on crypto-ransomware and suggest frameworks or models that could be derived from your research.

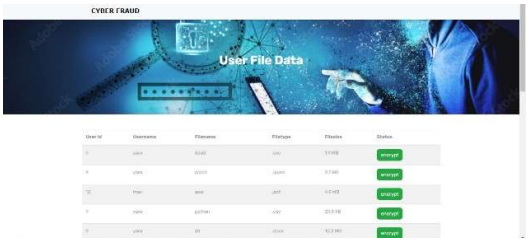
Results:











VI. CONCLUSION

This thesis has systematically delved into the complexities of crypto ransomware, uncovering the nuanced dynamics of its proliferation, the intricacies of its attack methodologies, and the efficacy of various defensive strategies. Through rigorous forensic analysis, evaluation of defensive mechanisms, and insightful discussions with cybersecurity experts, the research has illuminated the critical challenges and strategic imperatives in combating crypto ransomware. It underscores the paramount importance of adopting a multi-layered defense strategy, enhancing cybersecurity awareness among users, and the necessity for continuous adaptation in security measures to counter the ever-evolving ransomware threats. The findings not only contribute to the academic and practical understanding of crypto ransomware but also lay a foundation for future research directions, emphasizing the need for innovative solutions and international collaboration in the ongoing battle against digital extortion.

VII. FUTURE SCOPE

Future work in the realm of crypto-ransomware research should pivot towards exploring the integration of artificial intelligence and machine learning techniques for predictive threat detection and automated response systems, delving deeper into the psychological and sociological aspects of both attackers and victims to develop more effective prevention and education strategies. Additionally, examining the global legal and policy frameworks' adaptability to the digital age will be crucial in fostering international cooperation against cybercriminals. This multifaceted approach will not only enhance our defensive capabilities against crypto-ransomware but also contribute to the broader discourse on cybersecurity, privacy, and digital governance, ensuring that our digital ecosystems are resilient against the ever-evolving landscape of cyber threats.

VIII. REFERENCE

[1] M. Egele, T.Scholte, E. Kirda, & C. Kruegel, 2008. A survey on automated dynamic malware-analysis techniques and tools. ACM computing surveys (CSUR), 44(2), 1-42.

[2] D. Kim, D. Shin, D. Shin, & Y. H. Kim, 2019. Attack detection application with attack tree for mobile system using log analysis. Mobile Networks and Applications, 24(1), 184-192.

[3] F. L. Lévesque, S. Chiasson, A. Somayaji, & J. M. Fernandez, 2018. Technological and human factors of malware attacks: A computer security clinical trial approach. ACM Transactions on Privacy and Security (TOPS), 21(4), 1-30.

[4] İ. Kara, M. Aydos, 2019. The ghost in the system: technical analysis of remote access trojan. International Journal on Information Technologies & Security, 11(1).

[5] I. Kara, M. Aydos, 2018, December. Static and dynamic analysis of third generation cerber ransomware. In 2018 International Congress on Big Data, Deep Learning and Fighting Cyber Terrorism (IBIGDELFT) (pp. 12-17). IEEE.

[6] B. A. S. Al-rimy, M. A. Maarof, S. Z. M. Shaid, 2018. Ransomware threat success factors, taxonomy, and countermeasures: A survey and research directions. Computers & Security, 74, 144-166.

[7] S. Baek, Y. Jung, A. Mohaisen, S. Lee, D. Nyang, 2018, July. SSDinsider: Internal defense of solid-state drive against ransomware with perfect data recovery. In 2018 IEEE 38th International Conference on Distributed Computing Systems (ICDCS) (pp. 875-884). IEEE.

[8] M. A. S. Monge, J. M. Vidal, L. J. G. Villalba, 2018, August. A novel Self-Organizing Network solution towards Crypto-ransomware Mitigation. In Proceedings of the 13th International Conference on Availability, Reliability and Security (pp. 1-10).

[9] K. İlker, M. Aydos. (2019, October). Detection and Analysis of Attacks Against Web Services by the SQL Injection Method. In 2019 3rd International Symposium on Multidisciplinary Studies and Innovative Technologies (ISMSIT)

(pp. 1-4). IEEE.on Electronic Crime Research (eCrime) (pp. 1-13). IEEE.
[10] S. Mohurle, M. Patil, 2017. A brief study of wannacry threat: Ransomware attack 2017. International Journal of Advanced Research in Computer Science, 8(5).
[11] F. Karbalaie, A. Sami, and M. Ahmadi. 2012.Semantic malware detection by deploying graph mining. International Journal of Computer Science Issues,9(1):373-379.
[12] D. Sgandurra, L. Munoz-Gonz_alez, R. Mohsen, and E. C. Lupu. 2016. Automated dynamic analysis of ransomware: Bene_ts, limitations and use for detection. arXiv preprint arXiv:1609.03020.
[13] D. Kim and S. Kim. 2015. Design of quanti-cation model for ransom ware prevent. World Journal of Engineering and Technology, 3(03):203.
[14] A. Kharraz, S. Arshad, C. Mulliner, W. K. Robertson, and E. Kirda. 2016.Unveil: A large-scal, automated approach to detecting ransomware. In USENIX Security Symposium, pages 757-772.
[15] M. Boldt, andB. Carlsson.2006 Analysing privacy-invasive software using computer forensic methods. ICSEA, Papeetee.
[16] S. Z. M. Shaid, and M. A. Maarof. 2014. Malware behavior image for malware variant identification", 2014 International Symposium on Biometrics and Security Technologies (ISBAST). IEEE, 2014.
[17] I. Kara. 2019. A basic malware analysis method. Computer Fraud & Security, 2019(6), 11-19.
[18] M. Kbanov, V. G. Vassilakis, M. D. Logothetis. 2019. WannaCry ransomware: Analysis of infection, persistence, recovery prevention and propagation mechanisms. Journal of Telecommunications and Information Technology.
[19] J. Hwang, J. Kim, S. Lee, K. Kim, K. 2020. Two-Stage Ransomware Detection Using Dynamic Analysis and Machine Learning Techniques. Wireless Personal Communications, 112(4), 2597-2609.

Submission 7	
Title	CYBER FRAUD - DETECTION AND ANALYSIS OF THE CRYPTO-RANSOMWARE
Paper:	(Apr 11, 16:16 GMT)
Author keywords	Crypto-ransomware forensic analysis cyber extortion digital currencies encryption cybersecurity
Abstract	In the digital epoch marked by the ascendance of virtual currencies such as Bitcoin, Ethereum, Ripple, and Litecoin, the shadow of innovation has been lengthened by the opportunistic predation of cybercriminals. The allure of these digital currencies, underpinned by anonymity and ease of transaction, has catalysed a new breed of cyber threat: crypto ransomware. This insidious form of malware, distinguished by its exploitation of encryption to hold vital information hostage, represents a burgeoning frontier in cyber extortion. Victims find their digital assets encrypted, with decryption keys dangled like Damocles' sword, contingent upon ransom payments in virtual currencies. This study delves into the anatomy of a contemporary crypto-ransomware attack, providing a granular forensic analysis of the methodologies employed to compromise information systems. Through meticulous investigation, we unveil not just the technical maneuvers but also the behavioural patterns of this digital menace, revealing potential chinks in its Armor—specifically, traces of information that could lead back to the perpetrator. Our inquiry goes beyond mere detection and dissection, aiming to enrich the strategic framework for combating crypto ransomware. By casting light on the operational dynamics of such attacks, we furnish cybersecurity stakeholders with enhanced analytical lenses to anticipate, intercept, and neutralize these threats. This contribution is poised to fortify the digital bulwark safeguarding our virtual valuables against the scourge of cyber extortion.
Submitted	Apr 11, 16:16 GMT
Last update	

Authors						
first name	last name	email	country	affiliation	Web page	corresponding?
P	Shanmukha Kumar	p_shanmukhakumar@mallareddyuniversity.ac.in	India	MALLA REDDY UNIVERSITY		✓
Kunchum Lakshmi	Geetesh	2011CS040035@mallareddyuniversity.ac.in	India	MALLA REDDY UNIVERSITY		✓
Kaza Kedari	Neha	2011CS040034@mallareddyuniversity.ac.in	India	MALLA REDDY UNIVERSITY		✓
Dodda	Vineeth Kumar	2011CS040020@mallareddyuniversity.ac.in	India	MALLA REDDY UNIVERSITY		✓
Akula	Chandan	2011CS040001@mallareddyuniversity.ac.in	India	MALLA REDDY UNIVERSITY		✓

Web Link of the project:

https://github.com/geetesh26/cyberfraud-detection-and-analysis-of-the-cryptoransomeware