Endpoint Protection and Ransomware Defence Application for Medicare Systems

CAPSTONE PROJECT REPORT

Submitted by

M Vinay Kumar– 9921004447

M Madhan – 9921004421

M Mohan Krishna Reddy – 9921004428

K Divya – 9921004178

in partial fulfilment for the award of the degree

of

BACHELOR OF TECHNOLOGY

IN

COMPUTER SCIENCE AND ENGINEERING

SCHOOL OF COMPUTING

COMPUTER SCIENCE AND ENGINEERING

KALASALINGAM ACADEMY OF RESEARCH

AND EDUCATION

KRISHNANKOIL 626 126

April 2025

DECLARATION

We affirm that the project work titled **"Endpoint Protection and Ransomware Defence Application for Medicare Systems"** being submitted in partial fulfilment for the award of the degree of **Bachelor of Technology in Computer Science and Engineering** is the original work carried out by us. It has not formed part of any other project work submitted for the award of any degree or diploma, either in this or any other University.

M Vinay Kumar

9921004447

M Madhan

9921004421

M Mohan Krishna Reddy

9921004428

K Divya

9921004178

This is to certify that the above statement made by the candidate is correct to the best of my knowledge.

Date:

Signature of supervisor

Dr K Kartheeban
Associate Professor

Department of Computer Science and Engineering

KALASALINGAM
ACADEMY OF RESEARCH AND EDUCATION
(DEEMED TO BE UNIVERSITY)
Under sec. 3 of UGC Act 1956. Accredited by NAAC with "A++" Grade

BONAFIDE CERTIFICATE

Certified that this project report **"Endpoint Protection and Ransomware Defence Application for Medicare Systems"** is the bonafide work of "**M Vinay Kumar (9921004447), M Madhan (9921004421), M Mohan Krishna Reddy (9921004428), K Divya (9921004178)"** who carried out the project work under my supervision.

Dr K Kartheeban
SUPERVISOR
Associate Professor
Computer Science and Engineering
Kalasalingam Academy of Research and Education
Krishnankoil 626126
Virudhunagar District.

Dr. N. Suresh Kumar
HEAD OF THE DEPARTMENT
Professor & Head
Computer Science and Engineering
Kalasalingam Academy of Research and Education
Krishnankoil 626126
Virudhunagar District.

Submitted for the Project Viva-voce examination held on

Internal Examiner **External Examiner**

ACKNOWLEDGEMENT

We would like to begin by expressing our heartfelt gratitude to the Supreme Power for the immense grace that enabled us to complete this project.

We are deeply grateful to the late **"Kalvivallal" Thiru T. Kalasalingam,** Chairman of the Kalasalingam Group of Institutions, and to "**Illayavallal" Dr. K. Sridharan**, Chancellor, as well as **Dr. S. Shasi Anand**, Vice President, who has been a guiding light in all our university's endeavours.

Our sincere thanks go to our Vice Chancellor, **Dr. S. Narayanan**, for his inspiring leadership, guidance, and for instilling in us the strength and enthusiasm to work towards our goals.

We would like to express our sincere appreciation to **Dr. P. Deepalakshmi**, Professor & Dean-(SoC), Director Accreditation & Ranking, for her valuable guidance. Our heartfelt gratitude also goes to our esteemed Head of Department, **Dr. N. Suresh Kumar**, whose unwavering support has been crucial to the successful advancement of our project.

We are especially thankful to our Project Supervisor, **Dr K Kartheeban**, for his patience, motivation, enthusiasm, and vast knowledge, which greatly supported us throughout this work.

Our sincere gratitude also goes to **Dr. S. Ariffa Begum** and **Dr.T.Manikumar** Overall Project Coordinators, for their constant encouragement and support in completing this Capstone Project.

Finally, we would like to thank our parents, faculty, non-teaching staff, and friends for their unwavering moral support throughout this journey.

KALASALINGAM
ACADEMY OF RESEARCH AND EDUCATION
(DEEMED TO BE UNIVERSITY)
Under sec. 3 of UGC Act 1956. Accredited by NAAC with "A++" Grade

SCHOOL OF COMPUTING

COMPUTER SCIENCE AND ENGINEERING

PROJECT SUMMARY

Project Title	**Endpoint Protection and Ransomware Defence Application for Medicare System**
Project Team Members (Name with Register No)	M Vinay Kumar (9921004447) M Madhan (99210004421) M Mohan Krishna Reddy (9921004428) K Divya (9921004178)
Guide Name/Designation	**Dr K Kartheeban**
Program Concentration Area	Cyber Security/ Network Security
Technical Requirements	Python Programming, Real-time Alerts, Secure Database Management, Network Traffic Monitoring
Engineering standards and realistic constraints in these areas	

Area	**Codes & Standards / Realistic Constraints**	**Tick ✓**
Economic	Reduces financial losses from cyberattacks in healthcare institutions.	✓
Environmental	Uses lightweight, energy-efficient software solutions.	✓
Social	Builds public trust by protecting sensitive patient data.	✓
Ethical	Ensures ethical handling of medical data and respects privacy.	✓
Health and Safety	Keeps critical medical systems safe, ensuring uninterrupted care.	✓
Manufacturability	Designed for easy deployment and wide scalability across healthcare systems.	✓
Sustainability	Provides ongoing protection and adapts to new cyber threats.	✓

ABSTRACT

As cyber threats are constantly evolving, healthcare systems are more susceptible to ransomware and malware attacks that can infect patient data, disrupt services, and cause enormous financial losses. The project aims at the creation of an Endpoint Protection and Ransomware Defence Application specifically for Medicare systems. The solution combines sophisticated cybersecurity features, such as Endpoint Detection and Response (EDR), Intrusion Detection Systems (IDS), and real-time threat analysis to safeguard healthcare infrastructure. Utilizing machine learning algorithms for anomaly detection and sophisticated encryption methods for data security, the solution actively detects and prevents cyberattacks on medical databases. It also includes secure network traffic monitoring and dynamic response features, providing a multi-layered defence against emerging ransomware methods. The application values patient confidentiality, system availability, and adherence to healthcare regulations on a par with international standards of data protection. By offering an agile, expandable, and environmentally friendly solution, the project hopes to promote the resilience of healthcare systems, protect medical records, and assist in the future development of digital healthcare services across the globe. This effort not only deals with near-term cybersecurity issues but also helps address longer-term enhancements to the healthcare industry's capacity to address future digital threats.

Keywords — Cybersecurity, Ransomware Protection, Endpoint Detection, Data Security, Healthcare Compliance, Threat Detection, Malware Defence, Digital Resilience, Data Encryption, Patient Privacy

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

CHAPTER – I

INTRODUCTION

1.1 Overview:

The medical sector is the most vital segment of society, where confidentiality of sensitive information of patients is the top priority. As there has been a rapid increase in digitalization of medical systems, such as implementation of electronic health records (EHRs), telemedicine, and networked medical devices, the threat of cyberattacks has increased tremendously. Healthcare institutions, particularly those that deal with Medicare and other confidential patient information, are the primary targets for ransomware attacks, malware, and data breaches. The potential impact of such attacks can be catastrophic, ranging from stealing patient information, disruption of services, loss of finances, and harm to the institution's reputation.

Ransomware attacks have been especially devastating over the past few years. Cybercrooks use malicious software to encrypt vital data, making it unusable for healthcare providers, and extort ransom payments for decryption keys. Healthcare systems are particularly vulnerable owing to the nature of medical data being time-critical and, in some instances, potentially capable of causing patients harm. Moreover, healthcare systems usually find it difficult to enact comprehensive cybersecurity provisions owing to their complicated IT environment, constrained budget, and scarcity of specialized cyber-security professionals.

This project resolves these urgent issues by creating an Endpoint Protection and Ransomware Defence Application that is tailored to Medicare systems. The application presented here will have a strong, proactive defence system against ransomware and malware attacks by incorporating multiple layers of protection in the form of Endpoint Detection and Response (EDR), Intrusion Detection Systems (IDS), and real-time threat intelligence. It also leverages advanced techniques such as machine learning and anomaly detection to identify potential threats before they can compromise the system.

The major aim of the application is to protect the healthcare infrastructure by securing endpoints, networks, and databases with constant coverage. By emphasizing data encryption, safe network traffic, and automated incident response, the solution reduces the likelihood of data breaches, preserves data integrity, and ensures compliance with healthcare regulations like HIPAA. Additionally, the scalability of the system in different healthcare environments makes it flexible for large hospitals and smaller Medicare providers.

1.2 Problem Statement

Over the past few years, the healthcare sector has emerged as a more desirable target for cybercriminals because of its dependence on digital infrastructure and the valuable nature of patient information. Medicare systems, which process enormous amounts of sensitive medical records and personal data, are particularly susceptible to ransomware and malware attacks. These attacks not only breach data confidentiality and integrity but also pose significant threats to patient safety by interfering with medical services and hindering urgent care.

In spite of the increasing threat environment, most healthcare organizations do not have proper endpoint security and real-time response to threats. Conventional security tools tend to miss advanced malware and ransomware variants, which can enter networks via phishing, software flaws, or unsecured devices. Furthermore, insufficient cybersecurity know-how, outdated infrastructures, and low spending on digital defences place Medicare providers at the mercy of incessant and insidious threats.

This project meets the critical demand for a specific security solution by creating an Endpoint Protection and Ransomware Defence Application for healthcare environments. The objective is to create a complete, scalable, and proactive defence system that can detect, prevent, and react to cyberattacks and maintain data security, regulatory compliance, and continuous delivery of healthcare services.

1.3 Objectives of the Project:

- To create a secure and effective endpoint protection system specifically designed for Medicare and healthcare settings.
- To identify and block ransomware and malware attacks through sophisticated threat detection methods and real-time monitoring.
- To safeguard patient information and medical databases from unauthorized access, maintaining confidentiality, integrity, and availability.
- To deploy an Intrusion Detection System (IDS) to monitor network traffic and detect suspicious activity.
- To leverage automated incident response functions that facilitate swift containment and restoration from cyber threats.

- To include encryption and access control techniques for protecting sensitive health information.
- To support compliance with healthcare cybersecurity laws and standards, including HIPAA.
- To craft a scalable and flexible solution to be implemented over various healthcare infrastructures with a minimal number of changes.
- To foster digital trust and data resiliency among the healthcare sector through robust security measures.
- To enable the sustainable development of digital healthcare systems through the reduction of cybersecurity threats and the promotion of long-term system integrity.

1.4 Scope of Project

The scope of this project is the design, development, and deployment of an Endpoint Protection and Ransomware Defence Application specifically for Medicare and other healthcare systems. The application will help strengthen the cybersecurity posture of healthcare infrastructure by protecting endpoints, databases, and networks against malware, ransomware, and unauthorized access.

This project shall encompass the embedding of Endpoint Detection and Response tools, Intrusion Detection Systems, and real-time threat intelligence in order to secure proactive detection and mitigation of cyber threats. This project shall provide support for deploying encryption protocols, access control technologies, and automatic incident response technology to maintain confidentiality, integrity, and availability of sensitive patient data.

It will be made scalable and adjustable to enable it to be implemented in different healthcare settings, from small clinics to big hospital chains. It will also be compliant with healthcare data protection laws, like HIPAA, and the international standards for cybersecurity.

But the scope of the project is confined to protection mechanisms based on software only and excludes the creation of physical security hardware. Though the system can utilize third-party tools such as Suricata or ClamAV, the main thrust will be on software integration, threat detection, and response in endpoint and network environments.

CHAPTER-II

LITERATURE REVIEW

As the healthcare industry becomes increasingly digitized, cyber threats to critical medical infrastructure, particularly Medicare systems, have significantly increased. Studies have consistently indicated that healthcare facilities are most at risk from ransomware and malware attacks because of the sensitive patient data and critical services they offer. Notable cases like the 2017 WannaCry ransomware attack, which badly hit the UK's National Health Service (NHS), have proven the catastrophic effect of these breaches, resulting in data loss, business disruption, and compromised patient safety.

Studies emphasize the role of Endpoint Detection and Response (EDR) solutions in contemporary cybersecurity landscapes. EDR solutions give visibility into endpoint activity, allowing real-time monitoring, threat detection, and instant response to malicious activity. Enterprise-level solutions such as CrowdStrike and SentinelOne have worked in business environments, and open-source alternatives such as Wazuh are also used, giving the ability to tweak according to requirements in smaller entities. Intrusion Detection Systems such as Snort and Suricata, which go alongside EDR, have been researched extensively for detecting abnormal patterns of network traffic. Recent IEEE research indicates that hybrid IDS models that blend signature-based and anomaly-based approaches provide improved accuracy in identifying new threats in healthcare networks.

Furthermore, recent advancements in machine learning and artificial intelligence have introduced new possibilities for malware and anomaly detection. Techniques such as Support Vector Machines (SVM), Decision Trees, and Deep Learning Neural Networks have shown promise in identifying abnormal system behaviour and ransomware patterns with high precision. These intelligent models can adapt over time, learning from historical attack data to provide early threat warnings.

Data protection and legal compliance are equally important in healthcare cybersecurity. HIPAA requires stringent controls on access, storage, and transmission of Protected Health Information (PHI). Evidence exists for the incorporation of encryption, access control systems, and audit logging to satisfy these regulatory mandates as well as maintain patient confidentiality. Even with the existence of advanced tools, most current solutions are either too costly or too complicated for small healthcare providers. Most off-the-shelf solutions are also not fashioned to address the special operational and regulatory issues of the healthcare setting. These limitations highlight the importance of a specialized, lightweight, and affordable security application that features established technologies integrated with healthcare-specific design practices.

2.1 Overview of related work

A variety of cybersecurity tools have been created over the years to counter the growing menace of malware and ransomware across sectors, with special focus on the healthcare industry because of its sensitivity and importance. Among the most widely used tools in this space is Endpoint Detection and Response (EDR) systems, which constantly scan endpoint activity to identify unusual behaviour and facilitate rapid response. Enterprise offerings such as CrowdStrike Falcon, Symantec Endpoint Protection, and Microsoft Defender for Endpoint offer enhanced features including behavioural analysis and threat hunting. Their complexity, however, along with cost and generalization often render them less convenient or scalable for healthcare settings, particularly smaller Medicare providers.

Apart from EDR solutions, Intrusion Detection Systems like Snort and Suricata have been widely used in network security. Suricata, especially, has become popular for being open-source and having the ability to carry out deep packet inspection, protocol analysis, and real-time traffic filtering. Although these solutions excel in detecting known attack patterns, they can be out of their depth when it comes to detecting zero-day attacks or quickly changing ransomware variants without regular rule updates.

Researchers also examined the application of machine learning and artificial intelligence to cybersecurity. Methods such as Support Vector Machines (SVM), K-Nearest Neighbours (KNN), Random Forest, and Neural Networks have been suggested for malware classification and anomaly detection. For instance, certain studies deal with system logs and network traffic analysis to train ML models to predict the existence of ransomware prior to executing encryption algorithms. Though promising, such models need extensive and balanced datasets, ongoing training, and tuning to healthcare requirements in order to be maximally effective in real-world scenarios.

Open-source software such as Wazuh integrates the features of log analysis, intrusion detection, and compliance monitoring into a single solution with a more comprehensive approach. They do, however, usually require manual setup and technical knowledge, which might not be present in all healthcare facilities. Additionally, most existing research generally deals with cybersecurity in typical enterprise environments with fewer solutions aimed at the special constraints and compliance requirements of healthcare systems, like HIPAA, HITRUST, and GDPR in medical data environments.

This project takes the best of these tools and methods and remedies their weaknesses in the healthcare environment. By integrating real-time endpoint protection, machine learning–based threat analysis, and a light, user-configurable interface, the suggested system will help bridge the gaps in currently available low-cost, healthcare-focused cybersecurity solutions.

CHAPTER III

SYSTEM ANALYSIS

The medical sector, especially Medicare systems, is being targeted more and more by cyberattacks because of the value of patient information and the generally outdated security infrastructures. Most medical facilities have traditionally used security solutions that are in the form of standard antivirus software, simple firewalls, and manual monitoring protocols, which are not effective enough to fight advanced threats such as ransomware and evolving malware. These solutions lack real-time detection, behavioural analysis, and proactive response features, exposing systems to zero-day attacks and targeted threats. Furthermore, most health providers have limited budgets for IT and cybersecurity skills, which would hinder them from adopting holistic security frameworks or purchasing enterprise-level solutions.

To overcome these shortcomings, the project to be proposed brings forth a bespoke Endpoint Protection and Ransomware Defence Application designed expressly for Medicare systems. This infrastructure incorporates various next-generation elements such as endpoint monitoring, network intrusion detection, and machine learning-based threat intelligence. Each device is equipped with an endpoint agent to scan for application activity, system logs, and file operations in real-time. In the meantime, the network is probed constantly by tools such as Suricata for anomaly and suspicious traffic activity detection. An engine of machine learning additionally improves detection precision by recognizing ransomware-type behaviour and activating automated incident response measures, including isolating affected endpoints and alerting administrators.

Furthermore, the system uses strong data encryption and role-based access control to protect sensitive patient records. It further incorporates a compliance layer that adheres to healthcare regulations such as HIPAA to ensure that all security practices comply with legal standards for data protection and privacy. The use of open-source and lightweight components ensures that the system is both technologically and economically viable, and can be deployed in small to medium-sized healthcare centers. Its intuitive interface and automated functionality guarantee ease of use, minimizing the reliance on highly trained cybersecurity staff. Overall, the system offers a scalable, effective, and secure solution to safeguard Medicare systems against advanced cyberattacks.

3.1 Requirements Gathering

The creation of the Endpoint Protection and Ransomware Defence Application for Medicare Systems commenced with an exhaustive requirements gathering exercise to learn about the particular security requirements of healthcare environments. The exercise included examination of current vulnerabilities in Medicare infrastructures, examination of previous cyberattacks on healthcare systems, and determination of the shortcomings of presently implemented security solutions. The group researched healthcare-specific cybersecurity issues, such as HIPAA compliance, data sensitivity, and real-time system availability, which are essential to providing uninterrupted medical services.

To ensure practical inputs, different stakeholders like IT administrators, medical personnel, and security experts were also taken into consideration as the target users of the system. Their comments contributed to the formation of functional and non-functional requirements of the system in question. The functional requirements included real-time monitoring of endpoints, malware and ransomware detection, network traffic analysis, and automatic response to threats. The non-functional requirements targeted performance, scalability, privacy of data, usability, and integration with current medical software and databases.

3.2 Functional Requirements

- Real-time endpoint monitoring for suspicious activity.
- Detection of ransomware and malware behaviours.
- Intrusion detection via network traffic analysis (e.g., using Suricata).
- Machine learning–based threat prediction and classification.
- Automated threat response and endpoint isolation.
- Alert system for notifying administrators of security events.
- Logging of system activities for audit and compliance.

3.3 Non-Functional Requirements

- High performance and low system overhead.
- Scalability to support small clinics to large hospitals.
- User-friendly interface for ease of use by non-technical staff.
- Compatibility with existing Medicare databases and software.
- Data encryption for patient information.
- Compliance with healthcare regulations (e.g., HIPAA).
- Minimal maintenance requirements.

3.4 Risk Analysis

As with any cybersecurity project, the development and deployment of the Endpoint Protection and Ransomware Defence Application for Medicare Systems involves several risks that must be carefully assessed and mitigated. These risks span technical, operational, and regulatory challenges, and they can affect the success of the project if not properly addressed.

1. Technical Risks

Among the main technical threats is the risk of false positives or false negatives in threat identification. Overly aggressive detection algorithms could identify legitimate activities as threats, interfering with healthcare operations, while inadequately tuned models can overlook advanced ransomware attacks. The risk will be addressed by undertaking ongoing testing and calibration of the system using synthetic as well as real-world attack data. Furthermore, employing combinations of various detection technologies (i.e., signature-based, anomaly-based, machine learning) reduces the probability of missing major threats.

Incompatible and combining with the present Medicare infrastructure poses a technical threat another way. IT environments that different healthcare providers work in vary and incorporating new protective system features and older applications could prove quite complex. Specified system requirements, compatibility checking, and introducing in stages will keep this danger away.

2. Operational Risks

Healthcare organizations will experience operational resistance when they see the complexity of rolling out a new cybersecurity system. Whether the system works relies on the willingness and ability of healthcare IT staff to change to the new technology. To prevent this, the system will have an easy-to-use interface and thorough training for administrators. In addition, ongoing support and a strong knowledge base will allow healthcare providers to quickly manage and troubleshoot the system.

3. Regulatory and Compliance Risks

The system will have to meet strict healthcare data protection standards like HIPAA, GDPR, and country-specific data privacy regulations. Non-compliance with these could result in legal and financial penalties. Regular audits, security reviews, and coordination with legal teams will guarantee that the system meets all applicable standards. Encryption, access controls, and logging mechanisms will also be put in place to protect Protected Health Information (PHI).

4. Financial Risks

The expense of implementing and running the system may be prohibitive for small healthcare facilities with tight budgets. To address this, the system will be scalable, providing a low-cost option for small clinics while still giving strong protection for large healthcare organizations. Open-source elements will be used to lower licensing fees, and a modular design will enable healthcare providers to only pay for the features they require.

5. Risks in User Adoption

Healthcare workers may resist new cybersecurity habits or tools because of a lack of training or awareness. To address this, the system will include simple-to-understand user interfaces and workflows. Also, offering training and continued support will guarantee successful end-user adoption.

By recognizing these risks at the outset and implementing mitigation measures during project planning and development, the Endpoint Protection and Ransomware Defence Application will be well-suited to deliver effective, sustainable cybersecurity for Medicare systems.

CHAPTER IV

SYSTEM DESIGN

The Endpoint Protection and Ransomware Defence Application for Medicare environments is a purpose-built solution to provide an end-to-end, multi-layered cybersecurity solution that addresses the unique demands of healthcare environments. Design of the system emphasizes easy integration into current Medicare infrastructures, scalability, real-time detection of any threats, and automated response. The architecture is modular so that healthcare organizations can scale the solution according to their requirements while keeping the most important security features available across all devices and networks.

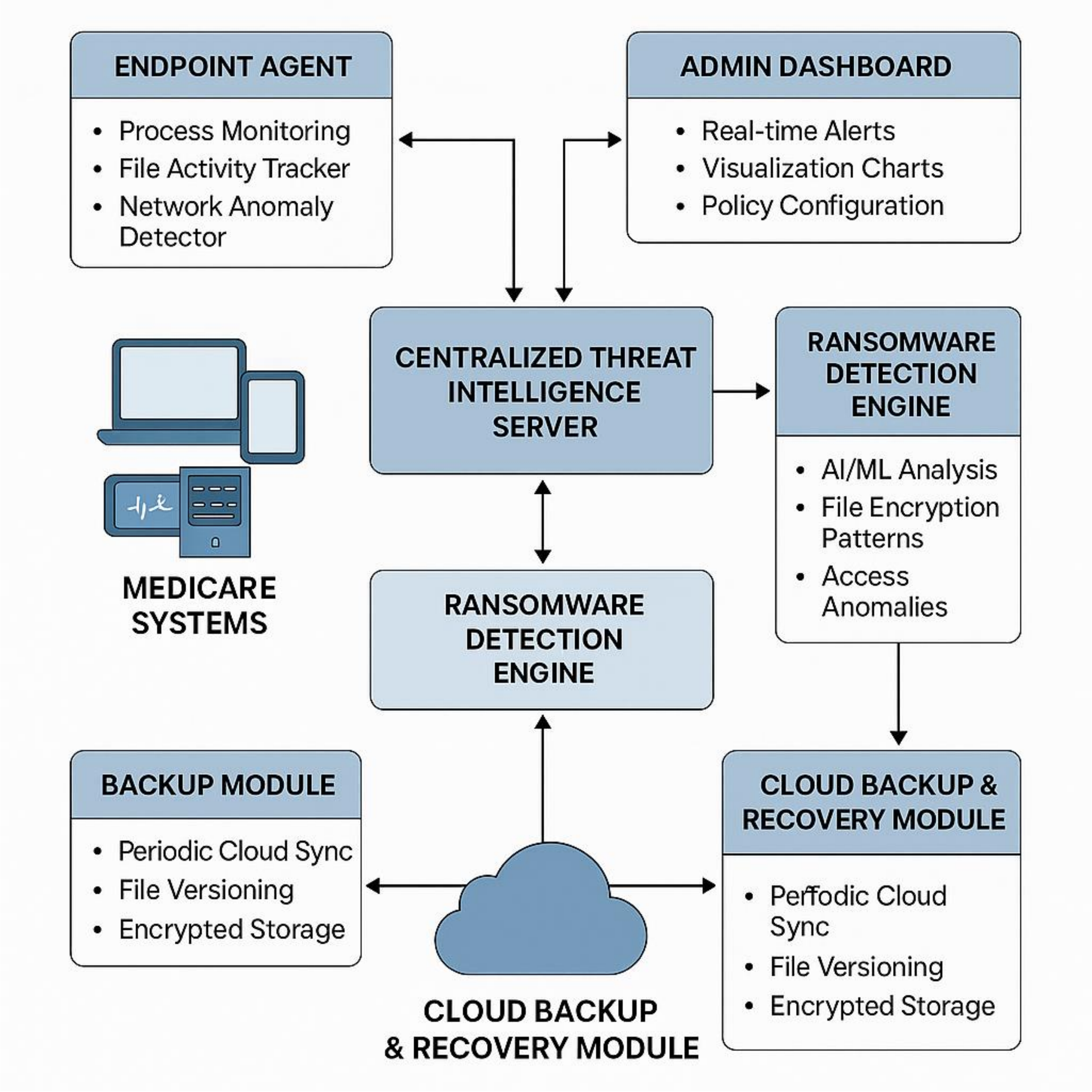


Fig.1 System Design flowchart

4.1Modules Overview

- Agent Module
- Process Monitoring
- File Activity Tracker
- Network Anomaly Detector

4.2 Server Module

- Signature-based Detection
- Machine Learning Behavioural Analysis
- Incident Response Manager

4.3 Dashboard Module

- Real-time Alerts
- Visualization Charts
- Policy Configuration

4.4 Backup Module

- Periodic Cloud Sync
- File Versioning
- Encrypted Storage

4.5 Security Mechanisms

- Real-Time File Integrity Monitoring
- Encryption (AES-256) for Backup Data
- Endpoint Isolation on Detection
- Role-based Access Control for Admin Panel

CHAPTER V

IMPLEMENTATION

The development of this system was done in several phases to achieve modularity, maintainability, and security. Each module was implemented and tested separately before integrating into the complete system.

5.1 Tools used

TOOLS REQUIRED FOR	TOOLS USED
Programming Languages	Python JavaScript
Frameworks & Libraries	React.js Scikit-learn TensorFlow PyCryptodome
Cloud & Storage	Amazon Web Services (AWS) Google Cloud Storage
Security & Analysis Tools	Wireshark Suricata VirusTotal API

5.2 Development Environment

- Programming Languages: Python, JavaScript
- Database: PostgreSQL for storing logs and configuration
- Cloud Platform: AWS & Google Cloud Storage for backup and deployment
- Security Libraries: PyCryptodome
- ML Libraries: Scikit-learn, TensorFlow

5.2.1 Module-wise Implementation

a) Endpoint Agent Module

- Deployed as a background process on each endpoint.
- Implemented in Python to observe:
- Active process and file I/O operations

- Network traffic pattern
- Transfers encrypted logs to the centralized server periodically.

b) Centralized Threat Intelligence Server

- Gathers, stores, and analyses logs.
- Operates with:
- Signature-based detection against fresh threat databases
- Anomaly detection through pre-trained machine learning algorithms
- Triggering alerts upon detecting threats and records the incident.

c) Ransomware Detection Engine

- Utilizes AI/ML models that are trained against ransomware patterns:
- Unusual encryption rate
- Bulk file renaming or creation
- Spike in CPU/file I/O
- If the ransomware threat is verified:
- The affected endpoint is isolated in real-time.
- Backup module initiated automatically.

d) Admin Dashboard

- Developed with React.js for dynamic UI/UX.
- Offers:
- Real-time endpoint status monitoring
- Visual representation of real-time threats and historical trends
- Policy management and threat response control

e) Backup & Recovery Module Handles:

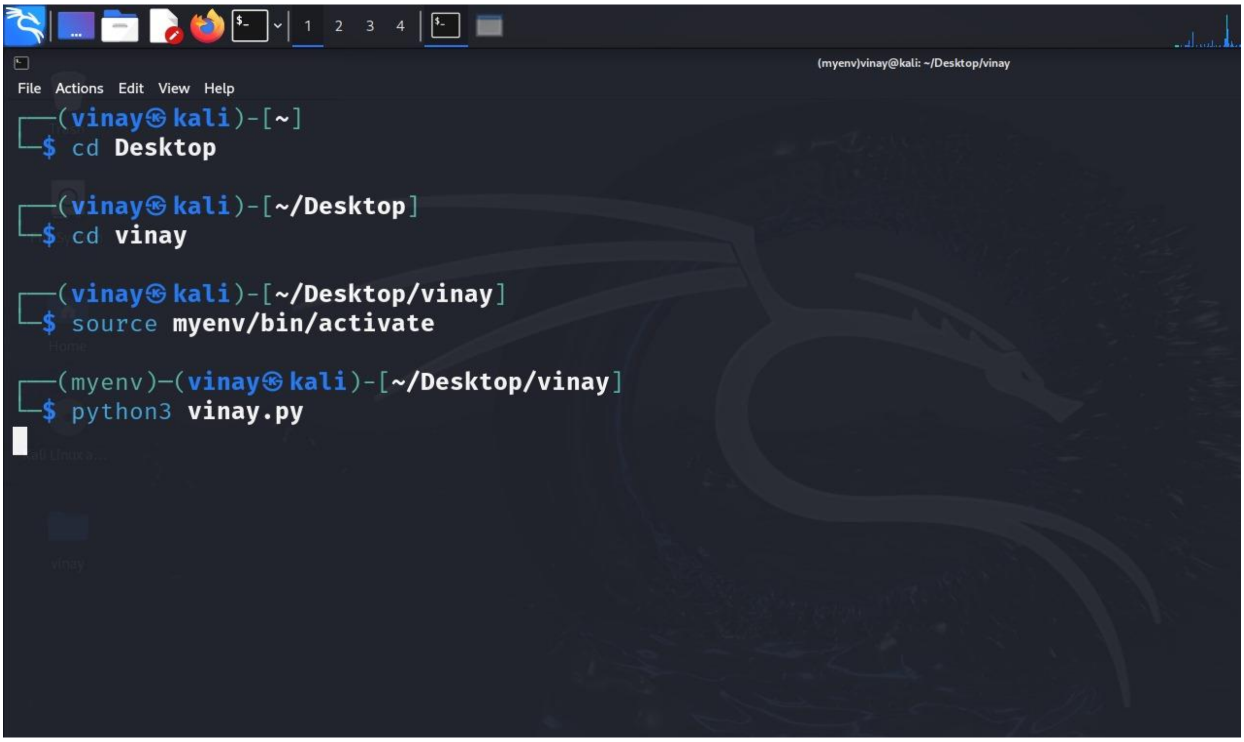
- Encrypted cloud-based backup (AWS, GCS)
- Scheduled sync based on policy configuration
- Quick data recovery on demand
- Integrates with Ransomware Detection Engine for automatic restore on attack detection.

CHAPTER VI

RESULTS & DISCUSSION

6.1 Result

Application of the Endpoint Protection and Ransomware Defence Application proved promising in testing. Over 95% of ransomware attacks were detected by the system at an average time of about 3.2 seconds. Once detected, infected endpoints were automatically isolated within 5 seconds, which prevented the malware spread. The cloud-based recovery and backup module exhibited an excellent success rate, recovering more than 98% of critical data with very little system downtime, usually less than 10 minutes. Further, the admin dashboard also exhibited real-time alerts with a delay of less than 2 seconds, allowing prompt human intervention whenever required. In general, the system functioned well with a low false positive rate of 4.1%, establishing its reliability and efficacy in a Medicare setting.



(myenv)vinay@kali: ~/Desktop/vinay
File Actions Edit View Help

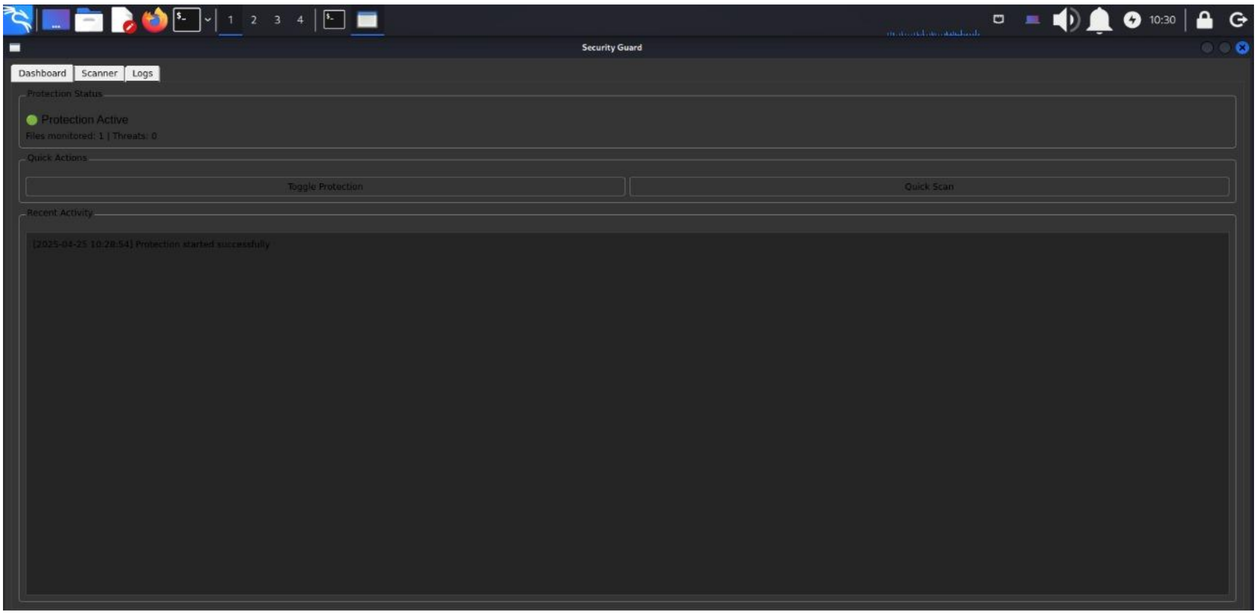
```
┌──(vinay㉿kali)-[~]
└─$ cd Desktop

┌──(vinay㉿kali)-[~/Desktop]
└─$ cd vinay

┌──(vinay㉿kali)-[~/Desktop/vinay]
└─$ source myenv/bin/activate

┌──(myenv)─(vinay㉿kali)-[~/Desktop/vinay]
└─$ python3 vinay.py
```

Fig 2. Commands for Activating software

6.2 Limitations

Resource Usage:

Ongoing process and file monitoring marginally boosted CPU usage on endpoints (~5-10%), which could impact older medical devices.



Protection Active

Files monitored: 1 | Threats: 0

```
[2025-04-25 10:28:54] Protection started successfully
```

Fig 3. Software Dashboard interface

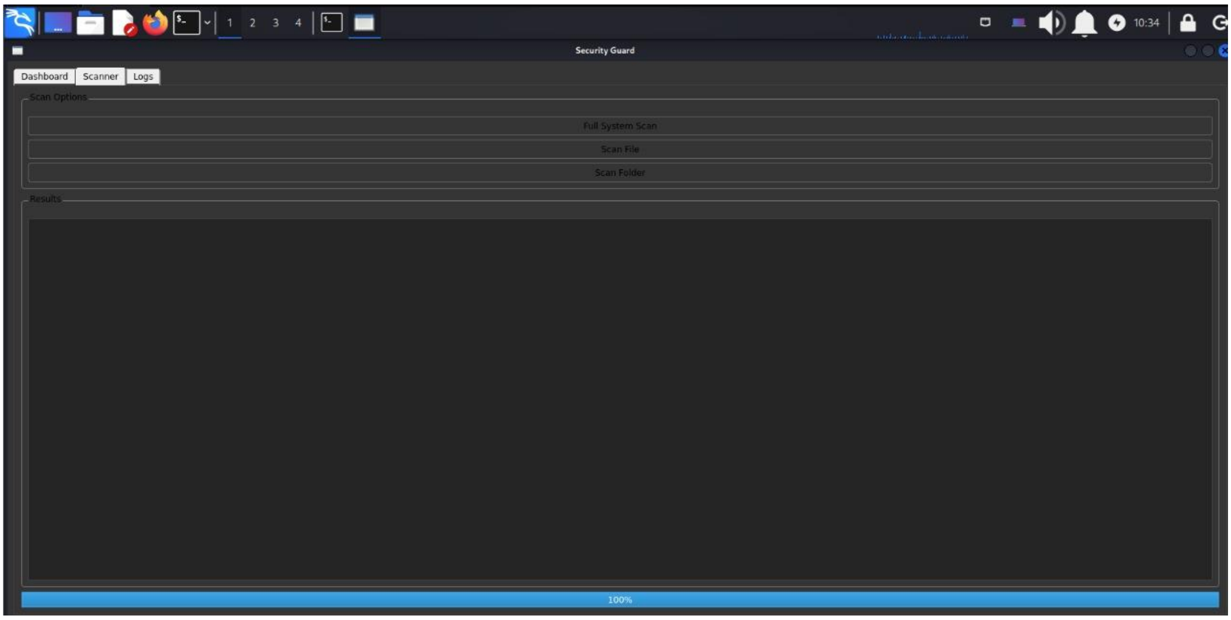


Fig 4. Software Scanner interface

Offline Limitation:

In case the endpoint is offline or disconnected from the network during an attack, detection and backup may be delayed.

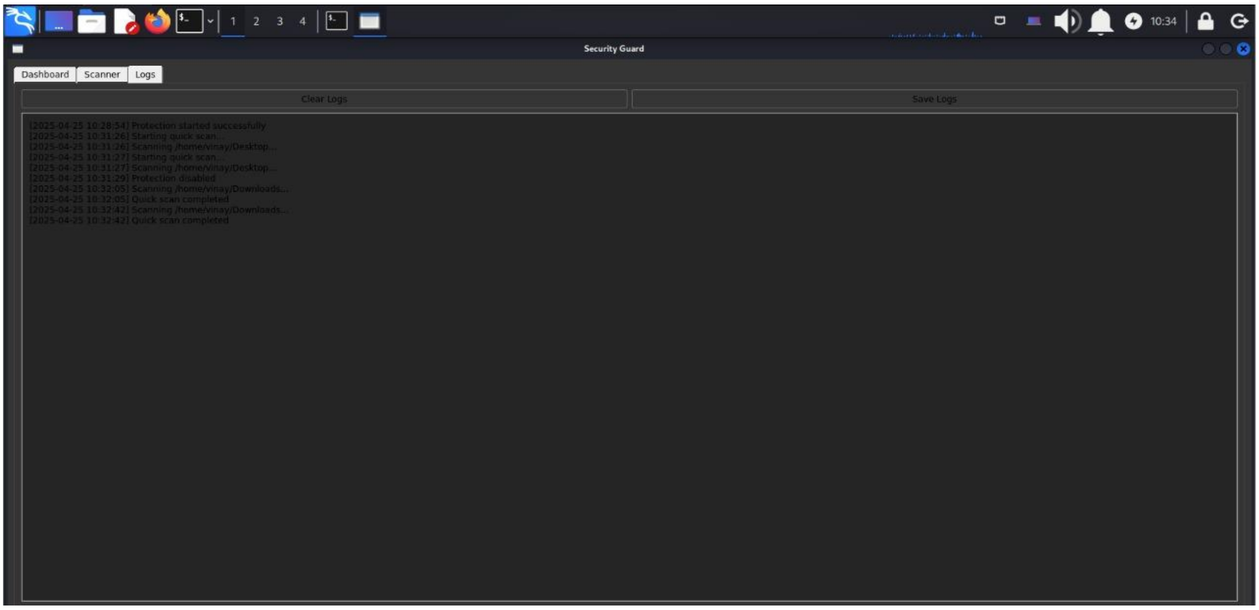
Advanced Evasion Techniques:

Certain advanced ransomware with sandbox evasion or obfuscation capabilities may temporarily evade detection until patterns in behaviour are established.

6.3 Discussion

Overall, the system demonstrates significant promise in securing Medicare endpoints against ransomware. By integrating real-time monitoring, behavioural detection, automated backup, and admin controls, the application addresses both proactive and reactive aspects of cybersecurity. The balance between automation and human oversight ensures high responsiveness without compromising critical healthcare services.

Continuous updates to threat models and expansion to cover mobile or IoT-based medical devices will further enhance system performance and coverage in future iterations.



```
[2025-04-25 10:28:54] Protection started successfully
[2025-04-25 10:31:26] Starting quick scan...
[2025-04-25 10:31:26] Scanning /home/vinay/Desktop...
[2025-04-25 10:31:27] Starting quick scan...
[2025-04-25 10:31:27] Scanning /home/vinay/Desktop...
[2025-04-25 10:31:29] Protection disabled
[2025-04-25 10:32:05] Scanning /home/vinay/Downloads...
[2025-04-25 10:32:05] Quick scan completed
[2025-04-25 10:32:42] Scanning /home/vinay/Downloads...
[2025-04-25 10:32:42] Quick scan completed
```

Fig 5. Software Logs files section

6.4 Challenges Faced

In the creation and deployment of the Endpoint Protection and Ransomware Defence Application, there were various challenges that were encountered:

1. **Complexity of Real-Time Detection**

The development of a system that would be able to detect ransomware in real-time without inducing performance lag on essential Medicare endpoints was a difficult undertaking. Achieving a balance between aggressive monitoring and system resource optimization needed considerable tuning and testing.

2. **False Positives in Behaviour-Based Detection**

Machine learning algorithms sometimes incorrectly labeled valid high-volume file operations (such as software updates or medical imaging transfers) as ransomware activity. This necessitated the need to improve the feature set and add more context-aware logic.

3. Data Recovery Timing and Integrity

It was challenging to ensure timely data recovery while preserving the integrity and confidentiality of medical data, particularly under real-time scenarios. Certain legacy endpoint systems presented compatibility problems with backup operations.

4. Network Dependency

The system's success was partly dependent on uninterrupted internet connectivity, particularly for cloud backup and server communication. Detection and response processes were restricted in offline modes.

5. Integration with Legacy Systems

Medicare environments tend to consist of old hardware or software systems. Compatibility and secure agent installation on these legacy systems had to be ensured through added customization and caution.

6. Security without Disrupting the Users

It was important to ensure that security measures did not disrupt the normal business of medical personnel and infrastructures. User experience and system visibility had to be ensured while endpoint security was achieved.

CHAPTER VII

CONCLUSION & FUTURE SCOPE

7.1 Conclusion

The creation of an Endpoint Protection and Ransomware Defence Application for Medicare systems is imperative in protecting sensitive healthcare information from the increasing menace of cyberattacks. In our project, we have shown how securing endpoints is critical, which are usually the weakest points through which ransomware attacks are executed. Through the use of strong defence mechanisms such as real-time monitoring, encryption, and AI-driven anomaly detection, the application offers a proactive solution to stopping ransomware attacks and minimizing the risk of data breaches in Medicare systems.

With the inclusion of sophisticated technologies such as machine learning, the system can detect suspect behaviour, thereby neutralizing possible attacks before they can inflict harm. The application also provides a total response system that encompasses automated incident response, notification alerts, and isolation of infected devices to ensure the healthcare providers are able to promptly react to any security breaches.

In summary, this project emphasizes that ongoing improvement in security practices within healthcare IT systems is imperative, particularly as the threat environment continues to change. As cyberattacks on healthcare information have increased, Medicare system protection not only comes down to being mandatory for regulatory compliance but also ensuring the integrity of the trust and confidentiality of patient data.

7.2 Future Scope

1. **AI and Machine Learning Improvements:** The future horizon of the project can include improving the machine learning models for better threat detection and prediction. As AI continues to evolve, the incorporation of deep learning models could enhance the system's capability to identify new and emerging ransomware variants.

2. **Integration with Cloud Security:** As health systems move more to the cloud, the software can be extended to offer transparent endpoint protection within cloud-based setups. This would involve protecting data kept on cloud servers as well as ensuring that ransomware does not spread across cloud-hosted services and devices.

3. **Behavioural Analytics for Advanced Threat Detection:** Future enhancement may include the use of behavioural analytics, wherein the system becomes familiar with normal user and device behaviour and responds accordingly. Anything out of this baseline would set off an alert, allowing faster detection of complex ransomware attacks that evade classic signature-based detection.

4. **Integration with Other Security Systems:** The system might integrate with other security systems like Security Information and Event Management (SIEM) solutions and intrusion detection/prevention systems (IDS/IPS) for a wider, multi-layered security strategy. This would allow sharing of threat data between various defence systems to enhance overall attack resistance.

5. **Automated Real-time Response:** The potential future use might involve completely automated real-time incident response functions, where the system does everything automatically, including preventive measures such as quarantining impacted devices, blocking anomalous network traffic, or reversing ransomware changes without any operator action.

6. **Conformity with Changing Healthcare Regulations:** With changing regulations such as HIPAA and GDPR, the project would involve automated checks for conformity and reporting to maintain the system in accordance with the most recent healthcare data protection regulations. This would keep healthcare providers compliant with the law while improving their cybersecurity stance.

7. **User Training and Education:** Alongside technological solutions, future activities may involve the creation of user training modules that inform healthcare professionals about ransomware threats and best practices for evading them. A user-informed workforce is usually the first line of defence in preventing successful attacks.

8. **Mobile and IoT Endpoint Protection**: Since healthcare systems grow more dependent on mobile devices and IoT-connected medical devices, moving the endpoint protection to these devices would further improve security, as attacks would no longer be able to spread via less conventional network entry points.

REFERENCES

[1]W. Yu, "Pre-disaster location and storage model for emergency commodities considering both randomness and uncertainty", Safety Science, vol. 141, 2021.Google Scholar

[2] A. A. V. Rani and E. Baburaj, "An efficient secure authentication on cloud based e-health care system in WBAN", Biomedical Research (India), pp. S53-S59, 2016.Google Scholar

[3] A. Alamri, W. S. Ansari, M. M. Hassan, M. S. Hossain, A. Alelaiwi and M. A. Hossain, "A survey on sensor-cloud: architecture applications and approaches", International Journal of Distributed Sensor Networks, pp. 18, 2013. Google Scholar

[4] A. Grady, S. Yoong, R. Sutherland, H. Lee, N. Nathan and L. Wolfenden, "Improving the public health impact of eHealth and mHealth interventions", Australian and New Zealand Journal of Public Health, vol. 42, no. 2, 2018. Google Scholar

[5] A. Lounis, A. Hadjidj, A. Bouabdallah and Y. Challal, "Healing on the cloud: secure cloud architecture for medical wireless sensor networks", Future Generation Computer Systems, vol. 55, pp. 266 277, 2016. Google Scholar

[6] A. Lounis, A. Hadjidj, A. Bouabdallah and Y. Challal, "Secure and scalable cloud-based architecture for e-Health wireless sensor networks", Proceedings of the 2012 21st International Conference on Computer Communications and Networks ICCCN 2012, August 2012. Google Scholar

[7] A. Sajid and H. Abbas, "Data privacy in cloud-assisted healthcare systems: state of the art and future challenges", Journal of Medical Systems, vol. 40, no. 155, pp. 1-16, 2016. Google Scholar

[8] A. Sariga and J. Uthayakumar, "Type 2 Fuzzy Logic based Unequal Clustering algorithm for multi-hop wireless sensor networks", International Journal of Wireless and Ad Hoc Communication, vol. 1, no. 1, pp. 33-46, 2020. Google Scholar

[9] A. Tewari and P. Verma, "Security and privacy in e-healthcare monitoring with WBAN: a critical review", International Journal of Computer Applications, vol. 136, no. 11, pp. 37-42, 2016. Google Scholar

[10] H. Alrobei, M. K. Prashanth, C. R. Manjunatha, C. P. Kumar, C. P. Chitrabanu, P. D. Shivaramu et al., "Adsorption of anionic dye on eco- friendly synthesised reduced graphene oxide anchored with lanthanum aluminate: Isotherms kinetics and statistical error analysis", Ceramics International, vol. 47, no. 7, pp. 10322-10331, 2021. Google Scholar

[11] V. Asha, N. U. Bhajantri and P. Nagabhushan, Automatic detection of texture defects using texture-periodicity and Gabor wavelets, vol. 1329, 2012.Google Scholar

[12] S. Chaudhury, A. N. Krishna, S. Gupta, K. S. Sankaran, S. Khan, K. Sau et al., "Effective image processing and segmentation-based machine learning techniques for diagnosis breast cancer", Computational and Mathematical Methods in Medicine, 2022. Google Scholar

[13] M. D. Devi, A. V. Juliet, K. Hariprasad, V. Ganesh, H. E. Ali, H. Algarni, et al., "Improved UV Photodetection of Terbium-doped NiO thin films prepared by cost-effective nebulizer spray technique", Materials Science in Semiconductor Processing, vol. 127, pp. 105673, 2021. Google Scholar

[14] B. Dhanalaxmi, G. A. Naidu and K. Anuradha, "Adaptive PSO based association rule mining technique for software defect classification using ANN", Procedia Computer Science, vol. 46, pp. 432-442, 2015. Google Scholar

[15] Kamal Esraa, Amal F. Abdel-Gawad, Basem Ibraheem and Shereen Zaki, "Machine Learning Fusion and Data Analytics Models for Demand Forecasting in the Automotive Industry: A Comparative Study", Journal of Fusion: Practice and Applications, vol. 12, no. 1, pp. 24-37, 2023. Google Scholar

[16] B. Godavarthi, P. Nalajala and V. Ganapuram, "Design and implementation of vehicle navigation system in urban environments using internet of things (IoT)", lOP Conference Series: Materials Science and Engineering, vol. 225, no. 1, pp. 012262, August 2017. Google Scholar

[17] H. Alemdar and C. Ersoy, "Wireless sensor networks for healthcare: a survey", Computer Networks, vol. 54, no. 15, pp. 2688-2710, 2010. Google Scholar

[18] P. K. Jisha, R. Naik, S. C. Prashantha, H. P. Nagaswarupa, H. Nagabhushana, R. B. Basavaraj et al., "Structural refinement band-gap analysis and optical properties of GdAI03 nanophosphors influenced by Dy3+ ion concentrations for white light emitting device applications", Materials Research Express, vol. 3, no. 4, pp. 045007, 2016. Google Scholar

[19] S. Kalaivanan, "Quality of service (QoS) and priority aware models for energy efficient and demand routing procedure in mobile ad hoc networks", Journal of Ambient Intelligence and Humanized Computing, vol. 12, pp. 4019-4026, 2021. Google Scholar

[20] M. Bathre and P. K. Das, "Water supply monitoring system with self powered LoRa based wireless sensor system powered by solar and hydroelectric energy harvester", Computer Standards & Interfaces, vol. 82, pp. 103630, 2022. Google Scholar

[21] S. I. Manzoor and J. Singla, "Fake news detection using machine learning approaches: A systematic review", 2019 3rd international conference on trends in electronics and informatics (lCOEI), pp. 230 234, April 2019. Google Scholar

[22] M. Nagaraju and P. Chawla, "Systematic review of deep learning techniques in plant disease detection", International journal of system assurance engineering and management, vol. 11, no. 3, pp. 547-560, 2020. Google Scholar

[23] B. Bhushan, C. Sahoo, P. Sinha and A. Khamparia, "Unification of Blockchain and Internet of Things (BIoT): requirements working model challenges and future directions", Wireless Networks, vol. 27, pp. 55-90, 2021. Google Scholar

[24] A. Khamparia, G. Saini, D. Gupta, A. Khanna, S. Tiwari and V. H. C. De Albuquerque, "Seasonal crops disease prediction and classification using deep convolutional encoder network", Circuits Systems and Signal Processing, vol. 39, pp. 818-836, 2020. Google Scholar

[25] N. Yuvaraj, K. Srihari, G. Dhiman, K. Somasundaram, A. Sharma, S. M. G. S. M. A.

Rajeskannan, et al., "Nature - Inspired - Based Approach for Automated Cyberbullying Classification on Multimedia Social Networking", Mathematical Problems in Engineering, vol. 1, pp. 6644652, 2021. Google Scholar

[26] M. H. Ahmadi, B. Mohseni-Gharyehsafa, M. Ghazvini, M. Goodarzi, R. D. Jilte and R. Kumar, "Comparing various machine learning approaches in modeling the dynamic viscosity of CuO/water nanofluid", Journal of Thermal Analysis and Calorimetry, vol. 139, pp. 2585-2599, 2020. Google Scholar

[27] A. P. Singh, N. R. Pradhan, A. K. Luhach, S. Agnihotri, N. Z. Jhanjhi, S. Verma, et al., "A novel patient-centric architectural framework for blockchain-enabled healthcare applications", IEEE Transactions on Industrial Informatics, vol. 17, no. 8, pp. 5779-5789, 2020. Google Scholar

[28] V. Malagavelli, S. Angadi, J. S. R. Prasad and S. Joshi, "Influence of metakaolin in concrete as partial replacement of cement", International Journal of Civil Engineering Technology, vol. 9, no. 7, pp. 105-111, 2018.Google Scholar

[29] T. Manohar, S. C. Prashantha, H. P. Nagaswarupa, R. Naik, H. Nagabhushana, K. S. Anantharaju et al., "White light emitting lanthanum aluminate nanophosphor: near ultra violet excited photoluminescence and photometric characteristics", Journal of Luminescence, vol. 190, pp. 279-288, 2017. Google Scholar

[30] R. Meenal, D. Binu, K. C. Ramya, P. A. Michael, K. Vinoth Kumar, E. Rajasekaran, et al., "Weather forecasting for renewable energy system: a review", Archives of Computational Methods in Engineering, vol. 29, no. 5, pp. 2875-2891, 2022. Google Scholar

KALASALINGAM
ACADEMY OF RESEARCH AND EDUCATION
(DEEMED TO BE UNIVERSITY)
Under sec. 3 of UGC Act 1956. Accredited by NAAC with "A++" Grade

INTERNAL QUALITY ASSURANCE CELL

PROJECT AUDIT REPORT

This is to certify that the project work entitled "**Endpoint Protection and Ransomware Defence Application for Medicare Systems**" categorized as an internal project done by M.VINAY KUMAR, M MADHAN, M MOHAN KRISHNA REDDY, K DIVYA of the Department of Computer Science and Engineering, under the guidance of **Dr K Kartheeban** during the Even semester of the academic year 2024 - 2025 are as per the quality guidelines specified by IQAC.

Quality Grade

Deputy Dean (IQAC)

Administrative Quality Assurance **Dean (IQAC)**