Republic of Iraq
Ministry of Higher Education and Scientific Research
University of Babylon
Information Technology
Department of Information Technology

BLOCKCHAIN TECHNOLOGY FOR SECURING MEDICAL HEALTHCARE RECORDS AGAINST RANSOMWARE ATTACK

A Thesis

Submitted to the Council of the College of Information Technology for Postgraduate Studies of University of Babylon in Partial Fulfillment of the Requirements for the Degree of Master in Information Technology-Information Networks

Noor Thamer Mahmood Ekaied

Supervised

Asst. Prof. Dr. Raaid Nasur Kadham Khalil

2022 A.D. **1444 A.H.**

Supervisor Certification

I certify that the thesis entitled (**Blockchain Technology for Securing Medical Healthcare Records against Ransomware Attack**) was prepared under my supervision (**Asst. Prof. Dr. Raaid N. Alubady**) at the department of Information Networks/ College of Information Technology/ University of Babylon as partial fulfillment of the requirements of the degree of Master in Information Technology-Information Networks.

Signature:

Supervisor Name: **Asst. Prof. Dr. Raaid N. Alubady**

Date: / /2022

The Head of the Department Certification

In view of the available recommendations, I forward the thesis entitled "**Blockchain Technology for Securing Medical Healthcare Records against Ransomware Attack**" for debate by the examination committee.

Signature:

Prof. Dr. Saad Talib Hasson

Head of Information Networks Department

Date: / /2022

Certification of the Examination Committee

We hereby certify that we have studied the dissertation entitled (**Blockchain Technology for Securing Medical Healthcare Records against Ransomware Attack**) presented by the student (**Noor Thamer Mahmood**) and examined him/her in its content and what is related to it, and that, in our opinion, it is adequate with () standing as a thesis for the degree of Master in Information Technology-Information Networks.

Signature:
Name:
Title:
Date: / / 2022
(**Chairman**)

Signature:
Name:
Title:
Date: / / 2022
(**Member**)

Signature:
Name:
Title:
Date: / / 2022
(**Member**)

Signature:
Name: Dr. Raaid N. Alubady
Title: Asst. Prof.
Date: / / 2022
(**Member and Supervisor**)

Approved by the Dean of the College of Information Technology, University of Babylon.

Signature:
Name: Prof. Dr. Hussein Atiya Lafta
Date: / / 2022
(**Dean of Collage of Information Technology**)

Dedication

I dedicate my thesis to:

To whom I live for her satisfaction, and I owe her my Happiness...

My Kind Aunt, and All My Family.

Acknowledgement

First of all, I am grateful to the Almighty Allah for his grace on me to finish this work.

My thanks are due to all my beloved family members who gave me their support and guidance throughout the period of study.

I wish to express my warmest thanks and deep gratitude to my supervisor Dr. Raaid N. Alubady, for his encouragement, invaluable advice, criticisms, encouragement, help, and supervision throughout this work to be in the best manner.

I owe earnest thanks to the Dean of the Al-Mustaqbal University College, as well as Dr. Hassan Shaker Magdi, Dr. Abbas Albawi, Asst. Prof. Dr. Alharith A. Abdullah, Zahraa Qassim and all the teaching staff at the College of Information Technology-University of Babylon.

Finally, I owe earnest thanks to all.

Abstract

Ransomware is defined as malicious software designed by specialized people in the field of computing to blackmail whether individuals or business by blocking their computer systems and encrypting their data. It considers an essential threat to Cyber Security. Medical Healthcare Records (MHRs) have been one of the main targets of Ransomware attacks. This could be attributed to the fact that attackers here deal with personal medical statistics and sensitive patient data. Most patients who fall under such threat hastily respond to their blackmailers as they fear being scandalized. Accordingly, utilization of Ransomware in medical healthcare has become an immoral means for those attackers to gain huge amounts of money.

The main objective of this thesis is intended to enhance the healthcare system through Blockchain technology to treat and investigate unusual transactions that may have unfavorable effects on people's privacy. For this purpose, an astute arrangement (smart contract) has been developed. Thus, MHRs are protected from any Ransomware attacks, especially from those attackers who pretend to be patients and attempt to penetrate the network through their claimed records. Besides, it is adopted two procedures in case a node is failed and is unable to do any transaction through the network. Either a copy of the impaired data is retrieved randomly from any network node or restored from the nearest node.

Finally, the proposed system is evaluated through the Blockchain-Ethereum platform. In addition, metrics are utilized for evaluating performance, including cost, immutability, data storage, estimated time required by attackers to attack the block, and recovery time needed to recover the lost transactions. According to that, the proposed system has improved the MHR protection based on Blockchain technology, by increasing the estimated attacker time required via the attacker to attack the network by 98%. Furthermore, it reduced the cost to 855304 Wei and the execution time for raising patient records on Ethereum Network compared to the standard system by 60%

Declaration Associated with this Thesis

- N. Thamer and R. Alubady, “A Survey of Ransomware Attacks for Healthcare Systems: Risks, Challenges, Solutions and Opportunity of Research,” *1st Babylon Int. Conf. Inf. Technol. Sci*. pp 1-6, 2021
- N. Thamer and R. Alubady. "Secure Medical Healthcare Record from Ransomware Attack Using Smart Contract", *Mathematical Statistician and Engineering Applications*. (Acceptance)

Table of Contents

List of Tables

List of Figures

List of Algorithm

List of Abbreviations

Abbreviation	Description
AES	Advanced Encryption Symmetric
AI	Artificial Intelligence
API	Application Programming Interface
APT	Advanced Persistent Threat
BFT	Byzantine Fault Tolerant
BTC	Bitcoin
CHF	Cryptographic Hash Function
CLI	Command-Line Interface
CoAP	Constrained Application Protocol
DDoS	Distributed Denial-of-Service
DDS	Data Distribution Service
ECG	Electrocardiogram
EEG	Electroencephalogram
EHR	Electronic Health Record
ETH	Ether
EVM	Environment Virtual Machine
GR	Gain Ratio
GUI	Graphic User Interface
GUI	Graphical User Interface
HIPAA	Health Insurance Portability and Accountability
HTTP	HyperText Transfer Protocol
ICT	Information and Communication Technology
IG	Knowledge Benefit
IoMT	Internet of Medical Things
IoT	Internet of Things
ISP	Internet Service Providers
MCFP	Malware Capture Facility Project
MHR	Medical Healthcare record

ML	Machine Learning
P2P	Peer to Peer
PCA	Principal Component Analysis
PCAP	Packet Capture
PHR	Patient Health Record
PoA	Proof of Authority
PoS	Proof of Stack
PoW	Proof of Work
PSTB	Parallel Spanning Tree Broadcast
RPC	Remote procedure call
RPM	Remote Patient Monitoring
SC	Smart Contract
SCA	Side-channel Attack
SDN	Software Define Network
SP	Shortest path
TF-IDF	frequency inverse document frequency
Tor	the onion routing
UI	User Interface

APPENDIX


BICITS'21
1st Babylon International Conference on Information Technology and Science
CERTIFICATE OF ACCEPTANCE
This certificate is granted to
Noir Thamer and Raaid Alubady
Certifies the acceptance of the research paper entitled:
A SURVEY OF RANSOMWARE ATTACKS FOR HEALTHCARE SYSTEMS: RISKS, CHALLENGES, SOLUTIONS AND OPPORTUNITY OF RESEARCH
in
BICITS'21
Which will be held on 28-29 April, 2021 in Babylon, IRAQ, by College of Information Technology, University of Babylon and Technically Sponsored by IEEE represented by IEEE Iraq Section.
University of Babylon-College of IT
BICITS'21
IEEE
IEEE
Iraq Section
IEEE

A Survey of Ransomware Attacks for Healthcare Systems: Risks, Challenges, Solutions and Opportunity of Research

Noor Thamer
College of Information Technology
University of Babylon, Babylon, Iraq
Al-Mustaqbal University College
Babil , Iraq
noor.tmit@student.uobabylon.edu.iq

Raaid Alubady
College of Information Technology
University of Babylon
Babylon, Iraq
alubadyraaid@itnet.uobabylon.edu.iq

echnology and Science (BICITS) | 978-1-6654-1573-6/21/$31.00 ©2021 IEEE | DOI: 10.1109/BICITS51482.2021.9509877

***Abstract*— Healthcare is one of the most vulnerable sectors of cyber-attacks. As it continues to expand exponentially and moves to digitally-enabled healthcare services, cyber-criminals are trying to take advantage of the weaknesses and security vulnerabilities correlated with these shifts. As a result of technical developments, a multitude of highly powerful risks such as Ransomware is facing the healthcare sector. Ransomware is cyber-attack targeting companies and household users and has increased lately due to its productive results. It conflicts have significantly improved over the last few years. The study shows an exhaustive survey on Ransomware attacks and fixes these attacks. The main aim of this study is to classify the solution strategies for Ransomware attacks in healthcare that used to prevent the Ransomware, such as Blockchain technology, Software define network technology, Machine Learning, and other tools as well as to highlight many issues faced by researchers during the process of discovering a way to solve Ransomware attacks in health care systems. In addition, the study will provide scientific benefits to researchers in the field of information security, health institutions, and security companies.**

Keywords*— *Healthcare System, Security, Ransomware Attacks, Blockchain, Machine Learning, Software Define Network.

I INTRODUCTION

malware can infect the computer as soon as a connection is accessed or a file is downloaded. Next, the attack may search through all information that can be encrypted, such as hard disks, network files, and remote drivers [4]. After encryption, a "key" is required to open the records; this key is protected by the hacker and is not distributed until the victim gives the demanded amount or ransom [5].

Generally, Health institutions were not considered a primary goal for Ransomware until 2016. However, by 16 October 2016, 14 Hospitals were targeted for Ransomware and a total of 173 incident data violations for hacking/information technology (IT) were registered officially, For two reasons, hospitals have been a simple target for hackers: (1) data storage for health care (e.g. electronic medical records) documents and (2) security flaws in IT processes. In addition, patient files' active hacking frequency rose from 55% in 2015 to 64% in 2016. When they are struck by Ransomware, some hospitals were desperate to pay for the most up-to-date information necessary to supply the patients with vital treatment, including opioid interactivities, medication instructions, and medical records. There is therefore now a significant risk of a Ransomware attack in the health sector, especially because it tracks other leading industries in securing essential information[6]

MATHEMATICAL STATISTICIAN AND ENGINEERING APPLICATIONS (MSEA)
ISSN: 2094-0343
2326-9865

4 Oct., 22

ACCEPTANCE LETTER

Paper ID: [MSEA 503]

Title of Paper: [Security Against Ransowmare Attack in Medical Healthcare Records Using Blockchain Technology]

Dear,

[1,2]Noor Thamer Mahmood, [1]Raaid Alubady,

[1]Department of Information Networks, College of Information Technology, University of Babylon, Iraq.

[2]Al-Mustaqbal-University College, Iraq.

We are pleased to inform you that, after our double-blind peer review, your manuscript identified above has been accepted for publication in **Mathematical Statistician and Engineering Applications, ISSN** [2094-0343,2326-9865] in **Vol 71.2022**. If there are any final comments from the reviewers or the editor, they can be found at the bottom of this letter.

.

الخلاصة

تُعرَّف برامج الفدية كبرامج ضارة تم تصميمها من قبل أشخاص متخصصون في مجال الحوسبة لغرض الابتزاز سواء للأفراد أو الشركات، حيث يتم ذلك عن طريق حظر أنظمة الكمبيوتر الخاصة بهم اوتشفير بياناتهم. هذه البرامج تعتبر تهديدًا أساسيًا للأمن السيبراني. سجلات الرعاية الصحية الطبية (MHRs) يمكن اعتبارها أحد الأهداف الرئيسية لهجمات برامج الفدية. يمكن أن يُعزى ذلك إلى حقيقة أن المهاجمين هنا يتعاملون مع الإحصاءات الطبية الشخصية وبيانات المرضى الحساسة. معظم المرضى الذين يقعون تحت هذا التهديد يستجيبون على عجل لمبتزهم خوفًا من انتهاك خصوصيتهم. وفقًا لذلك، أصبح استخدام Ransomware في الرعاية الصحية الطبية وسيلة غير أخلاقية لهؤلاء المهاجمين لكسب مبالغ ضخمة من المال.

الهدف الرئيسي من هذه الرسالة هو تعزيز نظام الرعاية الصحية من خلال تقنية Blockchainلمعالجة والتحقيق في المعاملات غير العادية التي قد يكون لها آثار غير مواتية على خصوصية الأشخاص. لهذا الغرض، تم تطوير عقد ذكي. وبالتالي، فإن MHRs محمية من أي هجمات رانسوم وير، لا سيما من هؤلاء المهاجمين الذين يتظاهرون بأنهم مرضى ويحاولون اختراق الشبكة من خلال سجلاتهم المزعومة. إلى جانب ذلك، يتم اعتماد إجراءين في حالة فشل العقدة وعدم تمكنها من إجراء أي معاملة عبر الشبكة. إما أن يتم استرداد نسخة من البيانات المعطوبة بشكل عشوائي من أي عقدة شبكة أو استعادتها من أقرب عقدة.

أخيرًا ، قيم النظام المقترح من خلال منصة Blockchain-Ethereum. بالإضافة إلى ذلك ، يتم استخدام مجموعة مقاييس لتقييم الأداء، بما في ذلك التكلفة والثبات وتخزين البيانات والوقت المقدر الذي يحتاجه المهاجمون لمهاجمة الكتلة ووقت الاسترداد اللازم لاسترداد المعاملات المفقودة. وفقًا لذلك، النظام المقترح حسّن من حماية MHR استنادًا إلى تقنية Blockchain، وذلك من خلال زيادة الوقت المقدر للهجوم المطلوب من قبل المهاجم لمهاجمة الشبكة بنسبة ٩٨٪. علاوة على ذلك ، خفضت التكلفة إلى ٨٥٥٣٠٤ Wei ووقت التنفيذ لرفع سجلات المرضى على شبكة Ethereum مقراتنا بالنظام القياسي بنسبة ٦٠٪.

بِسْمِ

(اقْرَأْ وَرَبُّكَ الأَكْرَمُ الَّذِي عَلَّمَ بِالْقَلَمِ
عَلَّمَ الإِنسَانَ مَا لَمْ يَعْلَمْ)

سورة العلق/ الاية ٣-٥

صدق الله العلي العظيم

جمهورية العراق

وزارة التعليم العالي والبحث العلمي
جامعة بابل-تكنولوجيا المعلومات
قسم شبكات المعلومات

تقنية السلسلة الكتلية لتأمين سجلات الرعاية الصحية الطبية من هجوم الفدية

رسالة

مقدمة إلى مجلس كلية تكنولوجيا المعلومات في جامعة بابل والتي هي جزء من متطلبات الحصول على درجة الماجستير في تكنولوجيا المعلومات-شبكات المعلومات

نور ثامر محمود كعيد

أشراف

أ.م.د. رائد نصر كاظم خليل

١٤٤٤ هـ

٢٠٢٢ م

1.1 Introduction

Healthcare is a top priority for every society and every human being in the world. Therefore, the sector should be covered with resources and technical expertise since life and death risks are involved in its work. In addition to treating patients, healthcare providers are responsible for keeping their patients' private information safe. Medical Healthcare records (MHR) is made up of Electronic Health Record (EHR) and Remote Patient Monitor (RPM) [1][2].

Information and Communication Technology (ICT) has facilitated improvements possible. Consequently, patient care has changed in many ways. Smart wearable devices and other sensors monitor a patient's data, which is collected and sent for intelligent analysis to make better inferences and provide more personalized care. In addition, hospitals keep EHR up-to-date with patient health information so that reports and medical histories can be accessed quickly and shared easily [3].

Malicious software, including worms, malware, viruses, and spyware, can attack computers in various ways. For example, cybercriminals have started targeting the healthcare industry with Ransomware, a type of malware that encrypts an infected device and any devices or network drives connected to it. After encrypting a device, cybercriminals ask for a ransom before they will decrypt it. Unfortunately, many businesses are forced to pay a ransom because they do not have good disaster recovery and backup plans [4].

In September 2020, a large hospital chain was hit hard by Ransomware, according to NBC News. Because of its effects, all workers and medical staff were relegated to using pen and paper to track the patient's condition over the weekend. Over 400 locations in the United States were impacted by this cyber-attack, making it the largest in history [1]. Ransomware is a type of malicious

software that encrypts data, *i.e.*, rendering it useless, and locks down the systems that rely on. There are two types of Ransomware, Crypto Ransomware and locker Ransomware. In the case of crypto Ransomware, it uses phishing email to attack the victim, Once Ransomware becomes active, and it encrypts files. TOR is a malicious program belonging to the Ransomware family. This malware encrypts data for the purpose of making ransom demands for the decryption. In other words, victims cannot access or use the files affected by this Ransomware, and they are asked to pay - to recover access/use of their data. Figure 1.1 illustrates to understand how Ransomware is worked [5].

Figure 1.1 Crypto Ransomware Attack [6]

Researchers have offered many ways to prevent Ransomware from attacking and encrypting MHR, like Implementing intrusion detection tools, awareness of users, Configuring firewalls, and backup data regularly. However, these tools are rudimentary compared to the rapid development of Ransomware. In addition, the researchers developed a methodology for preventing the Ransomware attack and mitigating its effects in the medical community, like

Machine Learning (ML), Software Defined networks(SDN), and Blockchain technology [7].

Researchers realize that Blockchain can be used for more than just financial transactions. As a decentralized technology, Blockchain can be used in a wide range of valuable ways, such as in healthcare, logistic support, supply chain management, and other areas (see Figure 2.1 [10]). Blockchain is a tamper-proof list of records implemented with a distributed ledger's help. Blockchain enables users to record transactions in a shared ledger within a community, such that under normal operation of the Blockchain network, no transaction can be changed once published. It gives us a secure, decentralized database that can do its work without any help or a central administration. Furthermore, Blockchain uses cryptographic methods (like hash functions, asymmetric encryption, and digital signatures) between different parties in a system. This helps keep their trust while interacting [8][9].

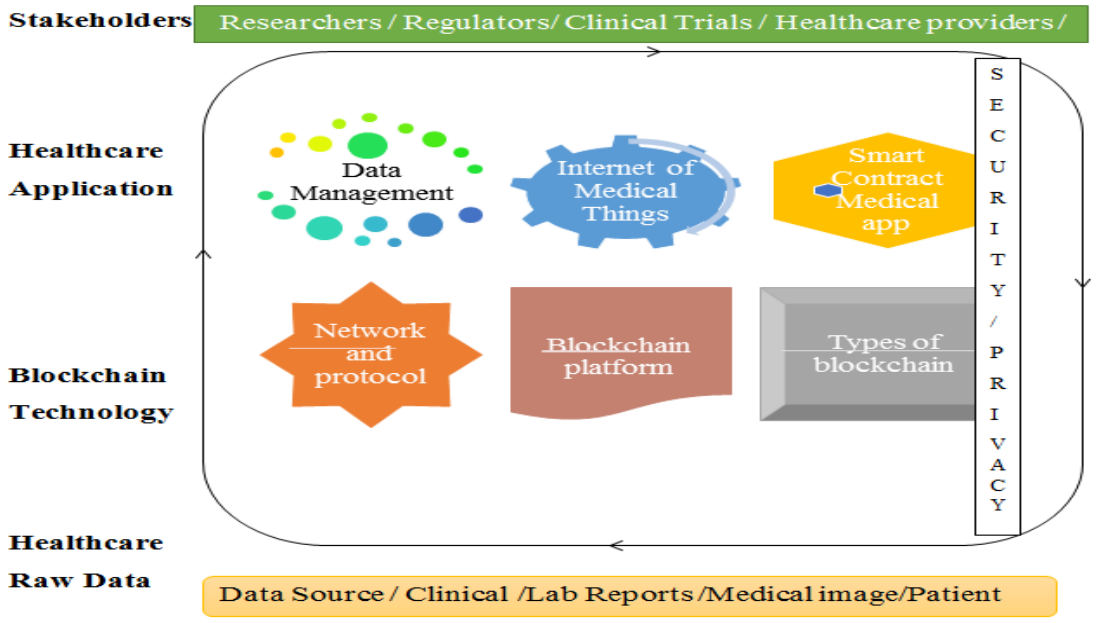


Figure 1.2 Workflow Environment for Healthcare Applications Using Blockchain Technology [10]

Currently, Blockchain technology in MHR has changed the traditional identity management utilized in numerous healthcare applications by which performance has boosted, and the healthcare industry's costs and expenditures have decreased. The four levels of Blockchain-based healthcare solutions consist of raw data sources, Blockchain technology, healthcare apps, and healthcare stakeholders.

1.2 Related Works

Several prior studies have been made regarding the Blockchain network by some researchers. Healthcare is one of the most sensitive areas regarding privacy, security, access control, and availability of medical data since it handles essential information[11]. Transmission, storage, and manipulation are three primary phases where this industry must ensure security. In this section, several works that used Blockchain technology to process the security of medical data are addressed

The author in [12] presented how people use healthcare systems and applications could identify the abnormality. The risk index is obtained by the individual conducting such activities, depending on their similarity to the standard behavior. When the risk value has been calculated in real-time, the device may either access a low-risk event during a login event, challenge Multi-Factor Authentication (MFA), or block access for risky events during the login event. The Artificial Intelligence (AI) and Machine Learning (ML) techniques have a 360-scale perspective of how (EHR) consumers communicate with patient data and consider the clinical context behind each access to turn reactive toward constructive data management. This will rapidly identify behavioral defects as critical factors in enhancing cyber-security in healthcare.

Almashhadani et al., [13] proposed a multi-classifier intrusion detection system with a modern topology to detect the Ransomware network's operation, which is implemented using machine learning techniques. It also uses a language-independent algorithm to detect gibberish domain names based on general sonic axioms. A dedicated testbed environment is created and recorded and analyzed Packet Capture (PCAP) images. In addition, the Malware Capture Facility Project (MCFP) data set for Locky's PCAP files are also compiled and carefully analyzed. The experimental evaluation of the proposed detection system reveals that it provides high detection precision, low false positive rate, legitimate extracted functionality, and detects Ransomware network activities in a highly successful way. The acute lack of Ransomware datasets is a key problem. Several benchmark datasets have been analyzed, such as KDDCUP 99, NSL-KDD, UNSW-NB15 and Canadian Institute for Cyber-security datasets. The core issue of this research was the extreme shortage of Ransomware datasets.

Hirano & Kobayashi [14] presented a novel machine for learning based on the Ransomware detection process. They investigated the features extracted from a live forensic hypervisor labelled way back visor access patterns. They also chose cinema-defining features from hardware I/O logs to distinguish Ransomware from harmless applications with close compliance with Ransomware. Three machine learning models were developed, namely the Random Forest, Support Vector Machine, and K-Nearest Neighbors. Their studies used the five-dimensional features and obtained a measurement score of 98%. They created and evaluated machine learning models using the same factors mentioned above.

Akbanov et al., [15] demonstrated Ransomware analysis findings and the SDN-based security system they've designed. The famed WannaCry Ransomware is utilized as a proof of concept. When WannaCry is being run in a virtual lab environment, they pay close attention to how it behaves. Create an SDN detection and mitigation framework based on OpenFlow, which is now the most commonly utilized SDN standard, and construct a solution based on it. Suspicious activity is detected by monitoring network traffic, which is then blocked by adding flow Table entries to OpenFlow switches in real-time. The POX controller has been updated to reflect the logic of the suggested architecture. The implementation makes use of WannaCry's characteristics and produces traffic for detection purposes. The test findings here with several WannaCry samples demonstrate that the created method can quickly identify the infected devices in every situation and stop WannaCry from spreading. An SDN-based mitigation mechanism for Ransomware with worm components, such as WannaCry, has been investigated and developed for the first time. The WannaCry features identified in the static and dynamic WannaCry analysis have been used to develop mechanisms for the real-time detection of WannaCry. However, this model neglects to preserve the privacy of users' data by making it visible to all, scalability issues.

A new framework was proposed by Kumar et al., [16] for malware detection mechanisms with the Internet of Things (IoT) devices in the healthcare sector using Blockchain, clustering, and classification machine learning. The machine learning mechanism collects threat information automatically using the clustering and classification algorithms and then holds data in Blockchain. The dataset includes 6192 benign and 5560 malware apps collected from the Google Play Store and Chinese App store. For evaluation measurement, they obtain true

positive and false positive rates and precision of classification. The drawbacks associated with the solution are its failure to deal with such hiding strategies and features when compiling APK with Dex2jar.

Akarca et al., [17] presented regulatory frameworks to facilitate handling health data, patient rights, cyber security, and provider-centric perspectives. They used Blockchain technology to improve healthcare processes and lower transaction costs by using smart contract techniques to promote the handling of health records and patient privileges and prevent Ransomware attacks. They presented legislative structures using Blockchain technologies to optimize healthcare practices. They reduced the processing costs through the use of a smart contract.

Chenthara et al., [18] proposed a system using the Hyperledger Fabric Blockchain platform. That can be used to efficiently share and maintain health information while implementing access control. As a result, this study presents a new patient-centric Blockchain called Healthchain for EHRs that, by establishing a distributed ledger platform, reduces the majority of bottlenecks and avoids the possibility of a single point of failure in current systems. The Health Chain Framework uses self-governing and continuously running smart contracts to retain patient history by synchronizing records in various formats and retrieving data through REST server API. This technical advancement, which includes cryptographic components, provides a more efficient framework for storing, transferring, and accessing EHR in the cloud environment. The results of the research and prototype implementation demonstrate that the method is tamper-resistant since information will be stored as hash values for each healthcare transaction on the Blockchain. The research must be well-versed in all varieties of healthcare applications, such as remote

patient monitoring, and all of the configurations of the Blockchain network have not been disclosed.

Wani & Revathi [19] suggested an SDN-based Crypto Ransomware mitigation method which is proposed for the IoT environment, known as IoTSDN-RAN, which keeps track of all IoT traffic with the outside world, including any connection between an IoT device and a Command and Control (C&C) server in the event of Ransomware. The SDN controller immediately deploys IOTSDN-RAN. Removing the Constrained Application Protocol (CoAP) headers may identify Ransomware. Three primary phases make up the suggested method's execution. The first step is Sample Collection, which entails gathering samples of both attack traffic and regular traffic using a realistic dataset. The suggested algorithm is trained in the second step using the particular traffic characteristics obtained in the first step. For producing correct results, the training algorithm parameters are changed. Naive Bayes and Principal Component Analysis (PCA) are utilized in the second and third rounds of the recommended technique to find Ransomware. Utilizing the data from the earlier phases, the third and last step, Detection and Mitigation, includes recognizing Ransomware assaults. Ransomware is reduced after its existence has been established. The experiment findings show that the suggested approach increases the Ransomware attack accuracy and detection rate. Future work should focus on reducing the false negative rate for identifying all Ransomware variants and other common malware that affect the IoT environment. As for the data set used to simulate the experiment, they used an online dataset. Even though the SDN technology remains not robust enough to prevent an attack on the IoT devices themselves, it still may help reduce the impact on the whole network of IoT devices

Al Qartah in [5] introduced a study on health systems that are a top target for Ransomware due to a variety of factors, such as the constantly growing attack surface, the inadequate cyber defenses, the human component, and the increased feeling of urgency to recover private patient information or medical systems. Also, it is noticed that Ransomware attacks may have significant repercussions, including harm to one's reputation, interruption of medical service, compromise of patient safety, loss of data privacy, and financial penalties. Examining the evolving Ransomware in the healthcare sector provides best practices to reduce cyber security risks. Understanding the effects of Ransomware attacks on the healthcare industry and the factors contributing to their success will help hospitals and cyber security professionals better prepare for Ransomware attacks and respond to successful breaches without paying the ransom and breaking the attack cycle. Numerous Ransomware attacks on healthcare professionals have occurred since 2016, costing the American health system about $157 million. The research findings suggest recommended mitigation measures to make healthcare providers resistant to Ransomware and extortion risks, including phishing simulation and awareness training, data backups, vulnerability and patch management, email security, threat intelligence, incident response plan, multi-factor authentication, network segmentation, and deception. From our point of view, all of these solutions are primitive solutions due to the continuous development of the Ransomware attack and their ability to break any system's security barriers.

In [20], the authors proposed an efficient and tractable data analytics framework to detect new malicious addresses in a Ransomware family automatically. Using a topological data analysis-based approach and novel Blockchain graph-related features showed that the proposed methodology

significantly improves precision and recall for Ransomware transaction detection compared to existing heuristic-based approaches. It can thereby utilize to automate Ransomware detection. As for the data set, a union of datasets from 27 Ransomware families has been deployed. However, their work results could have been improved by combining their approach with other methods and including intelligence information to increase prediction accuracy.

Sowthily et al., [21] presented a new method of Ransomware identification suggested based on Hexacodes only and without opcodes and invoking machine learning classifiers. There are two methods of functionality selection: Knowledge Benefit (IG) and Gain Ratio (GR). They concluded that IG with RF is statistically important. It is suggested that Shell-based feature discovery techniques may be used over Hexacodes features and deep learning techniques as classifiers. In addition, when constructing a paper word matrix, the term frequency-inverse document frequency (TF-IDF) values of the hex can be directed instead of the frequency. Table 1.1 is presented to summary the selected related works studies.

Table 1.1 Summary of Related Works

Ref.	Method	Advantage	Disadvantage
[16]	Blockchain and ML	A framework can achieve higher accuracy for Ransomware detection with a low number of false-negative and positive rates.	Its failure to deal with such hiding Strategies and features when compiling APK with Dex2jar.

[17]	Blockchain, and Smart Contract	Facilitate the handling of health data in the context of regulatory frameworks, patient rights, and cyber-security.	Scalability and Storage issues for nodes and networks requiring greater Bandwidth.
[20]	Blockchain graph-related features	Efficient and tractable data analytics framework to automatically detect new malicious addresses in a Ransomware family.	Difficult to know Ransomware address detection after the ransom is received.
[21]	ML	Detect & prevent Ransomware only from Hexacodes using ML.	High Level of Error Susceptibility.
[12]	AI and ML	Identify the abnormality in healthcare systems.	Susceptible to errors.
[14]	ML, Domain Generation Algorithm	The multi-classifier intrusion detection system detects the operation of Ransomware in case of Locky.	The acute lack of Ransomware datasets was a key problem.
[15]	SDN and Open Flow Protocol	Mitigate the WannaCry Ransomware attack.	Scalability issues.
[19]	IoT SDNRAN application and Open Flow Protocol	Detection mechanism for IoT healthcare sector from the Ransomware attack.	Not robust enough to prevent an attack on the IoT devices themselves.

[13]	ML techniques	Offers high detection accuracy, low false positive rate, valid extracted features, and is highly effective in tracking Ransomware network activities.	Not tested on healthcare implants and other internet-connected gadgets, and an extreme shortage of Ransomware datasets.
[17]	Hyperledger Fabric Blockchain platform	secure and effective framework to store, transfer and access HER.	Lack in scalability.
[5]	Miscellaneous Technologies	Providing solutions such as paying attention to the user's awareness of the system, constantly taking a backup copy of the data.	Primitive solutions due to the continuous development of the Ransomware attack.

According to the above studies, even though many studies and tools were found to handle Ransomware attacks, they did not mention how the attack can choose and encrypt patient records. Instead, the proposed system considered the possible attack cases for Ransomware, whether the attack was from outside or inside the network. Therefore, it is noted that the Blockchain is the best technology to prevent and detect Ransomware attacks. The main reason is that Blockchain solutions are not centralized, therefore, there would be no copies of information that could be held for ransom. Also, Blockchain cannot be changed; no one, not even the person in charge of the system, can change information written to a Blockchain.

1.3 Research Problem

One of the most significant challenges facing MHR systems is patient data protection. Currently, MHR depends on centralized systems for managing and transmitting patient data and healthcare providers [22][23]. As a result, MHR is one of the fields most likely to be targeted by cyber-attacks. As health insurance continues to evolve fast and keeps moving toward digitally-enabled services, cybercriminals look for ways to take advantage of the security holes and weaknesses that come with these changes, especially the Ransomware attack. There are various ways for Ransomware to attack. Methods of a Ransomware attack on MHR that have not been discussed by researchers may be accrued from outside or inside the Blockchain (Ethereum) network. By impersonating a patient and trying to send transactions that contain the attack link, or one of the nodes in the Blockchain network fails or is damaged for any reason.

1.4 Research Question

To meet such motives, though Blockchain technologies have played a decisive role, its efficacy remains unexplored to answer the following research questions:

i. How could Ransomware attack to victim of the health sector?
ii. Can Blockchain technology prevent the Ransomware attack probability?
iii. What effective measure could be employed in the Blockchain technique to detect Ransomware at the initial stage? (To thwart away the possibility of the future adversary).
iv. How can a Blockchain-driven proposed system enable seamless data recovery post-error conditions?

v. How to evaluate the proposed system?

1.5 Research Objective

The primary goal of the present study is to provide a system with security against Ransomware attacks on MHRs using Blockchain technology. The proposed system can prevent attackers using Ransomware programs from attacking the victims who have MHRs and exploiting them financially. This is achieved by employing the latest security technology (Blockchain Technology) by which will provide complete protection of patient data and reduce additional costs to the user incurred by relying on a third party.

In addition, the following specific research goals can also help to reach this goal:

1. To investigate and study the behavior or the ways of Ransomware attacks in the health sector?
2. To develop a security system against Ransomware attacks on MHRs using Blockchain technology to prevent the Ransomware attack probability.
3. To build a new smart contract algorithm that can detect Ransomware at the initial stage.
4. To develop data recovery methods in case of post-error conditions.
5. To validate and evaluate the proposed system based on several metrics: cost, immutability, data storage, estimated, and recovery time.

1.6 Scope of Research

The scope of this study includes the implementation using the smart contract that will be written in the Solidity language to be published on one of

the Ethereum networks. Three cases have been highlighted; the first case, prevent any attempt to attack patients' records from outside the network. In the second case, prevent any attempt to attack patients' records from inside the network. The third case is where one of the network nodes is failure or assuming hacked by a Ransomware attacker.

1.7 Major Contribution of this Thesis

The major contributions of this thesis are listed below:

1. Developing a smart contract algorithm to protect patient healthcare records using Blockchain technology.
2. Increasing the security of the MHR by preventing the outside and inside attacker from transmitting a hyperlink infected with Ransomware using privet Ethereum Blockchain network-based smart contracts.
3. Designing a backup model in case any node included in the Blockchain network cannot transmit its transactions for any damage. This may be done by employing two methods of data retrieval.

    a) The First Method: Retrieve a copy of the lost data from one of the nodes at random.
    b) The second method: Retrieve a copy of the lost data from the nearest node, depending on the shortest path between the failed node and the rest of the node.

1.8 Research Plan

In this Section, a general view of our research plan has been illustrated in Figure (1.3).

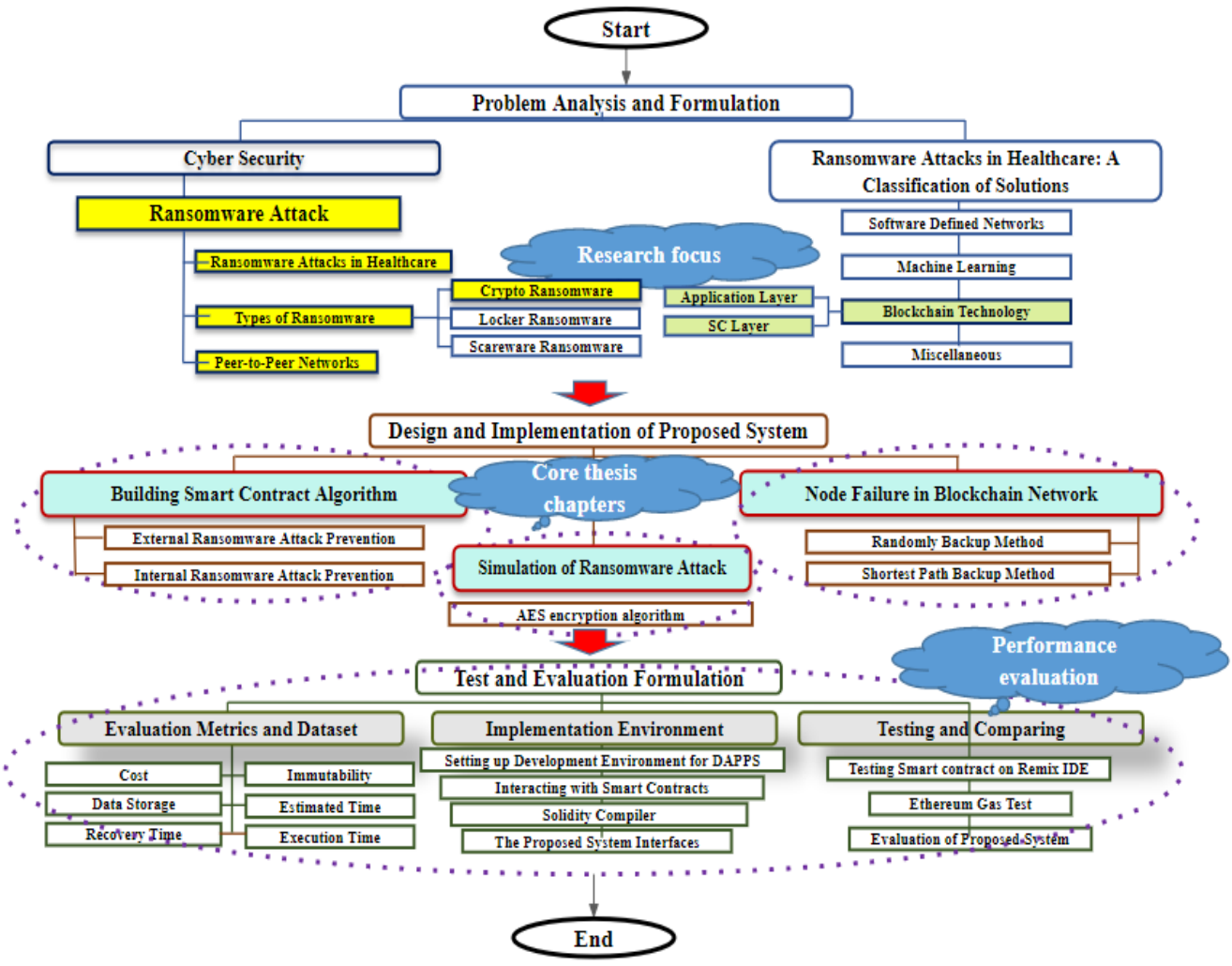


Figure 1.3 Research Plan

1.9 Thesis Outline

There are five chapters in the thesis. Each chapter starts with a short introduction that says what the chapter is about and what its main points are. The following is a summary of each chapter:

- **Chapter One:** gives a general overview of the research area. It shows the problems with this study and emphasizes how important the study is.
- **Chapter Two:** This chapter presents a review of the works of researchers

who investigated Blockchain, the Ethereum network, and the smart contract with the healthcare system.

- **Chapter Three:** The goal of this chapter is to explain and define all the algorithms listed in this thesis, then to have a widespread idea about the used algorithms and the ideas of all parts.
- **Chapter Four:** The objective of this chapter is to show and compare the different methods used in the thesis.
- **Chapter Five** :This explains what our research is about and to suggesting some thoughts to extend the current work.

2.1 Introduction

In the previous chapter, a general introduction to health care is given, and how important and sensitive patient data is in this field. Since the care is seen as a target for most types of cyber-security attacks, especially Ransomware attacks, some researcher's works have tried to find methods for preventing these attacks in healthcare. This chapter provides an overview of Blockchain technology, its structure, features, and its most important applications. It also explains that Ethereum is a programmable application for Blockchain, what an electronic healthcare record is and how it works with health systems. Finally, it provides an overview of the development tools of Ethereum that are used in the proposed application.

2.2 Medical Health Records Applications

Medical Health Records (MHRs) are the most crucial data source about how a patient's health is handled. Consistent recording by doctors, nurses, and other staff shows that health, planning, and treatment are monitored correctly. The first medical records were used to describe each process. In the past, only doctors kept records of their patients' medical histories, but now a far wider range of stakeholders contribute to these documents [24].

Individuals rely on their health records and documentation for a variety of reasons, including the protection of their privacy, verification of their health history, and the resolution of any disputes that may arise as a result of their civil or legal interactions. MHRs applications include two basic classifications: electronic health records and remote patient monitoring [25].

2.2.1 Electronic Health Records

Electronic Health Records (EHRs) are long-term electronic records of a patient's health information coming from one or more care experiences in any setting. This information includes the patient's demographics, progress notes, complaints, prescriptions, vital signs, past medical history, immunizations, lab results, and radiology reports [8]. Creating, expanding, and connecting EHR systems are essential goals of highly developed health systems. The use of EHR technology comes with a slew of advantages. Electronic patient data storage and transmission can minimize clinical errors, enhance patient safety, and enable clinicians to communicate more rapidly and accurately, moreover, identifying relevant data more easily. Figure 2.1 shows examples of EHR.

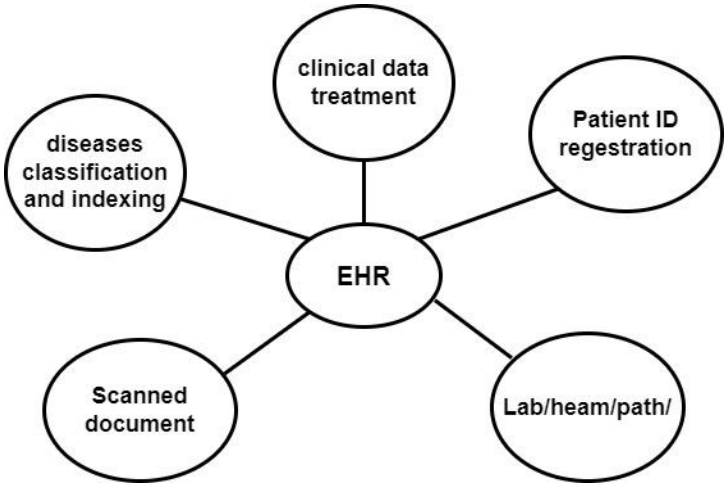


Figure 2.1 Examples of Electronic Health Record [26]

Well-designed EHR programs will improve effectiveness, reduce waste and duplication, and improve the cost-effectiveness of healthcare services. EHR systems will also make information more accessible to patients and give them more control over their health history, allowing them to take a more active role in their self-care. Furthermore, electronic health information databases can be used for various other purposes [27]. For example, provide direct care, such as clinical auditing and research.

2.2.2 Remote Patient Monitoring

RPM refers to Remote Patient Monitoring, also called telemonitoring, in which a patient sends health information to a care provider (sometimes through a data processing service) safely and securely, sometimes outside a traditional care setting. Remote patient monitoring devices obtain data about a patient's health. Electrocardiogram (ECG), Electroencephalogram (EEG), heart rate and breathing, oxygen volume in blood or pulse oximetry, nervous system signals, blood pressure, body/skin temperature, and blood glucose are the most common types of information. In some cases, the patient's weight, activity level, and sleep amount are also considered [27] [28]

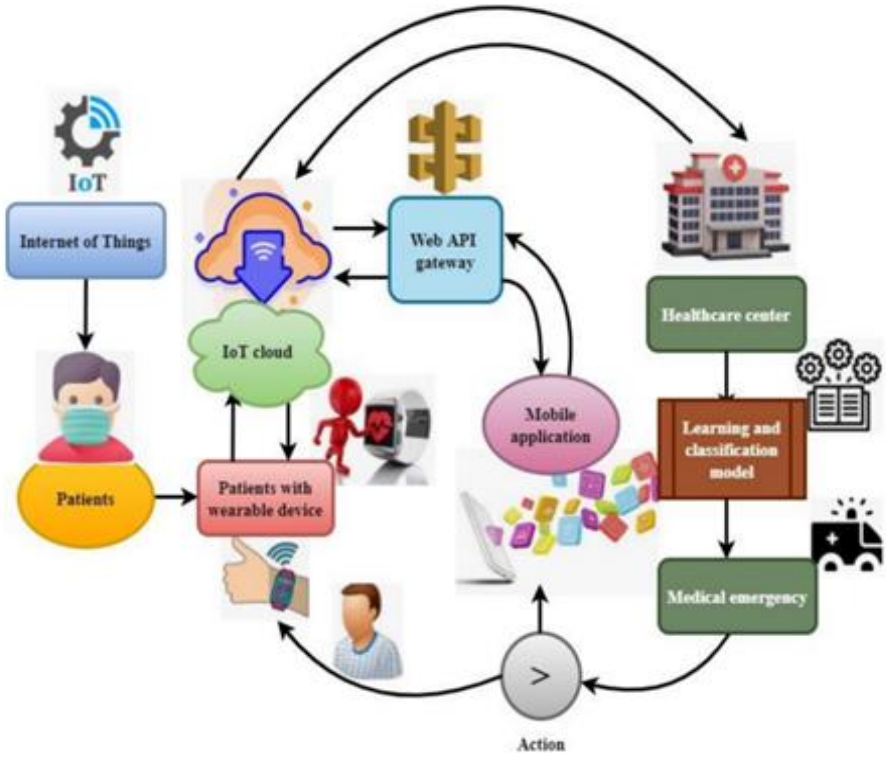


Figure 2.2 Remote Patient Monitoring [11]

2.3 Healthcare Application Issues

This section presents the issues facing healthcare systems in the current central environment.

2.3.1 Data Management Issue

Data has become an important part of all business operations, but managing data for healthcare is still the most important. By identifying the three main challenges in managing healthcare risks, it can give a big picture about the ability to identify accurate strategies to reduce them and finally make hospitals and patients safer [29]

2.3.2 Data Storage Issue

With the rate of data explosion, organizations and enterprises' storage systems are experiencing enormous issues from massive amounts of data and the ever-increasing amount of generated data [30]. Big data has the benefit of predicting future health issues, but it also carries a significant risk: doctors will be replaced. Big data cannot yet be exploited without human intervention, although this is a concern. If its use grows, patients will stop going to doctors and instead turn to technology, undermining doctors' authority. In the case of healthcare, big data cannot be ruled out since more and more institutions and organizations invest in this rapidly growing industry. However, one must consider its flaws to create a safe technique for doctors and patients [31].

2.3.3 Healthcare Security Issue

The United Nations described health security for the first time in 1994. Many references after that have used the term "health security" to describe health problems that directly impact human security. Public health security, global health security, international health security, and global public health security are all commonly used [19]. Although information security is a top priority for all organizations, healthcare providers must be vigilant in protecting sensitive patient information. Government regulations, such as the US Health

Insurance Portability and Accountability Act (HIPAA), create privacy protections for protected health information, in addition to the emerging threat posed by hackers and other intruders. The development of a network firewall alone is inadequate. Instead, providers must take a holistic approach to safeguard patient data at all points of entry, both within and outside the network. Healthcare organizations are becoming more vulnerable to nontraditional attacks as they rely on networks for their core operations [32].

2.4 Cyber Security

According to the National Institute of Standards and Technology (NIST), cyber security is the ability to protect or defend the use of cyberspace from cyber-attacks[10],which mean any form of malicious activity that occurs over the internet and targets people who are not taking adequate precautions to protect their personal information (cyber stalking or inside man, etc.). MHRs industry has been facing many cyber-attack problems, such as malware attacks, Distributed Denial-of-Service (DDoS) attacks [33], and so on, which have led to identity theft and data manipulation by people who should not have access to it[33]. As shown in Figure 2.3, the most common types of cyber-security are:

- **Botnet Attack:** The Mirai botnet attack was a DDoS attack that employed tens of millions of insecure Internet of Things (IoT) devices to knock out service for major ISPs [33].
- **Advanced Persistent Threat (APT):** It is a complex set of continuous, stealthy computer hacking processes done by a person or group of people after a specific entity. The goal of an APT attack is to steal high-value information from businesses and government agencies, like those in the manufacturing, financial, and national defense industries.

- **Side-channel Attack (SCA):** This type of attack is hard to stop with traditional methods because they take advantage of the flaws in IoT devices and only depends on the manufacturer's ability to predict flaws in their system.
- **Denial of Service Attack (DDos):** an attempt to stop a computer system or network from giving its intended user access to its computing resources.
- **Data Identity Theft:** This attack leads to leaks of private information and information about how people act, turning the hacked device into spyware.
- **Ransomware Attack:** Ransomware is one of the most dangerous things that can happen online, and it can cause companies to lose so much money. People are willing to pay the amount they asked to get their private information back, so it is becoming the most successful cyber-attack. The most significant types that impact the (MHRs) are WannaCry, CryptoLocker, CryptoWall, Petya, Locky, and TeslaCrypt [34].

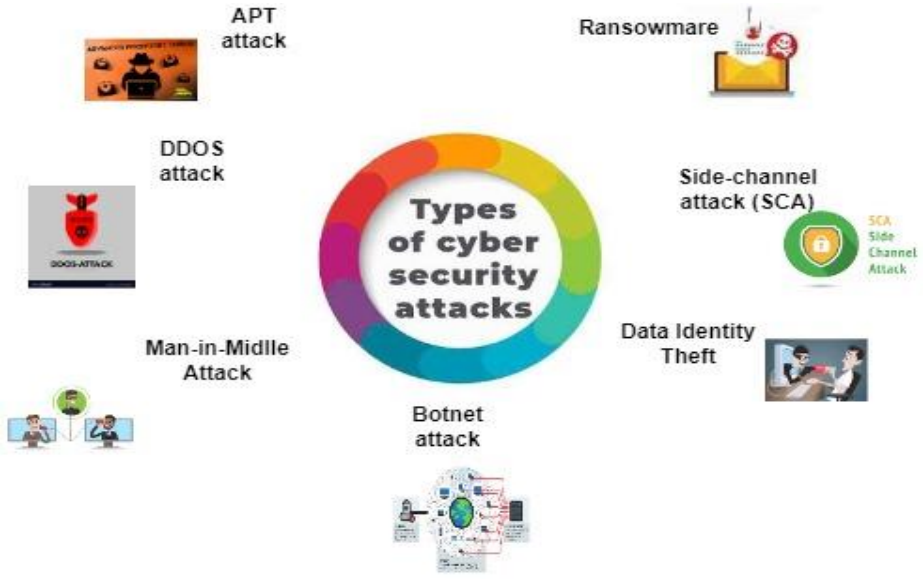


Figure 2.3 Types of Cyber Security

2.5 Ransomware Attack

Ransomware is a type of malware that is especially bad. It has become very common and is causing many troubles for businesses and individuals [4]. Ransomware can attack a person's hardware by locking their screens, which stops them from using their system and forces them to pay a ransom to get their hardware back. It can also break into a user's files, encrypt them, and demand a ransom from the user to get the files back. Most of the time, the ransom is paid in Bitcoins or another crypto currency. As a result, Ransomware is boosting business by a huge amount.

2.5.1 How Ransomware Works

The steps a Ransomware attacker holds to attack a patient using email are as follows [4]:

In this attack, the hacker contacts the victim via email. The intended recipient receives an email that appears to come from a trusted source, like a manager, and contains a malicious link or zip file. The user is taken to what looks to be an authentic website when they click the URL. When the web page is loaded, the server abuses the package that initiates communication with the target device. The toolkit attempts to take advantage of the vulnerability once a version has been accepted. It repeats the steps from this shield, like making a backup copy, to eliminate any shadows that can be used on the victim's computer and make new ones to cover them up. The binary runs a PowerShell script that can be run to make copies of itself and spread them through the file system.

The powershell.exe process makes three copies of the original malware binary. The first copy is in the AppData directory, the second is in the Start directory, and the third is in the C directory. The malware sends the encrypted

key and the rest of the information about the host to the server that controls the malware. The server then sends a note to the victim asking for a ransom.

2.5.2 Types of Ransomware

Symantec, a computer security company, thinks that Ransomware makes people pay millions of dollars every year. However, it also argues that if a ransom is paid, there is no guarantee that the encrypted file will be sent back to the person who paid it [35]. According to [35], there are mostly three different kinds of Ransomware (see Figure 2.4).

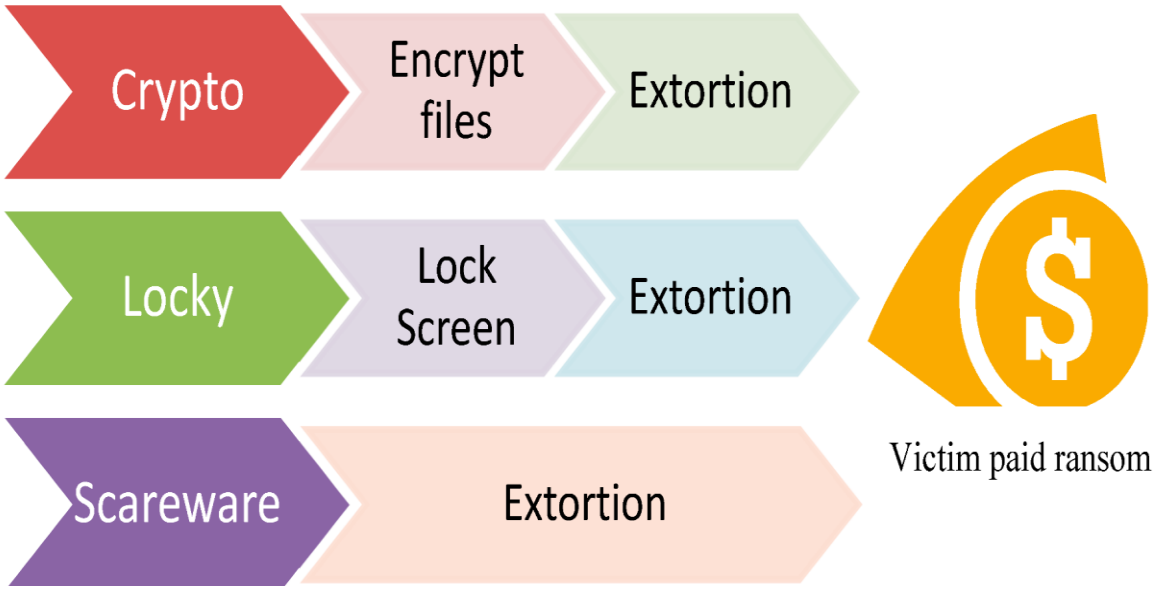


Figure 2.4 Types of Ransomware [36]

2.5.2.1 Crypto Ransomware

Recently, the focus of Ransomware attacks has changed more toward crypto Ransomware. Crypto-Ransomware is becoming more common because it encrypts files and threatens to delete them if a ransom is not paid. The encrypted files cannot be opened even after the malware has been removed. When sensitive files are lost and there is no backup, Ransom demands may be paid by the victim [34].

2.5.2.2 Locker Ransomware

This type of Ransomware locks the victim's computer by showing them a post where they need to log in. The hacked person will have to pay a ransom to get the password that will let them get into the system again. Locker-Ransomware is not very dangerous because most attacks can be stopped by restarting the computer in safe mode [4][36].

2.5.2.3 Scareware Ransomware

Scareware is one type of Ransomware. This kind of Ransomware does not hurt the person who gets it. Its main goal is to make the person scared enough to pay the ransom. Scareware works by pretending to be an authority that has found that the victim did something wrong. To avoid legal repercussions, it will seek a ransom payment. Another kind of Scareware threatens to tell the victim's family and friends about the wrongdoing; it is also called leakware [36].

2.5.3 Common Encryption Algorithms Deployed by Ransomware

In this section, two types of encryption algorithms will be described, which are Advanced Encryption Symmetric (AES) and Rivest-Shamir-Adleman (RSA) Encryption Algorithm.

2.5.3.1 Advanced Encryption Symmetric Algorithm

The Advanced Encryption Symmetric (AES) is an algorithm for encrypting and decrypting information files, text and documents. Specifically, the symmetric-key block cypher technique is used for encryption and decryption. Also, the AES algorithm uses different encryption keys to encrypt data, such as ones with 128, 196, or 256 bits, to encrypt data [37], as shown in Figure 2.5.

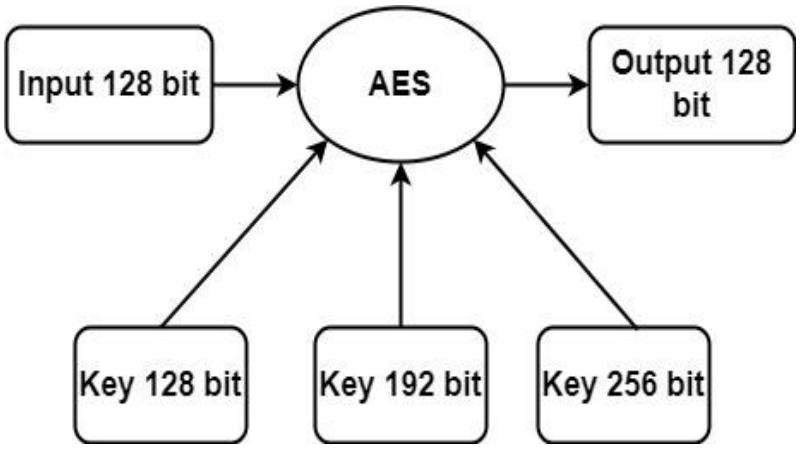


Figure 2.5 AES Encryption Keys

The AES works with blocks of data that have 128 bits. This is because the input block, the output block, and the State all have the same length, 128 bits. Therefore, the algorithm can both encrypt and decrypt blocks using secret keys. Key lengths can be 128 bits, 192 bits, or 256 bits. The AES comprises the first Round Key Addition, the first Nr-1 Rounds, and the last Round [38].

2.5.3.2 Rivest-Shamir-Adleman Algorithm

RSA refer to Rivest-Shamir-Adleman encryption. It is an example of asymmetric cryptography, where a public key is used for encryption, and a private key is used for decryption [37]. RSA cryptography has many benefits, some of which are privacy, integrity, validity, and the fact that it cannot be changed. Many programs use the Internet to send encrypted messages and data that are meant to be kept secret[38][39] **.**

2.6 Blockchain Technology

The Blockchain is a distributed database that stores all data securely, transparently and verifiable**.** Blockchain is a digital transaction arranged in chunks of data called blocks; it is linked by chain via a cryptographic validation called hashing function that forms an unbroken chain. A Cryptographic Hash

Function (CHF) of the previous block is included in each new block, as shown in Figure 2.6 [40]. Blockchain is programmed not only to record financial transactions but also for everything that has value. Blockchain is also called Distributed Ledger [41]. The most popular Blockchain implementation is the Bitcoin (BTC) to handle crypto-currency that was proposed in 2008 by Satoshi Nakamoto [42].

Figure 2.6 Create Chain in Blockchain [42]

Blockchain operates in a P2P network, meaning each node in the network has a full copy of the information. No single node can control the network, thus removing the central authority over this database [43]. The P2P architecture of Blockchain technology increases the toleration of error. Even if some peers are removed from the network, they still work in a normal way. Furthermore, since blocks cannot be changed without changing the complete chain of blocks, it makes the system more flexible and increases the difficulty for the attacker [44]. Modern researches exhibit that Blockchain technology is an efficient solution for issues such as unsecured data storage, high cost, and low efficiency [45]. Bitcoin, Ethereum, and Hyperledger Fabric are just a few of the most well-known and representative Blockchain platforms[45].

2.6.1 Components of Blockchain Structure

The Blockchain system generally consists of a number of peers, each owning a local duplicate of a distributed ledger. These nodes do not need a central authority to confirm and coordinate transactions. However, they communicate with each other to obtain an agreement on the content of the ledger [46]. A block header and the body header make up the block (see Figure 2.7).

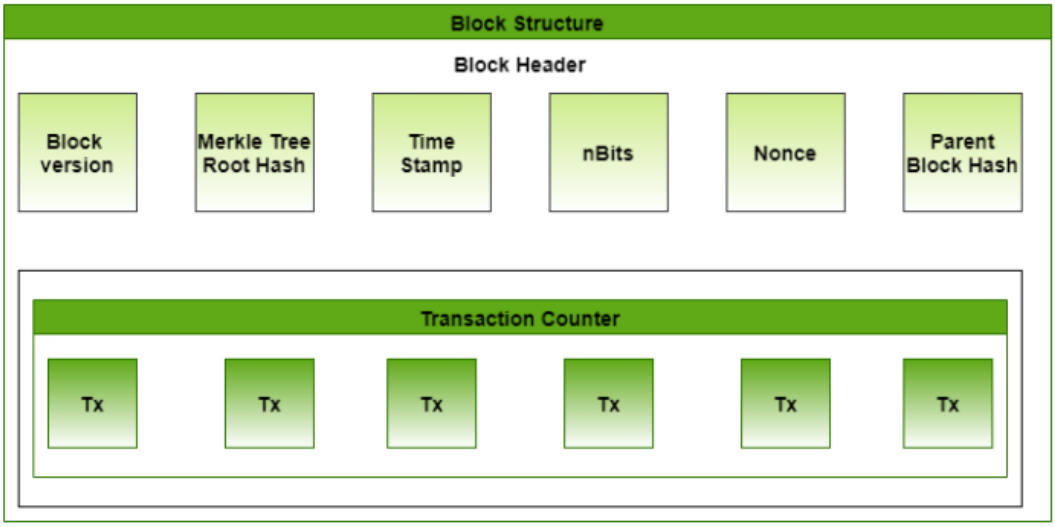


Figure 2.7 Block Structure [47]

The most important components are explained as follows:

1) **Transaction:** In Blockchain, the transaction represents the procedure the user launched on the network. It could be recording information that a Blockchain-based system deals with [48].
2) **Block:** is the set of valid transactions and other details. In the Blockchain, any peer can initiate a transaction and broadcast it to all peers in the network. Network peers validate the transaction using the old transactions, the moment that the transaction is validated next step is added to the existing Blockchain. It can be divided into two parts, block

header and block data [49]. It is worth noting that each Blockchain can define its block fields; Many Blockchain s contain the following fields:

A. **Block Header:** The Blockchain comprises blocks, each of which has a complete record of all the transactions that have ever occurred in that particular block. A block has just one parent if its header includes a hash of the block before it. The first block in a Blockchain is called the genesis block, and it does not have any parents. These fields of the Block header are summarized as follows:
   - ✓ The block number: It represents the block's sequence in the Blockchain.
   - ✓ The previous hash block: The Blockchain system uses the previous hash to create the new block's hash, making the Blockchain tamperproof.
   - ✓ The current hash block can be accomplished in various ways using the hash of the fully integrated block information.
   - ✓ A timestamp is a recorded unit of information that records the order in which transactions occur in blocks, given by time reference.
   - ✓ The block size: which determined by protocol rules applied in each Blockchain.

B. **Block Data:** These fields of the Block Data are summarized as follows:
   - ✓ A list of transactions.
   - ✓ The number of transactions.
   - ✓ The number of validated transactions in each block.

- ✓ After validation, the block is distributed to all participants in the network. The first block in any Blockchain is called a Genesis Block [47].

3) **Mining:** is the process of appending a new block (transactions) to the Blockchain. The Blockchain relies on the miners (specific nodes in a network) to aggregate valid transactions into blocks and append them to the Blockchain. New blocks are broadcast across the entire network, so each node contains an exact copy of the entire data structure [47][49].
4) **The Consensus Algorithm:** is used in the Blockchain to solve the problem of guaranteeing data consistency in various failure peers in a distributed system. Consensus mechanisms allow distributed systems to work together and stay secure. There are several consensus mechanisms used in different Blockchain networks. The most famous of them is Proof of Work (PoW) is adopted in Bitcoin, and Proof of Stake (PoS) is adopted in Ethereum. The main advantage of PoS over a PoW is that PoS uses much less electricity to run and is thus more cost-effective [50].

2.6.2 Layers of Blockchain Technology

Blockchain architecture generally consists of six-layer [47][51][52]:

- **Data Layer:** This layer specifies the essential structure of data, including digital activities, blocks, and cryptographic keys, arranges them into Blockchain s, transaction pools, and wallets, and manages a wide range of data functions (read/write/cache/encrypt/decrypt).
- **Network layer:** The technology of point-to-point transmission (P2P network technology is another name for peer-to-peer network technology), propagation mechanisms, and verification methods are the major components of this technology. Consensus techniques, encrypted

signatures, data storage, and other features are included. The network layer's main goal is to create a chain of information communication between nodes in a network.

- **Incentive layer:** The main purpose of the incentive layer, which combines economics with Blockchain technology, is to offer incentives to encourage other blocks to check the security of the Blockchain and to get people to help with the computing power.
- **Smart Contract Layer:** The contract layer encompasses a variety of script codes, algorithmic processes, and smart contracts that create regulated and auditable contract specifications. Smart contract flaws include a disordered exception, reentrancy, dependency on timestamps, reliance on block numbers, appeal for a damaging delegate, and freezing, to name a few. Hackers can easily exploit smart contracts owing to faults and weaknesses. A single trusted verifier or a group of trusted verifiers can confirm a smart contract. Smart contract development, on the other hand, lacks discipline and consistency. Program testing can be performed to discover the presence of bugs. However, it is unable to determine whether or not bugs exist. Given the financial nature of smart contracts, vulnerabilities or faults in their systems could have disastrous effects. On the other hand, smart contracts can benefit from the formalized process.
- **Consensus Layer:** The network maintainers of this layer validate digital activity and generate new blocks for system consensus. Consensus mechanisms fall into two categories when it comes to describing the trade-off between security and expense. Any entity can be a maintainer for permission less consensus. Permission less consensus can help to

promote network neutrality and democracy, but it can also add a lot of overhead.

- **Application layer:** This is the highest layer of the Blockchain which comprises its applications in various practical fields such as IoT, finance, AI, etc. The application layer, as the uppermost layer, provides clients and developers with trusted Application Programming Interfaces (API), as well as supports a variety of DAPPs such as ubiquitous access, edge services, and trusted intelligence.

2.6.3 Blockchain Consensus Layer Algorithms

In this section, the most famous Blockchain algorithms are explained. Then, compare them in terms of processing time and choose the best algorithm in the proposed system.

- **Proof of Work**

The combination of encryption and processing power in a Proof of Work (POW) algorithm establishes consensus and ensures the authenticity of data stored on the Blockchain. After proving the validity of a block, network nodes (known as miners) use their computational power to validate transactions (ensure that a sender has sufficient funds and is not engaging in double-spending) and, more significantly, compete in a race to solve the protocol's cryptographic challenges [53] [54].

- **Proof of Stake**

One of the most promising strategies for replacing (POW) while maintaining similar resilience qualities is Proof of Stake (POS). Despite the fact that (POW) necessitates the honesty of a (qualified) majority of computer power, (POS) assumes that honest participants control the majority of the money in the

system. Individuals with significant interests in the system have a financial motive to keep it working according to the protocol specifications because they risk losing their shares if the coin loses trust [55]. To accomplish the leader's election and maintain network consensus, (POS) uses virtual resources such as a node's stake. Because the mining resources are virtual, the POS-based consensus process is instantaneous and has no costs. However, some attacks that specifically target POS protocols using voting mechanisms are far-reaching [56].

- **Proof of Authority**

It is a permissioned Blockchain consensus algorithm family that has grown in popularity due to improved efficiency over traditional Byzantine Fault Tolerant (BFT) algorithms due to lighter message exchanges. Proof of Authority (PoA) was first proposed as part of the Ethereum ecosystem for private networks [57]. Because it permits different blocks to be appended to the same chain index, the standard Ethereum protocol based on (PoW) can fork. If not identified early enough, this forking condition can lead to security issues such as double-spending. Alternative protocols aimed at avoiding forks, known as PoA protocols, have recently been implemented into the most extensively deployed versions of Ethereum, parity. As a result, PoA has grown in popularity, and it is currently available from major SaaS providers and used on several Blockchain networks [58].

2.6.4 Blockchain Features

Blockchain provides a new model for securely storing information based on decentralization property. The major features can be summarized as follows [40] [59] [60]:

- **Decentralized Data Management:** Each user owns the authority to add data to the Blockchain; thus, no single user owns the system more than any other user.
- **Immutability:** Blockchain is a way to store information that cannot be changed or tampered with. A unique cryptographic hash is used to check the data in the Blockchain. The previous block's hash links the new block to the one before it. Even if changes are made to the block, the next block will still have the previous block's hash. So, the hacker must change all blocks to hide the change to one block.
- **Transparency:** Every information or transaction on the Blockchain is public, which allows each node in the Blockchain network to access all information or transactions without tampering with it; this makes the system transparent.
- **Disintermediation:** When middlemen like banks are taken out of transactions, costs and risks related to the existence of this middleman go down.
- **No Risk of Central Failure:** Usually, the central server stores the big data. However, users do not control their data. The decentralized storage of the Blockchain is not stored in one location, and that means keeping a copy of the data on every peer in the network.
- **Redundancy:** All Blockchain nodes keep a copy of the information on a P2P network. This means that a malicious action cannot change it (attacker). Therefore, if a hacker wants to change any information in a Blockchain, he or she has to make the same changes to all nodes in the network. This takes a lot of computing power.

2.6.6 Blockchain Classification Forms

Blockchain technology comes in many forms, but the most important ones are [61]:

- **Public Blockchain:** They are chains that anyone can join and have a say in what happens. In this type, no participant has a ledger because it is accessible to everyone. Instead, the instructors use a decision-making method called "distributed consensus" to keep a copy of the ledger on their contract.
- **Private Blockchain:** This kind is not available to everyone. Only a certain group of people can access it, and only those can see the ledger.
- **Semi-Private Blockchain:** Some parts of the network are controlled and run by a group, while others are available to anyone.

2.7 Peer-to-Peer Networks

Peer-to-peer (P2P) networks refer to the fact that nodes in a network are peers to one another, that they are all equal, and that all nodes share the responsibility of delivering network services such as file sharing and storage. The network nodes connect in a decentralized network with a “flat” topology. There is no controlling authority or centralized server within the network. The P2P networks are inherently resilient and open. This means th at any node in the network can send and receive data and that nodes can enter or leave a P2P network at any time [62]. One of the most fundamental ideas behind P2P technology is decentralization. Blockchain decentralized peer-to-peer structure makes it possible for different nodes in the Blockchain network to share information directly with each other [62]. The nodes, may perform a variety of functions.

It can do a lot of simple things such as accepting or refusing a transaction, transaction process, and simplifying communication [63] [64].In this thesis, hybrid P2P network has been used Hybrid P2P networks are a mix of structured and unstructured peer-to-peer networks. This is beneficial in networks where a central organizer is needed to coordinate the connections and interactions among nodes[65][66]. There are three types of P2P networks: Unstructured P2P Networks, Structured P2P Networks and Hybrid P2P Networks[64] [65].

2.7.3.1 Random Method

Many unstructured P2P and overlay networks are built on top of random graphs of varying types. The nodes in unstructured networks are not structured in any particular way. This indicates that contact between the nodes is random [62][67]. For message transmission, the nodes depend solely on adjacent nodes. Broadcasting (flooding) schemes are used in the search. It is ideal for applications that need a lot of interaction, such as social media networks. For the failure nodes, a random mechanism was used. For example, Parallel Spanning Tree Broadcast (PSTB) mechanism randomly selects a node from the core nodes as the backup node [68][63]. On the other hand, unstructured P2P networks need more network resources, which is why they are less scalable but have a higher degree of fault tolerance [69] [70].

2.7.3.2 Shortest Path Method

The shortest path between pair of nodes is the one in which the total weight of all edges is minimized. When a node in a network wants to communicate data, it uses the shortest path connection between those nodes, which will minimize the total cost of the path[71]. In particular, the global search (flooding) process is used when a node wants to find a new short route [72][73].

The initiator node uses a broadcast to notify all of its neighbors to determine the shortest route to the receiver node.

2.8 Ethereum

Ethereum is a public, open-source platform that runs on Blockchain technology and with smart contract functionality features. Ethereum is built as a Turing-complete scripting language. This is important due it needs to understand the agreements that allow for defining smart contracts. Ethereum is a programmable Blockchain. It allows anyone to build decentralized applications. Developers can use it to write code that controls digital assets and build any kind of application and not limited to crypto-currencies [42].

Ethereum owns a digital crypto-currency called Ether (ETH). ETH, like Bitcoin, has many of the same features. It can be sent through the internet immediately. ETH is uncontrolled by the government or company (it is decentralized). Users around the world use it to pay for services on the network [74].

2.8.1 Smart Contract

The smart contract (as shown in Figure 2.8) is a piece of program code that runs on the Blockchain. It is called a "contract" due to its codes that running on Ethereum can control valuable things (e.g. Ether or digital asset value). The contracts in the Blockchain are formatted in binary format in Ethereum Virtual Machine (EVM) bytecode, Ethereum smart contract written in Solidity that compiled into byte code using an EVM compiler and then uses Ethereum client to be uploaded on the Blockchain [75].

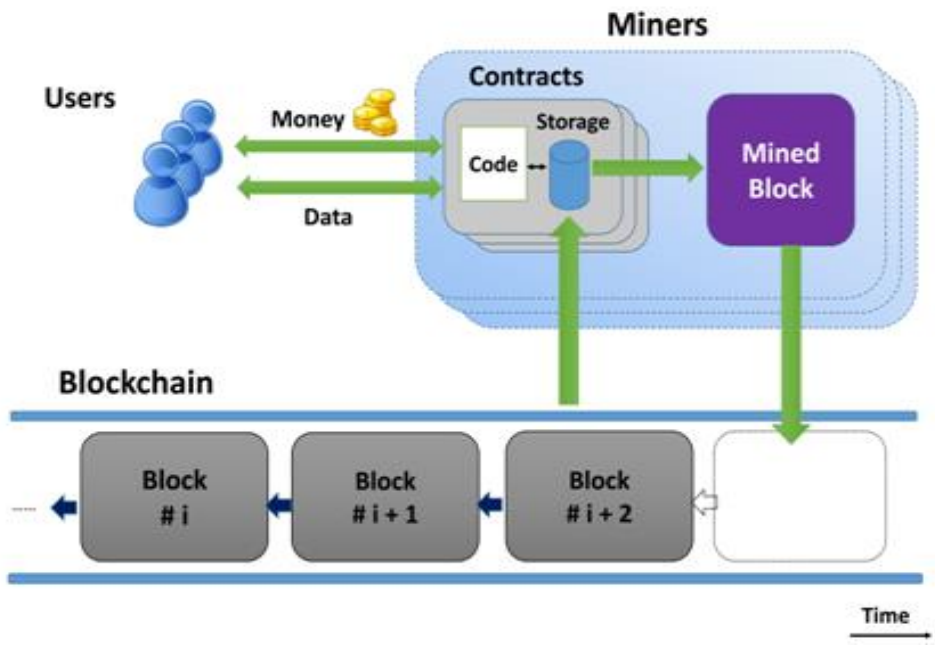


Figure 2.8 Smart Contract [76]

2.8.2 Ethereum Virtual Machine

The Ethereum Virtual Machine (EVM) is a part of Ethereum. It is considered with the runtime environment that deals with the deployment and execution of the smart contract. All peers in the network are running EVM and executing the same codes. EVM contains a stack-based structure. It is used to store values and contract program bytecode and includes several components: ROM, volatile memory, and permanent storage [77][78].

2.8.3 Solidity Language

Solidity language is a modern programming language for constructing EVM-compatible smart contract applications. The norms of networking, assembly code, and web programming are all combined in this modern language. Solidity is a high-level contract-oriented language similar to JavaScript. It allows you to write contracts and compile them into bytecode for EVM. At the moment, it is Ethereum official language. While it is the most

widely used language library for the EVM, it was not the first and is unlikely to be the last.SC written in Solidity may contain a function, function modifiers, state variables, struck types and events. Figure 3 is an example of SC written in solidity [79].

2.8.4 Ganache

Ganache is a personal Blockchain for the Ethereum platform. It can be considered an Ethereum client. That allows us to run the test locally, deploy smart contracts, and develop an application in a secure and deterministic environment without needing to connect to a real Blockchain. Ganache has two versions: Command-Line Interface (CLI) as a command-line tool and Graphical User Interface (GUI). Figure 2.9 shows the second version of GUI of Ganache [42].

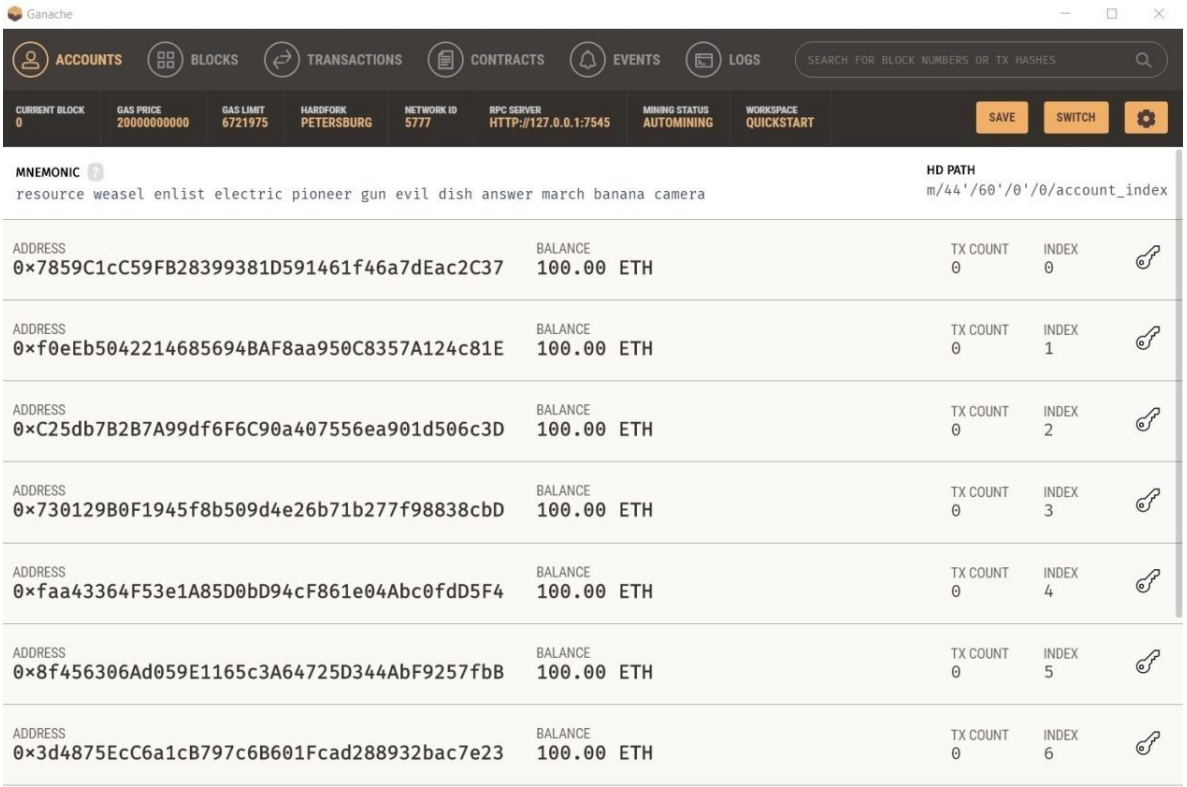


Figure 2.9 GUI of Ganache

2.8.5 Truffle

Truffle is a framework development environment for Ethereum, testing, and asset pipeline with Blockchain using EVM. Truffle makes life for Ethereum's developers easier [80], e.g., the developers can use Truffle to:

- Built smart contracts compilation, deploying, linking and binary management.
- Automated contracts testing for fast-developing.
- Network management for the deployment of any number of private and public networks.
- Interacting console for direct contract connection.
- An external script runner executes the script in a truffle environment.

The project structure consists of the following items:

- ✓ The contracts/: are solidity language files that include all smart contracts in the project.
- ✓ The migrations/: are JavaScript files that include scripts for deploying contracts to the Ethereum network.
- ✓ The test/: includes files for the testing application and smart contract.
- ✓ Truffle-config.js: is a JavaScript file that executes code to create the configuration file. The default configuration for the network, running on 127.0.0.1: 7545

2.8.5 Remix IDE

Building contracts in Solidity language using the online Remix IDE is the simplest method. It served as the Blockchain technology for medical devices. With the following restrictions, any user with an Ethereum account may publish a bounty in ETH. The remix is used as an IDE for SC implementation.

2.9 MetaMask

MetaMask is a browser extension that allows users to use the distributed web in the browser. It allows running Ethereum decentralized applications right in the browser. The regular web browser does not know how to connect to the Ethereum network and read && write to the Blockchain. MetaMask is a special browser that is able functions to make write and read requests to the Blockchain. As shown the Figure 2.10, by injecting a JavaScript library called Web3.js in the namespace of every page loaded in the browser An Investigation into Smart Contract Deployment on Ethereum Platform Using Web3.js and Solidity Using Blockchain [2]. To Connect MetaMask with Ganache, the RPC (Remote procedure code) Server address shows the endpoint link; this link will be used for the connections:

- In MetaMask wallet setting put http://127.0.0.1:7545 as a new RPC address.
- Select the new custom network.

MetaMask also allows the user to create and manage their own identity. Thus when dApps want to make a transaction and set data to the Blockchain, the user will get a secure interface to review the transaction before approving or rejecting it [81].

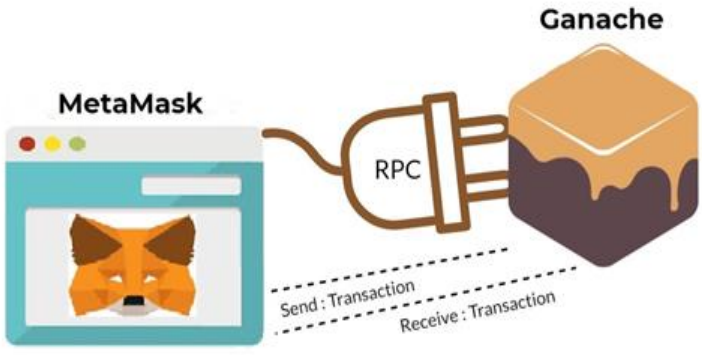


Figure 2.10 MetaMask and Personal Blockchain (Ganache) [81]

2.10 Web3.js

Web3.js is a set of built-in libraries that let users communicate to Ethereum nodes that are distant away or nearby. It is used by Node.js on the server side. Figure 2.17 shows that Web3 connects to the Ethereum network through an Ethereum node using an HTTP (Hypertext Transfer Protocol) connection. This could be a local system node for ETH wallets. MetaMask is a wallet for Ethereum that you can use in your browser. It links the browser to a Web3 provider class. A Web3 provider is a data structure that links to publicly accessible Ethereum nodes. With MetaMask, a user can use, save, and keep track of public and private keys that are unique to their account. Combining Ethereum, MetaMask, and web3.js with a web interface lets the back and front end talk to each other [82][42].

2.11 Performance Evaluation of Proposed System

This section presents the main interesting metrics and the dataset that employed to evaluate the proposed system. The Performance Evaluation is critical in checking the completed results for any study or research results. Therefore, choosing the right dataset and metrics is an essential key to differentiating in all performance evaluations.

2.11.1 Performance Metrics

In this study, the performance evaluation will be done using the same performance metrics which were employed by other studies in the related works. Thus, to be used multiple different metrics for validating the model of this thesis, such as cost and immutability, while the evaluation metrics are Recovery time, time estimated, Data storage and timely execution, giving us entire facts of how the proposed system will work.

2.11.1.1 Cost

To calculate the cost of Ethereum in relation to the dollar, you must know the following things [83]:

Gas: It is a unit that measures the amount of crypto currency required to execute each operation on Ethereum, as each operation on Ethereum, whether a smart contract instruction or a transaction, requires a certain amount of gas.

Gas Limit: The maximum amount of gas for all transactions created in the remix. We going to website (https://eth-converter.com/) to calculate the Ethereum. In Ganache the Default GAS Price =20000000000.

According to Equation 1, the cost can be calculated:

$Cost_{transaction} = Ether_{Wei} * Ether_{IQD}$ …….. (2.1)

Where $Ether_{Wei}$ is represented the value of Ether in Wei, and $Ether_{IQD}$ is represented the value of Ether in IQD.

According to the website:

https://thecoinacademy.co/blockchain/how-to-calculate-the-cost-of-an-ethereum-erc20-transaction-in-dollars/, the updating of the cost to both $Ether_{Wei}$ and $Ether_{IQD}$

$Ether_{Wei}$ = 10^18 Wei

$Ether_{IQD}$ = 2,689,379.68 IQD

Cost (1 Ether) =10^18 * 2,689,379.68

$Cost_{transaction}$ = 0.00000000000268937968 IQD

2.11.1.2 Immutability

Immutability, also defined as irreversibility, means transactions cannot be changed or removed after they have been successfully validated and registered on the Blockchain. The blocks are linked and combined with the hash of the genesis block, resulting in this property. Each block has been written

based on the block header by providing a hash of the data transaction in the previous block in its header. For all of the transactions in the block, Blockchain uses a Merkle tree to calculate this hash [84]. Increasing the immutability of the system depends on two main factors is the blocks number and the miner's number. This was demonstrated in the reference [85] by measuring a system that uses dual chain design, mixed chain Design, and Concurrent-Dual-Chain Design according to the equations below. In writing the equations, the work of Satoshi was relied upon, as Satoshi used the problem of destroying the gambler to find the probability of the attacker.

Equation of Mixed-Chain Design:

The immutability measure of MC based on Equation 2.2.

Immutability =1 - Pr (attack) ……..……. (2.2)

Where ***n*** is the number of miners, ***z*** represents the total number of blocks. Pr (attack) is the probability of attack [84] that an attacker can mine ***z*** blocks ahead of other miners, which is:

Pr (attack) = $(1/n)^z$ ……....…….(2.3)

Where n is the number of miners and z is the total number of blocks

So:

Immutability =1 - $(1/n)^{2z}$…….. (2.4)

Equation of Concurrent-Dual-Chain Design:

Immutability = 1 - Pr (attack) = 1-$(2/n)^{4z}$ …… (2.6)

As for the number of z-block and how to increase it, the proposed system uses a multi-peer distribution system, where the peers are distributed in different blocks instead of everyone being in one block. The number of blocks will be the same number of miners [84].

2.11.1.3 Data Storage

The data storage metric refers to the amount of data stored in the application database. Blockchain, storing and unlocking the power of data through a distributed means not just in one server, not just in the cloud controlled by one company, but by many nodes. The use of smart contracts will limit the amount and type of data stored on the Blockchain, reducing the rate of data inflation. Using Blockchain technology significantly reduced the size of files and solved the storage problem, freeing up less storage space. In addition, this procedure will speed up the knowledge of the patient's condition instead of observing normal and abnormal readings [86].

2.11.1.4 Estimated Time

Estimated time is the measure of time that an attacker needs to hack into a block in the Blockchain. If the attacker cannot hack the block on time, it will retry from the last created block instead of the specified honest miner. To calculate the estimated time, the equations mentioned in reference [77] are applied to the proposed system to prove the effectiveness of the system, which is shown below.

Estimated Time for the Standard System:

E (time Success) = $\boldsymbol{T} * (\boldsymbol{n})^{2z}$ ……..... (2.6)

Where $\boldsymbol{T}$: difficulty time for Ethereum =12s

$\boldsymbol{n}$: No. of miners.

$\boldsymbol{z}$: No. blocks

Estimated Time for the Proposed System:

E(time success) =$\boldsymbol{T} * (\boldsymbol{n}/2)^{4z}$ …… (2.7)

2.11.1.5 Recovery Time

This section evaluates and quantifies the performance of Blockchain connection when it recovers from a failure in the underlying network. On the collapse of the node, the Blockchain connection and transaction stream to the failed node is interrupted. Therefore, we can define the recovery time as the period from when the node in Blockchain synchronization lost blocks to the moment it resumes them [87].

2.11.1.6 Execution Time

The time for each set of transactions. The time required to implement the smart contract, the execution time, is the total amount of time (number of seconds) during which the Blockchain platform took to execute and confirms all transactions in the dataset [88] [89].

2.11.2 Dataset

In the proposed system, the dataset used contains a set of Tables. Each Table contains different data about the patient. The dataset is integrated into the patient health record database. The dataset's purpose is to apply the metrics defined for system evaluation and validation. Due to the suffering of choosing a dataset suitable to the proposed system format, as well as the lack of sources that talk about the use of the dataset with the Blockchain technology. In this research the dataset is used according to this link: https://figshare.com/articles/dataset/A_dataset_of_radarrecorded_heart_sounds_and_vital_signs_including_synchronised_reference_sensor_signals/9691544.

The dataset contains 11 patients' records for different periods of time, the dataset contains the records for set of patients, and those records are the result

of heart rate sensor readings, which were represented by symbols reflecting the patient's state, In our work, we provide protection for these records from the attempted Ransomware attack by dealing with this data in the form of a string and preventing any link from being sent, and this is what will be clarified in the chapter three. The dataset was also uploaded to MySQL so that the records could be read in sql format. Figure 2.11 shows the database (Electronic record), contains datasets.

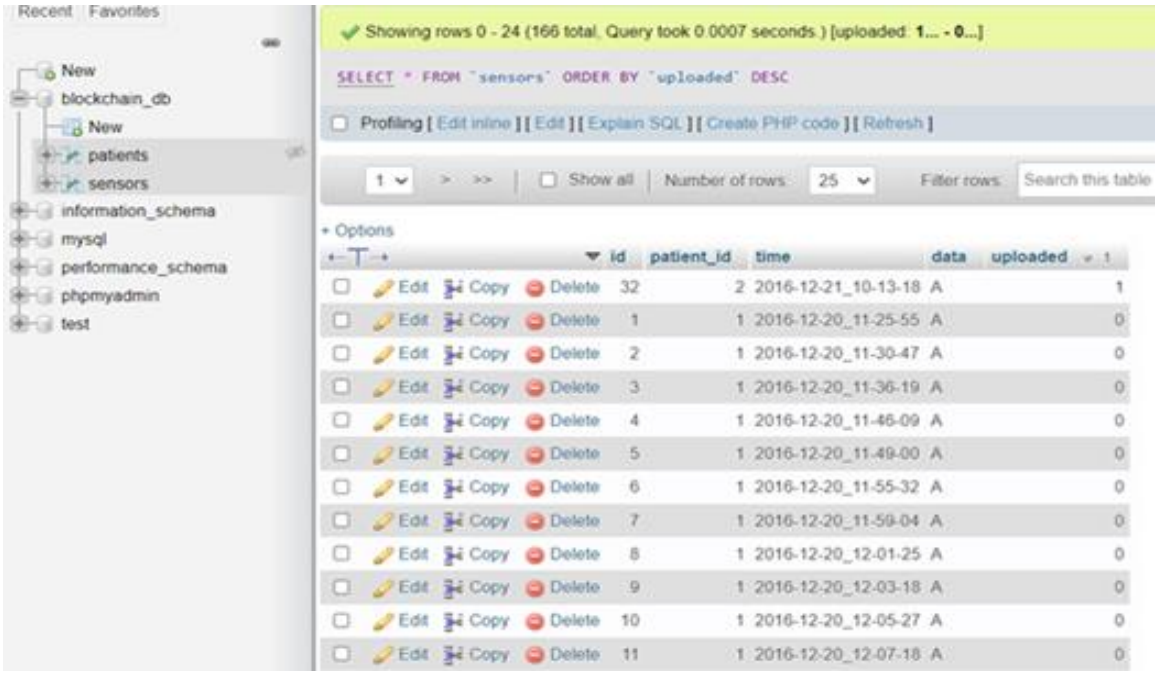


Figure 2.11 Database of Patients

3.1 Introduction

The previous chapter presented an overview of Blockchain technology, Ethereum, smart contracts, and all tools and environments used to implement the proposed model. This chapter presents an overview of the proposed model of the healthcare system that provides a unique privacy and security approach through a Blockchain framework and also describes the design of the proposed system in detail. Each part has a different function integrated to protect the data. A brief description of the steps of the research method and the system will be included in this chapter, the algorithms that use in our proposed system and Blockchain Ethereum environments and their tools.

3.2 The Proposed System

The research methodology of the thesis consists of several stages, including a preliminary plan for this research, a study of related works, a discussion of the techniques used against Ransomware as well as criticizing them, model design, and implementation, and the development of a simulation of one of the crypto-Ransomware attack types to understand the working environment of this assault and how to cope with it.

The proposed system focuses on Medical healthcare records protection. Blockchain technology is presented as a solution to privacy and security issues. Leveraging the distribution feature of Blockchain technology, a multi-peer distributed system has been created to distribute the data among multiple peers to protect patients' records from tampering. The methodology of protecting the patient's record, and protecting it from the attempted external or internal Ransomware attack on the Ethereum Blockchain network, is done by preparing algorithms programmed in the Solidity language in the smart contract.

Finally validation, and evaluation to check the performance of the works using specific metrics like cost, immutability, estimated time, data storage and recovery time, and finally, the reporting of the work. This section is described the high-level architectural design of the Healthcare system. The proposed system focuses on criteria that enable it to cover healthcare requirements, simplify the system, and make it more valuable and reliable for users. Figure 3.1 shows general view of our reaserch plan.

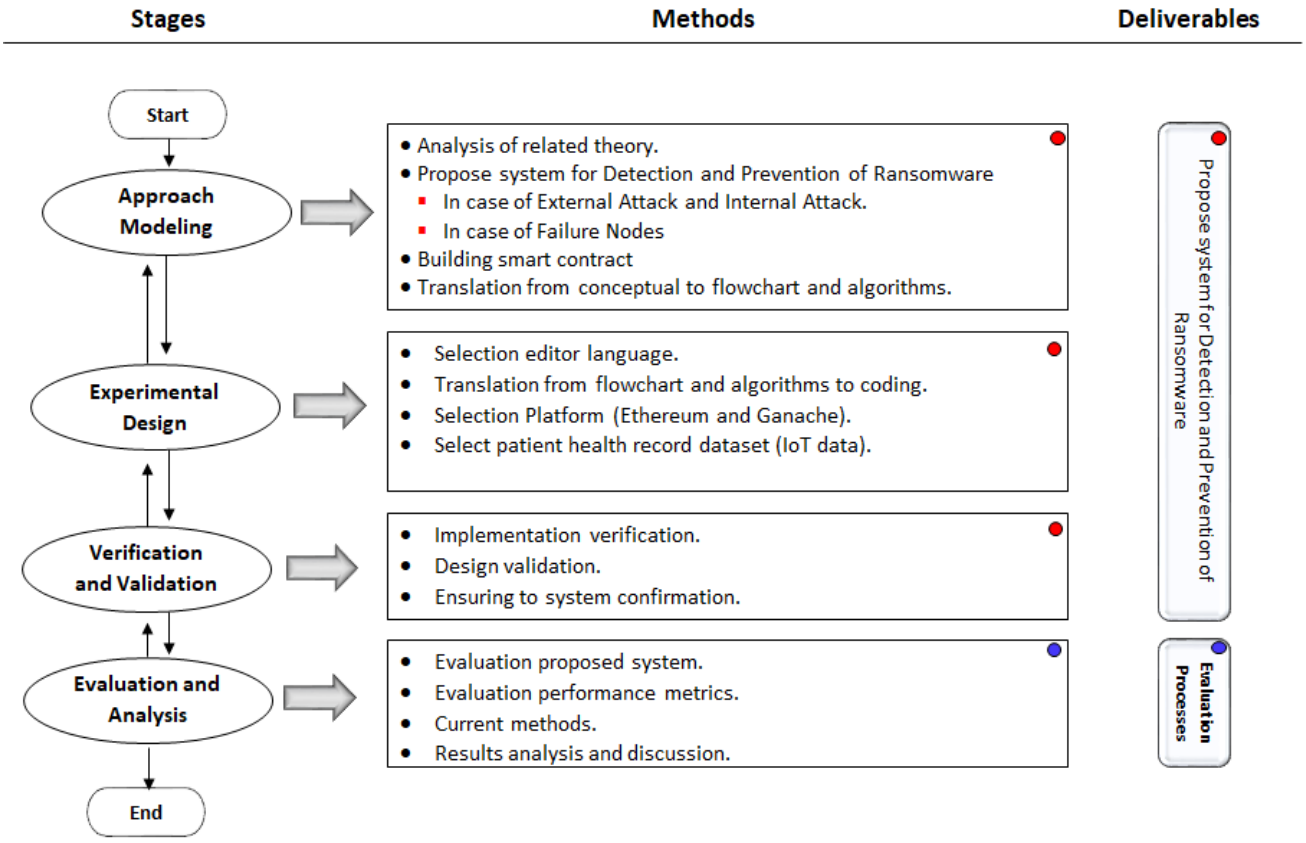


Figure 3.1 Block Diagram of Research Methodology and Proposed System

As illustrated in the Figure 3.2, the system steps start with receiving patient's record from the dataset:

1- The dataset contains the Patient's healthcare record collected from the IoT heart rate sensor. Then, it feeds the application fields for each patient, which consist of a set of records for each user.

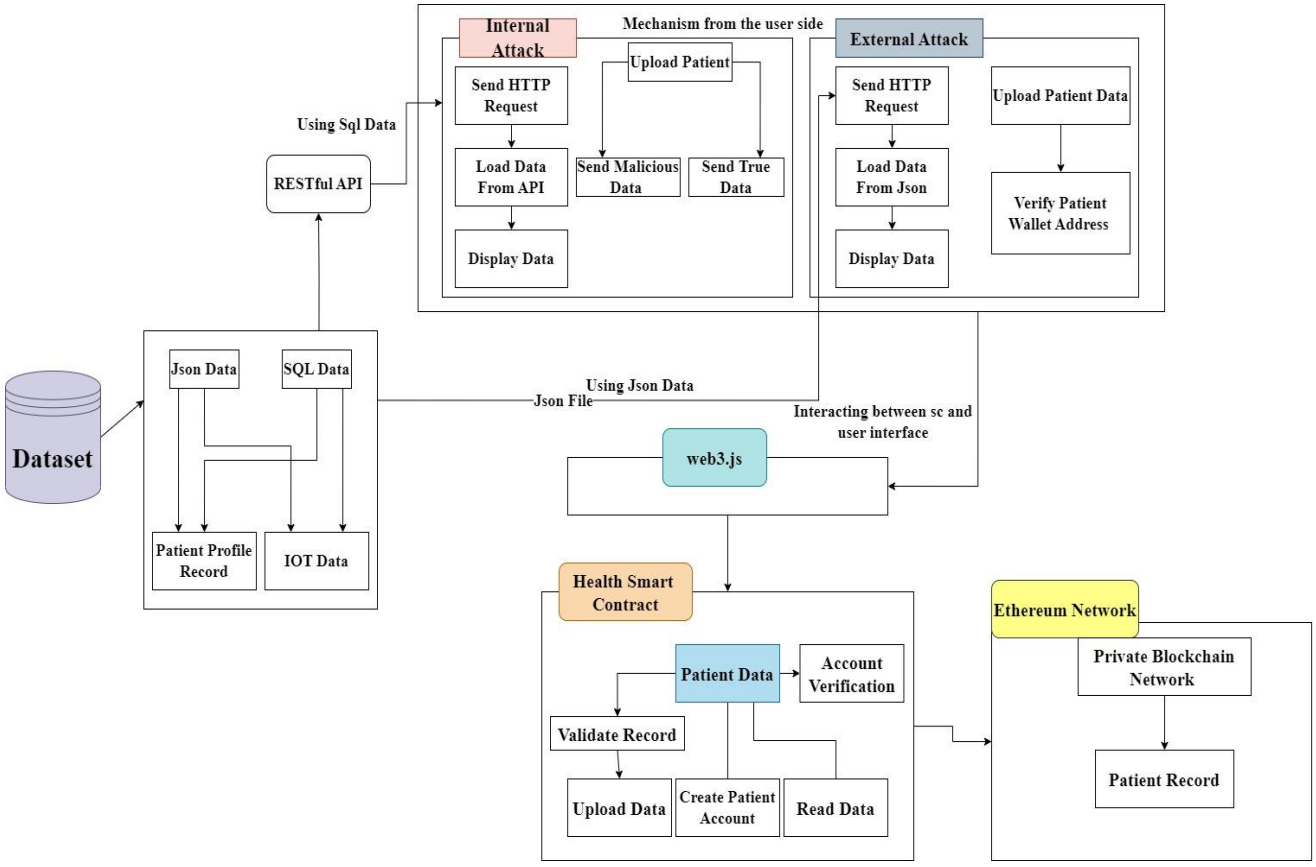


Figure 3.2 The Proposed System Block diagram

2- Next, the application reads the dataset to upload to the Smart Contract in two ways: JSON and SQL Data.

3- After that, it is sent to the smart contract for analysis of the data and sends it to private Ethereum networks according to the type of data in the form of a transaction.

4- The Ethereum network distributes the transaction's hash to each Patient's wallet (MetaMask Wallet).

5- Before sending the Transaction to the Ethereum network, the smart contract will check the validity of the transaction when the transmission is from outside or inside the network.

6- An algorithm for smart contract has been developed to handle the following cases:

- The first case includes: when a Ransomware attack tries to send the attack link from outside the network, the algorithm of smart contact checks the Ether address of the sender's wallet because the addresses of patients already known to the contract in the system are fixed. Any other external Ether address gets rejected.
- The second case includes: In this case, the Ransomware pretends to be one of the patients in the system and tries to send a transcription containing the attack link. Here, the smart contract algorithm checks the transaction metadata to see what kind of record was sent. Any Ransomware link is initially rejected. At the same time, the right transaction is accepted. The metadata transaction for that medical record will be processed. A portion of data called transaction metadata is appended to a transaction after it has been processed. Contracts provide metadata about record titles, access, and data integrity. The metadata owner, who is also the data set owner, can start giving, rejecting, or restricting access permission automatically through a smart contract.

7- After being processed by smart contract algorithms to protect the medical healthcare records from a Ransomware attack, the correct readings are sent to the Ethereum Blockchain network.

3.3 Simulation of Ransomware Attack

In this study, simulates the working environment of the Ransomware attack where it is closer to a type of encryption attack named TeslaCrypt use AES encryption algorithm. As shown below in the flowchart (see Figure 3.3), which encrypts as many files as possible using the 128-bit key length**.**

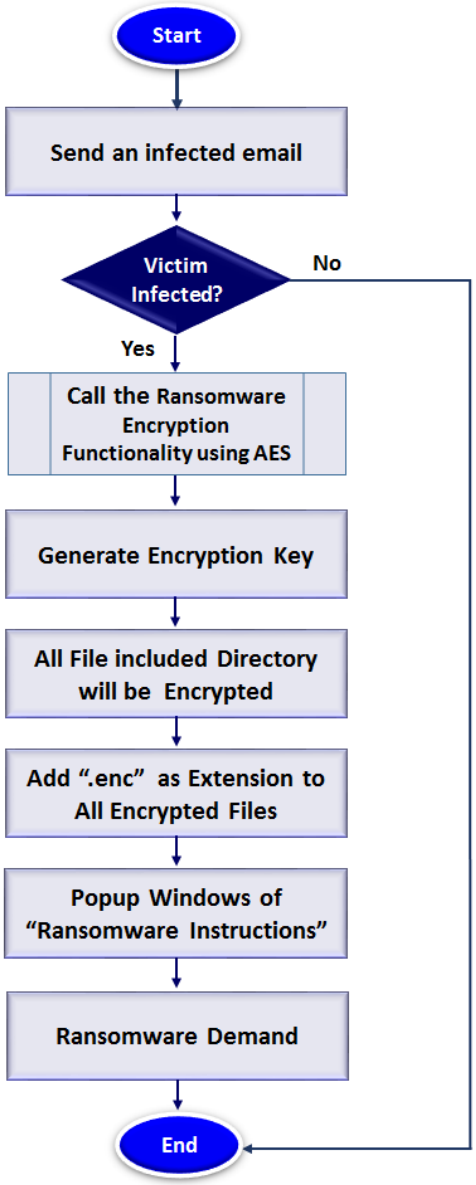


Figure 3.3 Flowchart Simulation of Ransomware Attack

The explanation of the simulated Ransomware attack consists of the following steps:

1- The Ransomware attack sends a Ransomware link via email to the victim; as the Ransomware does not work randomly, it identifies the victim that it wants to target because it's first and last purpose is to obtain the ransom.

2- The victim downloads the file, and malicious code can be executed secretly by hiding the Windows console of an executable file.

3- Generate the encryption key of the AES encryption algorithm and send it via email to keep it away from the victim; it also generates a random number for the victim's device.
4- AES encryption functionality encrypts all files inside the path where the attack executable is located and changes the file extension so that it is not open or readable.
5- Change the file extension to (.enc) or any other extension, to be unreadable format.
6- After the encryption process is completed, an interface will appear to the victim explaining that all files have been encrypted and that to retrieve them, he must pay a ransom and send it to an address placed by the attacker.

We noticed that the time takes the attacker execution to encrypt the files depends on the size of the files inside the Folder path.

3.3.1 External Ransomware Attack Prevention

To prevent an external attack, where the Ransomware attacker tries to send a transaction containing the Ransomware attack link to encrypt the patient medical record inside the systems, Figure 3.4 depicts an attempt by someone from outside the Blockchain network to join the network and send a transaction. The attacker takes a patient's identity to trick a doctor into thinking that message is a link to all of the patient's medical healthcare records and images using email phishing.

The proposed system uses a private Blockchain, and the smart contract checks any request based on the sender's Ether address. Because the smart contract preserves all of the Ether addresses of patients identifiable inside the network, it does not allow any new ether address to transmit any transaction, even if the person has a MetaMask wallet account.

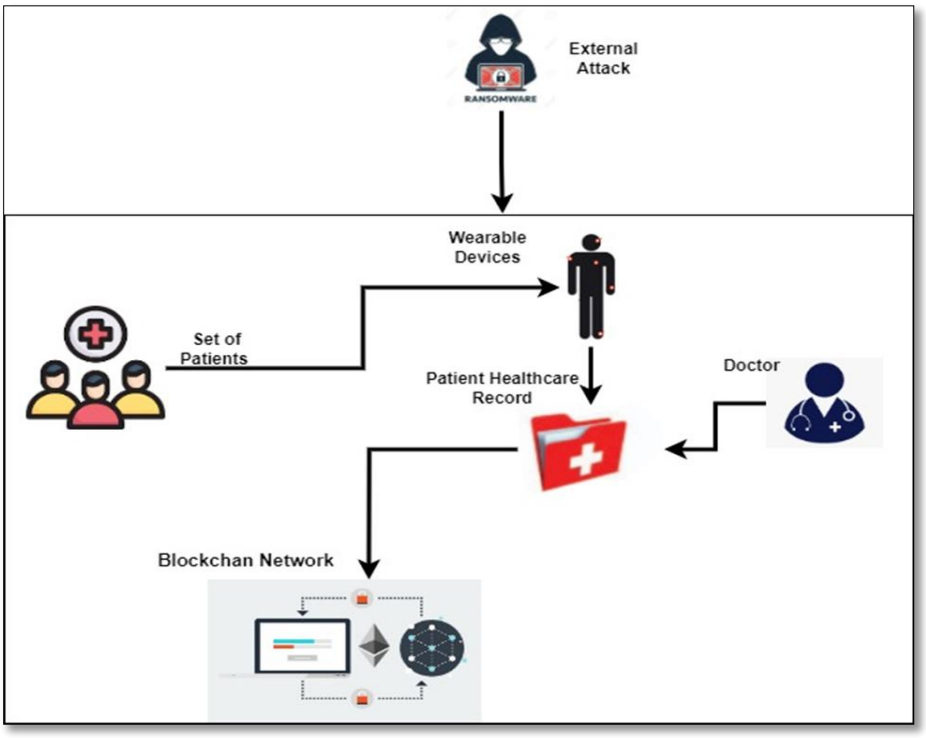


Figure 3.4 External Attack

All steps of the external attack algorithm are shown in the Flowchart (see Figure 3.5).

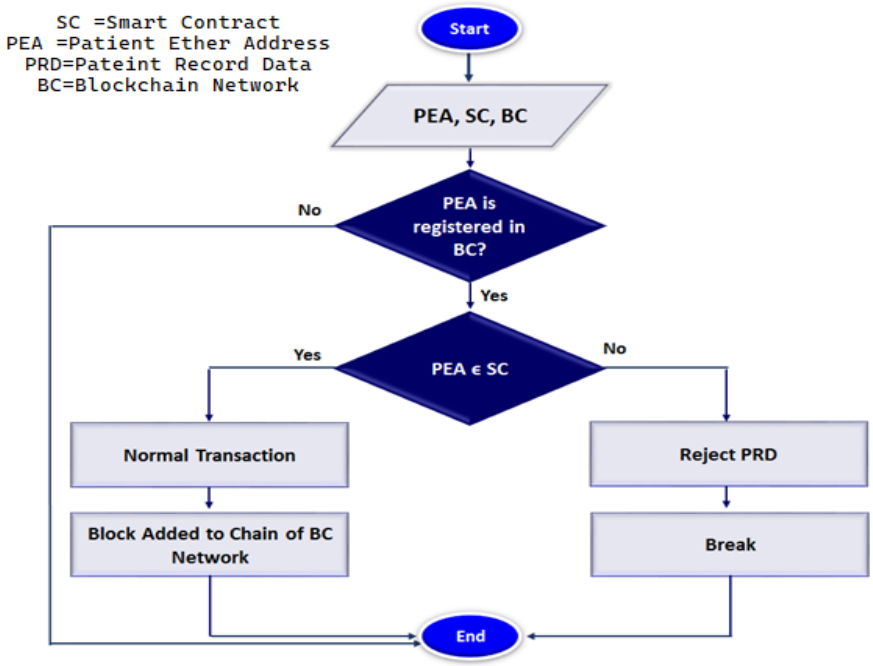


Figure 3.5 Flowchart of External Ransomware Attack

The main stage of the external attack:

1. Once the Medical healthcare record has been uploaded to the application, the smart contract will begin the verification process.
2. The smart contract will check the sender's Ether address to see if it's registered in the Blockchain network or not. All patient's Ether addresses in the private Blockchain network are well known.
3. If the smart contract knows the sender's Ether address, will start checking the validity of the requested transaction to see if it is empty or not.
4. After that, the transaction is confirmed.
5. Otherwise, the smart contract will prevent the requests.

3.3.2 Internal Ransomware Attack Prevention

An internal attack is defined as an attempt to attack the MHRs, by a trusted patient inside the network, as shown in Figure 3.6.

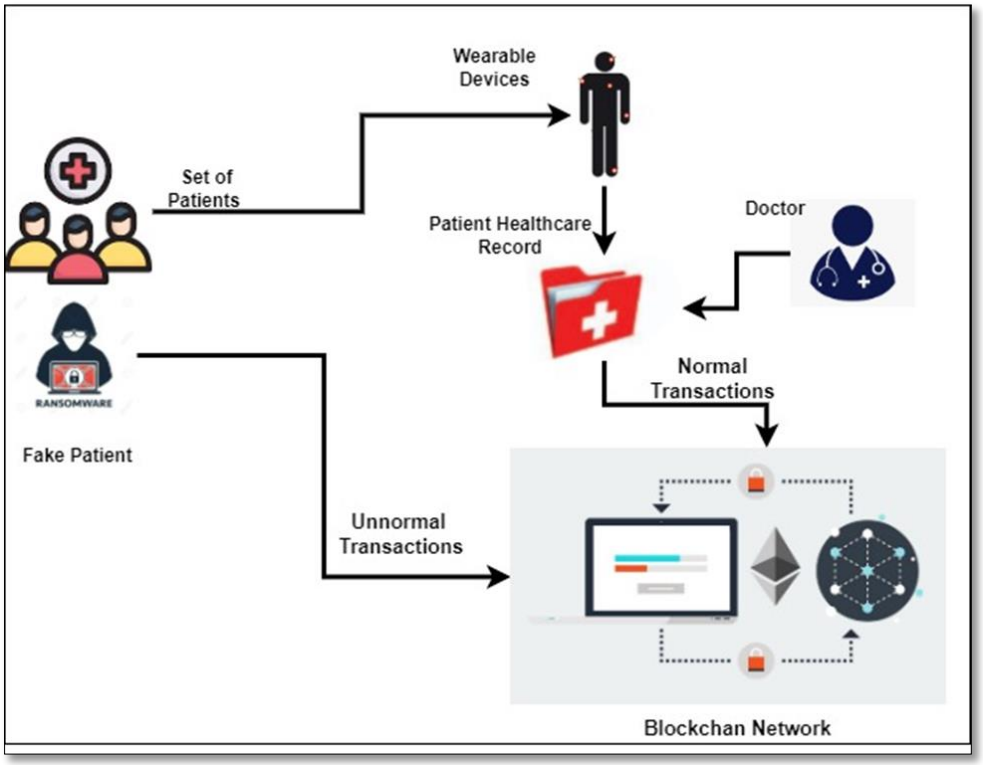


Figure 3.6 Internal Attack

To prevent the internal attack, the medical record's metadata (data of data) transaction will indeed be handled. The Smart Contract checks the content of the record, as the records of the dataset that was previously shown in the chapter two, contains only a string data, so when a patient send transaction contained a hyperlink , the SC will reject this transaction and block this patient and prevent him from sending any other transactions.

In Internal attack part, the XAMPP is used to upload patients' information as SQL data format so that it can be read based on the priority of each patient's health. The Flowchart 3.7 below shows each algorithm step.

The main stage of the internal attack:

1. Once the MHR has been uploaded to the application, the smart contract will begin the verification process.
2. The smart contract will check the sender's Ether address to see if it's registered in the Blockchain network or not. All patient's Ether addresses in the private Blockchain network are well known.
3. If the smart contract knows the sender's Ether address, it will start checking the validity of the requested transaction to see if it is empty or not.
4. Where patients are not allowed to send hyperlinks through the transactions. The smart contract rejects any transaction that contains a link. By checking the regular expression of the hyperlink.
5. If the transaction is correct, immediately, the smart contract will accept the transaction.
6. Otherwise, the smart contract will block all other records of that fake patient.

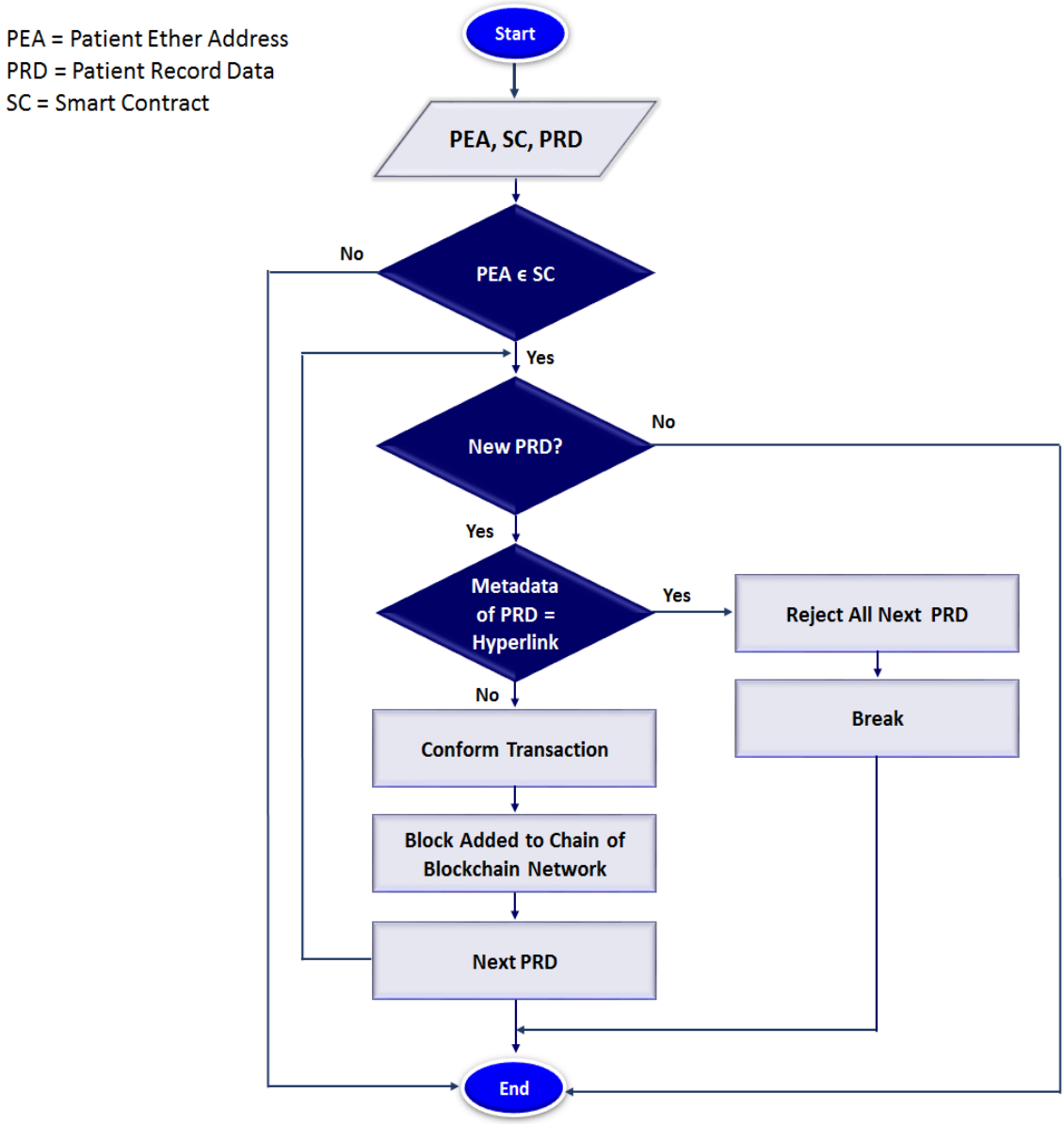


Figure 3.7 Flowchart of Internal Attack

Both external and internal cases use the Proof of Authority (PoA) conscience algorithm to validate the blocks.

3.6 Node Failure in Blockchain Network

In the third case, the worst-case scenario for the Blockchain network, when one of the nodes in the network stopped working, which was either the node

had not ability to send and received the transactions for any own properties or maybe Ransomware attacker was able to attack a transaction inside the node . Therefore, we designed a model that attempts to simulate the environments on a Blockchain network produced by several nodes and clients. This simulation was based on the Flask framework, the Pycharm editor, and the Python programming language. The simulation has two dashboards, one for the node and one for the client. These dashboards were built from scratch using HTML, CSS, and JS.

The features of the node in the simulation of Blockchain network:

- ✓ The capability of incorporating additional nodes into the Blockchain network.
- ✓ Using the Proof of Work (POW) algorithm.
- ✓ RSA encryption is used for transactions, the most used public-key cryptography algorithm.

The features of the client in the simulation of Blockchain network:

- ✓ Wallets are made using encryption with public and private keys (based on the RSA algorithm).
- ✓ Transactions with RSA encryption have been created.

As depicted in the above (Figure 3.8), the processes for establishing the Blockchain network are as follows:

1. All nodes are immediately notified of new transactions.
2. Each node collects new transactions into blocks.
3. Verifying the validity of the transactions using PoW algorithm.

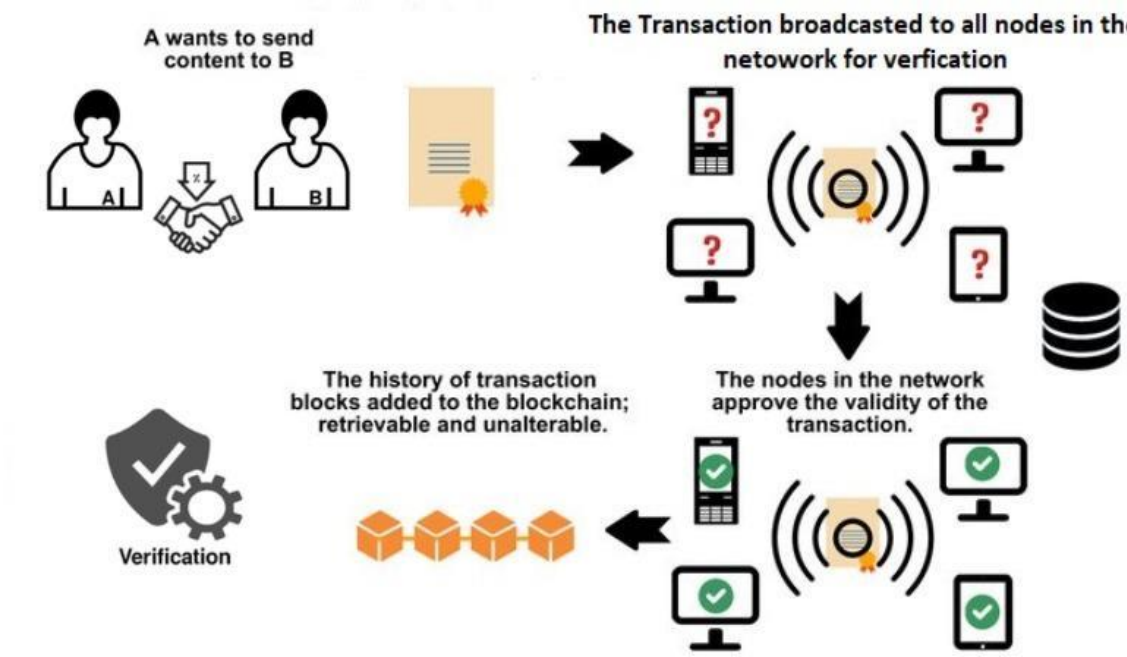


Figure 3.8 Simulation of Blockchain Network

For this purpose, two techniques have been employed to retrieve the data of a failed node whose own data has been damaged for any reason.

3.6.1 Randomly Backup Method

The first technique is the standard method of connecting nodes, the random method, in which nodes are connected at random, as illustrated in the flowchart (see Figure 3.9). When a failure occurs in one of the nodes, it sends an HTTP request to random connected nodes and backup of the lost transactions from the other connected nodes. As soon as it gets a copy of the backup, it will check the backup, if it is readable or not, and then restores its data completely.

The main steps of the random method:

1. When a node cannot read the transactions, either because of node failure or because a Ransomware attack encrypted it.

2. The failure node will send HTTP request to random neighbor-connected nodes in the network to get a backup of the Transaction.
3. Download the backup of transactions and back to work normally.
4. Otherwise, choose another node.

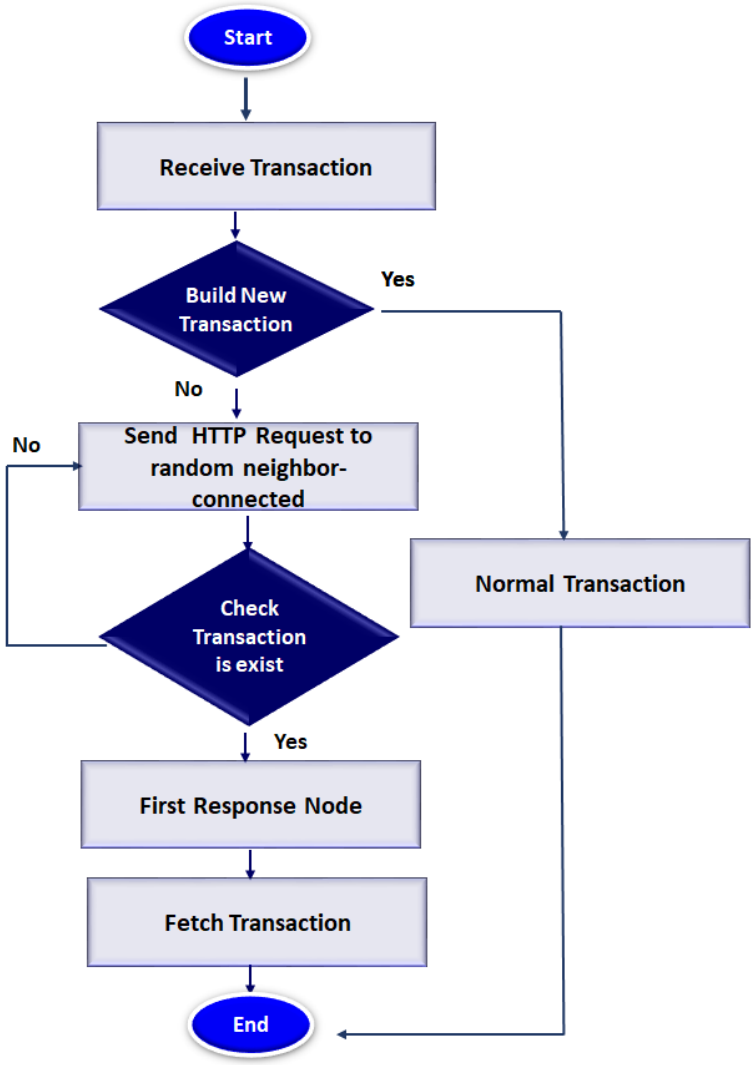
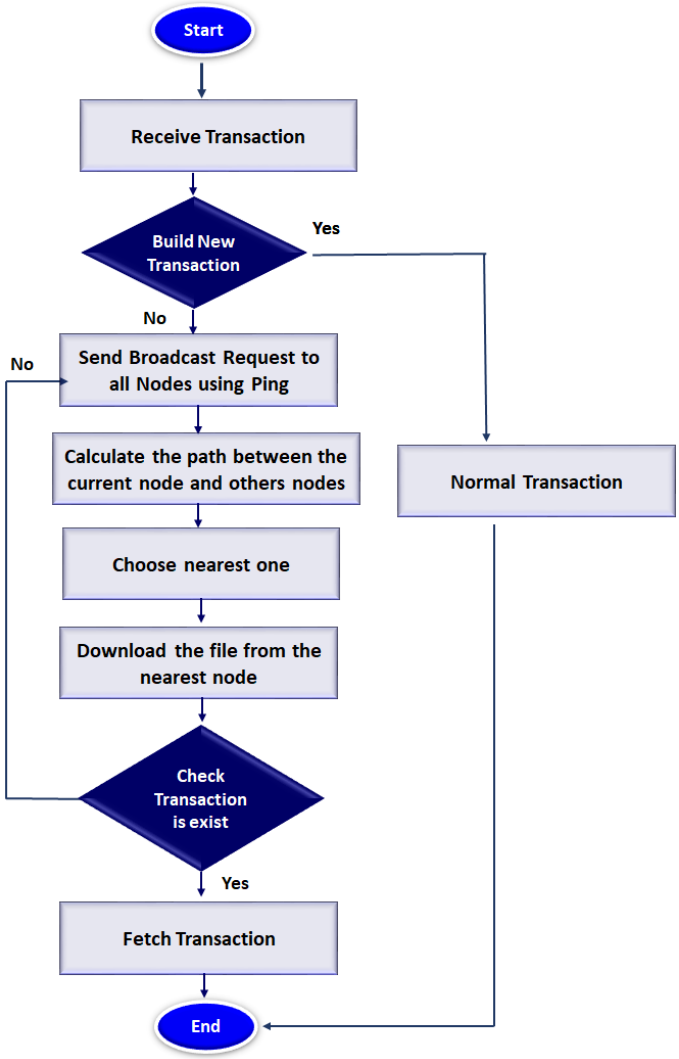


Figure 3.9 Flowchart of Randomly Backup Method

3.6.2 Shortest Path Backup Method

In the second backup technique, when one of the nodes in the Blockchain network could not be able to send its transaction because of failed or gets hacked

by a Ransomware attack. In this thesis, five nodes are used, and it is assumed that one of these nodes fails, rendering it unable to receive new transactions or read old ones, so it sends a Broadcast request to all neighbor nodes and calculates the shortest path, based on the delay transmission between the failed nodes and the rest of the nodes in the network. An http request is sent to the nearest node and the damaged data is restored, which means it chooses the URL, based on the shortest path between the failure node and other nodes, it sends the request from the failure node to the nearest destination node and returns it to the failure node. Figure 3.10 illustrates the flowchart for this technique.



Flowchart 3.10 Shortest Path Backup Technique

The main steps of the shortest path method:

1. When a node cannot read the transactions, either because of node failure or because a Ransomware attack encrypted it.
2. The failure node will send a ping request to the other neighbor-connected nodes in the Blockchain network to get a shortest path.
3. The shortest path length between the failure nodes and the other nodes is determined after getting the responses from the nodes.
4. Calculate the shortest path length between the failure node and other nodes, by sending a ping to all nodes and the shortest path is approved.
5. Check if the backup is readable.
6. Download the backup of transactions and back to working normally by using http protocol
7. Otherwise, select another node.

3.7 Building Smart Contract Algorithm

In this section, the smart contract for protecting the medical healthcare record from external and internal Ransomware attacks is building. This smart contract use two basic libraries:

- HitchensUnorderedkeySet.sol**:** To create, Retrieve, Update and Delete the dataset in the solidity smart contract.
- Stringsutil.sol**:** Dumping data as a string in Solidity can be simpler.

The below steps must be done to implement this contract:

- Run Ganache Network.
- Open Git Bash terminal, and write the path of the location of code.
- Open Node.js, in terminal Npm run dev.
- Reset deploying the smart contract in terminal Truffle migrate-reset.

- Upload smart contract to Ganache.
- Convert HealthContract.sol to HealthContract.json.
- Loading the files project using window. load function
- Load APP.web3provider (http://localhost:7545).
- ABIEEncoderV2 for encodes data into bytes.

The smart contract has a set of special functions for adding, deleting, updating, and checking the patient's Ether address format to update the data coming from the smart contract and link it to the interface and vice versa web3.js. In the normal state of the Blockchain network, which is that the node is working, the smart contract allows only normal patient's records to be stored on the Blockchain. The smart contract will reject all transactions from unknown Ether addresses or abnormal patient records containing Ransomware attack hyperlinks, and the smart contract will block the transactions. Algorithm 3.1 is presented in the smart contract created as a part of the proposed system.

Algorithm 1: Smart Contract Algorithm for Proposed System

Input:
MHR: Medical Healthcare Record

Output:
Accepted transaction or rejected transaction

Begin:

```
1.    Check whether the PS greater and equal 0.5.0   # Check the solidity version
2.    Set PatientArray                               # Array that store Patient data
3.    Set PatientSet                                 # Set that store Ether address
4.    Set MHR                                        # Medical healthcare record
5.    Set incomingPat is True      # To all incoming patient try to enter this network
6.    While incomingPat do
7.        Check whether MHR[patient-Ether-address] equal address(0x0) and
          MHR[patient-Ether-address] in PatientSet then
8.            Repeat
9.                Read MHR_data from PatientArray[MHR]   # Read the patient data
10.               Check  MHR_data included hyperlink then  # Metadata for each
                  transaction
```

```
11.                 Block MHR[patient-Ether-address]  # All new transaction of this
                    patient will be rejected
12.                 Break
13.             Otherwise; add MHR_data to the Blockchin network as new
                transaction                                  # Accept the transaction
14.             End_check
15.             Next MHR_data
16.         Until no anymore transaction
17.         End_loop
18.     Otherwise; Ignore MHR[patient-Ether-address]    # Outside private network
19.     Break
20.     End_check
21. End_loop
```

End Algorithm

4.1 Introduction

The previous chapter discussed algorithm and the tools used to build a new smart contract and a Blockchain network to secure patient records against Ransomware attacks. This chapter presents an implementation and a discussion of the practical results of the security of the proposed system to improve Ransomware security systems based on Blockchain technology. It is important to note that the obtained results that will be presented are a simulation of the system since the real results require deploying the smart contract on a real network of Ethereum.

4.2 Implementation Environment

The proposed system is implemented using a Lenovo laptop with the following specifications:

- **Windows edition:** Windows 11 Home.
- **Version:** 21H2
- **The processor:** Intel(R) Core(TM) i5-9300H CPU @ 2.40GHz.
- **The memory (RAM):** 8.00 GB.
- **System type:** 64-bit Operating System, x64-based processor.

4.3 The Proposed System Interfaces

The implementation of proposed system interfaces consisted of two parts, the front-End part and the Back-End part:

4.3.1 Step-by-step process of the system (Front-end Part)

The front end includes some basic parts as follows:

4.3.1.1 The Main Interface

The main interface of the proposed system is shown in Figure 4.1 below. It has two main parts: before using Blockchain technology, the normal state of the standard system, and after using Blockchain technology to protect patient healthcare records from Ransomware attacks.

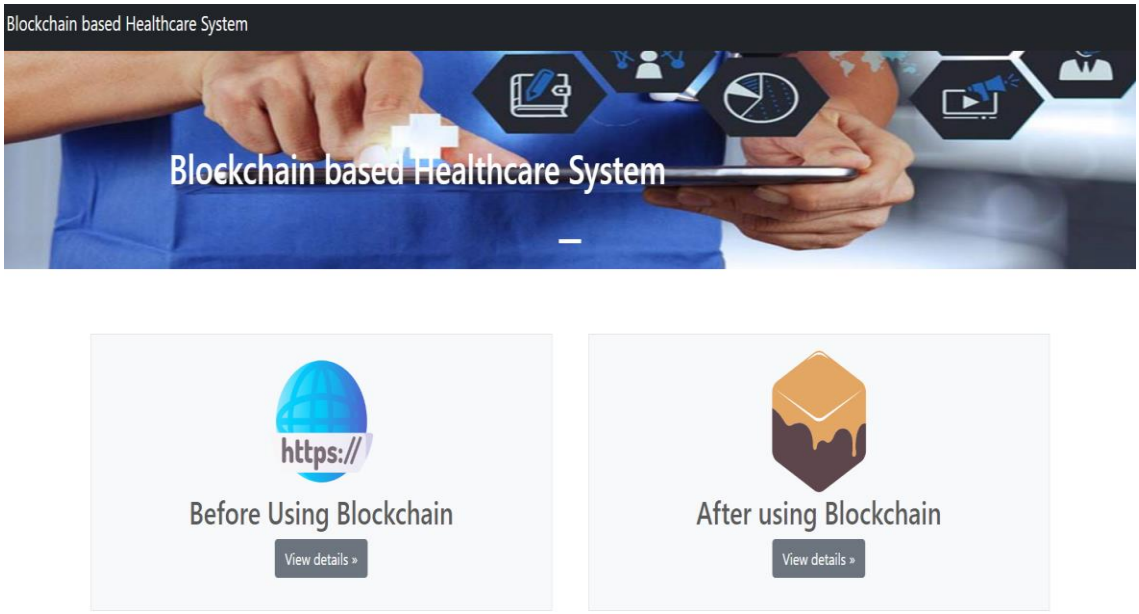


Figure 4.1 Main Interface of the Proposal System

A. Standard System without Using Blockchain: Figure 4.2 below illustrates the normal case in the standard system, where a Ransomware attack sends a fake message that tricks the doctor into thinking that the email link contains the needed medical images and analyses. In reality, this link contains the Ransomware attack code to encrypt patients' files.

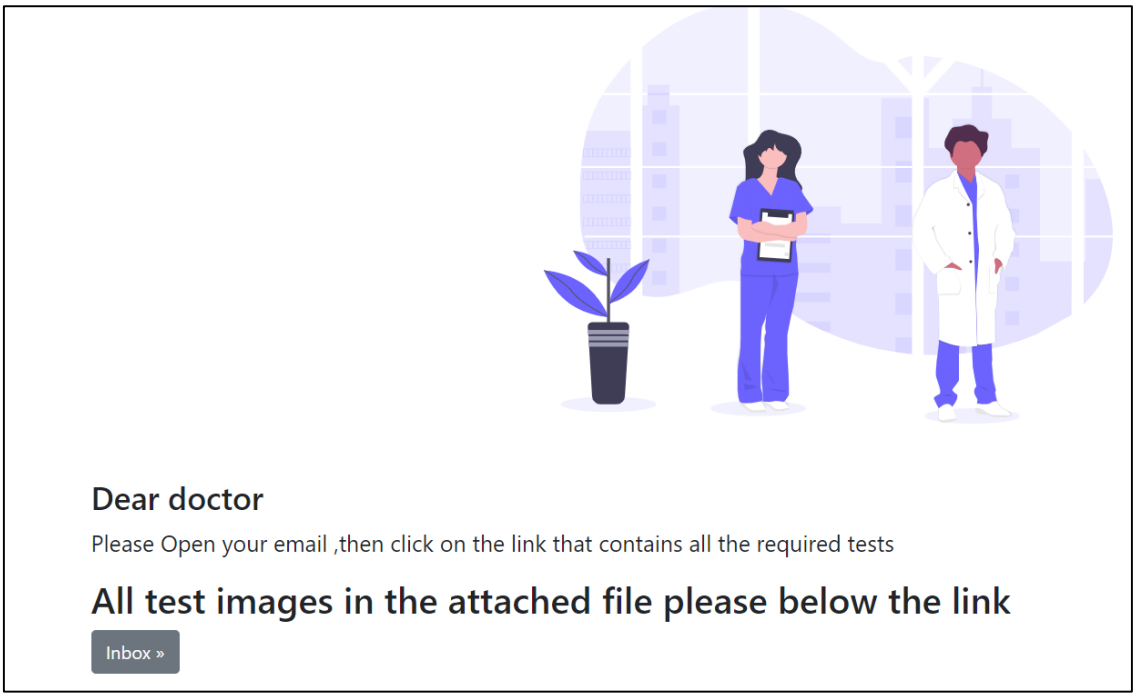


Figure 4.2 Before using Blockchain Interface

B. Proposed System based on Blockchain: All parts of the model are used in this interface, from uploading a patient's record to the smart contract and Ethereum Blockchain network. Also, how to protect a patient's health record from a Ransomware attack, whether the attack came from outside or inside the Ethereum Blockchain network (see Figure 4.3).

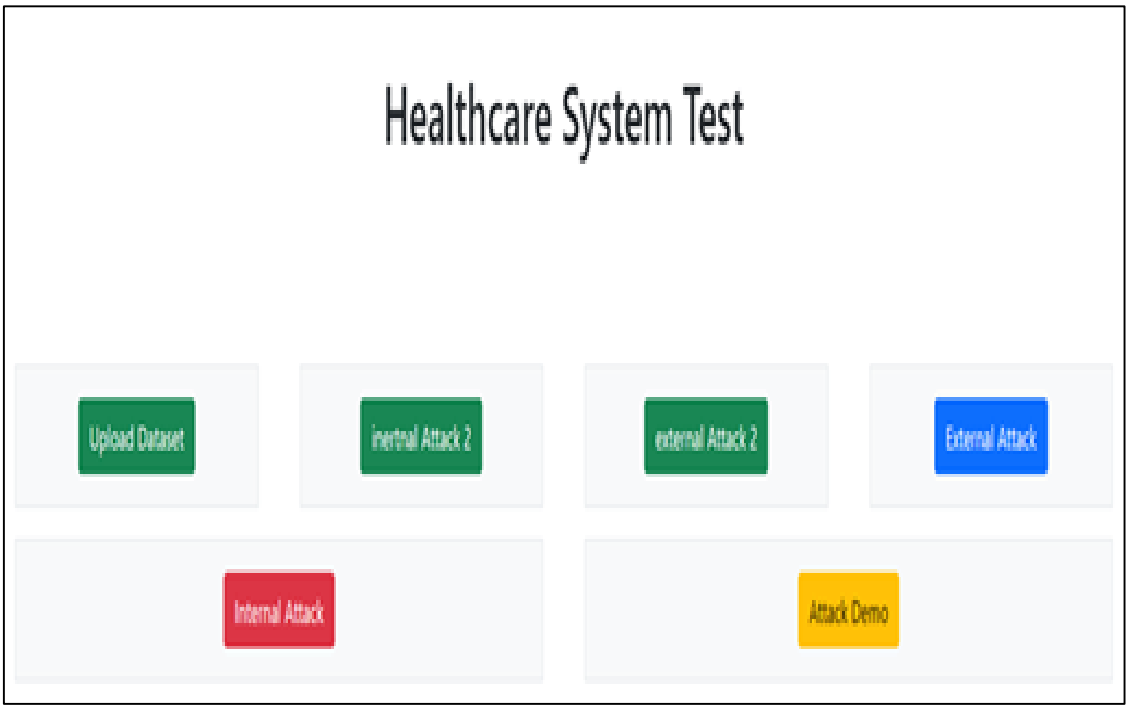


Figure 4.3 Proposed System Based on Blockchain Interface

4.3.1.2 Uploading Dataset Interface

On the "upload patient data" page, the patient records from the "Dataset" are sent to the smart contract in two different ways, as shown in Figure 4.4. Since the smart contract in the Ethereum Blockchain network cannot read the data directly from the "Excel file", so the file is changed into two different formats:

1- The patient record was read from the JSON file so the records could be sent one at a time.
2- Read patients' records using MYSQL to read patients' records based on the patient's health condition and the priority of response.

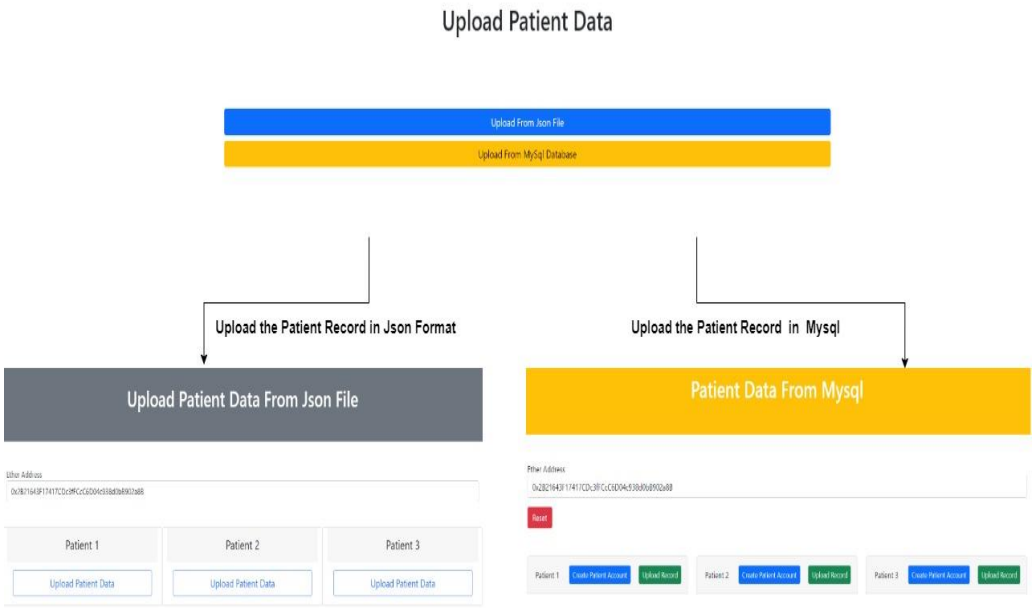


Figure 4.4 Upload Patient Dataset

It is important to mention that the MetaMask pop-up will appear, as shown in Figure 4.5, by selecting the account that will be used.

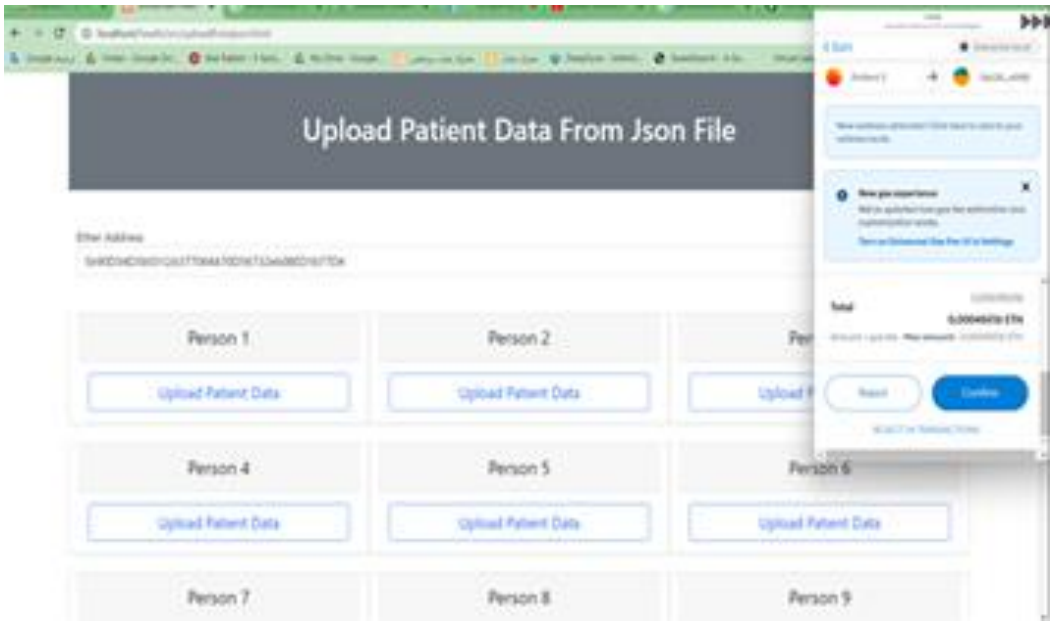


Figure 4.5 Upload Patient Record

4.3.1.3 External Attack Interface

In case of external Ransomware attacks, every transaction sent from outside the Blockchain network is automatically rejected based on the Ether address of the sender, even if the sender has data and an account in the MetaMask wallet (see Figure 4.6).

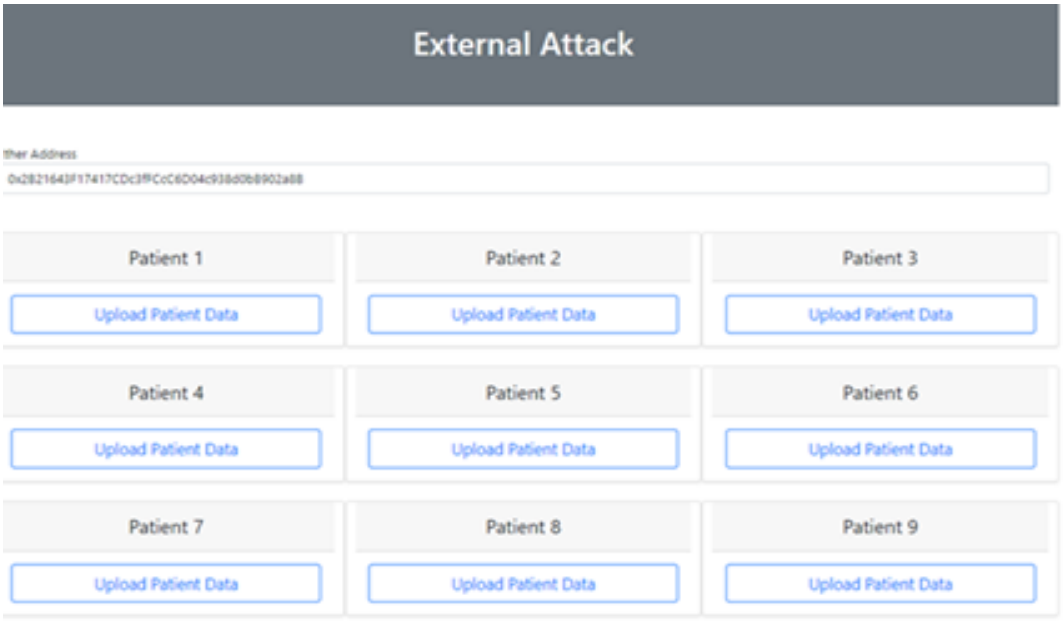


Figure 4.6 External Attack Interface

Figure 4.7 shows the error message in the MetaMask wallet that appears when the external attack tries to send transactions containing a Ransomware attack.

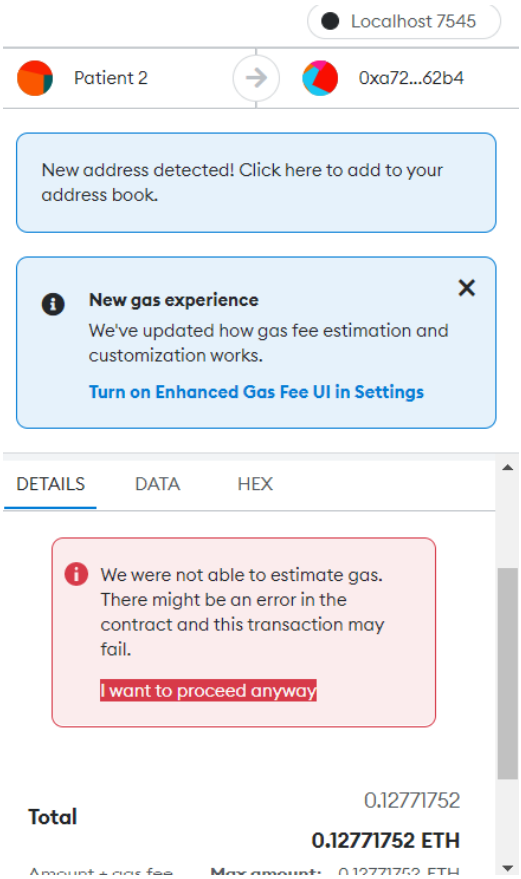


Figure 4.7 Error Message for External Attack in MetaMask Wallet

4.3.1.4 Internal Attack Interface

In case of an internal attack, the Ransomware attack manipulates a patient inside the Blockchain network and simultaneously tries to transmit the Ransomware attack link as a transaction. Therefore, the Ransomware attack link may be randomly located in any patient's records. In our test, we have assumed that the seventh patient is the Ransomware attacker, and he/she transmitted the Ransomware attack link in any record.

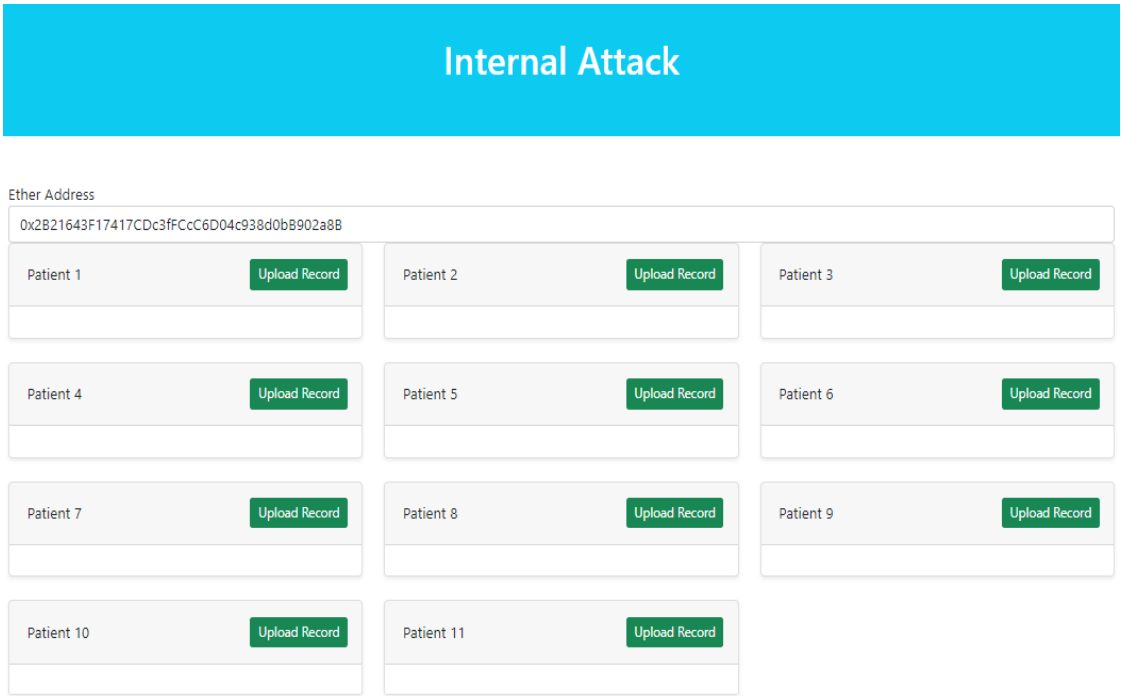


Figure 4.8 Internal Attack Interface

As depicted in Figure 4.9, an alert message of rejecting the transaction and blocking all remaining records.

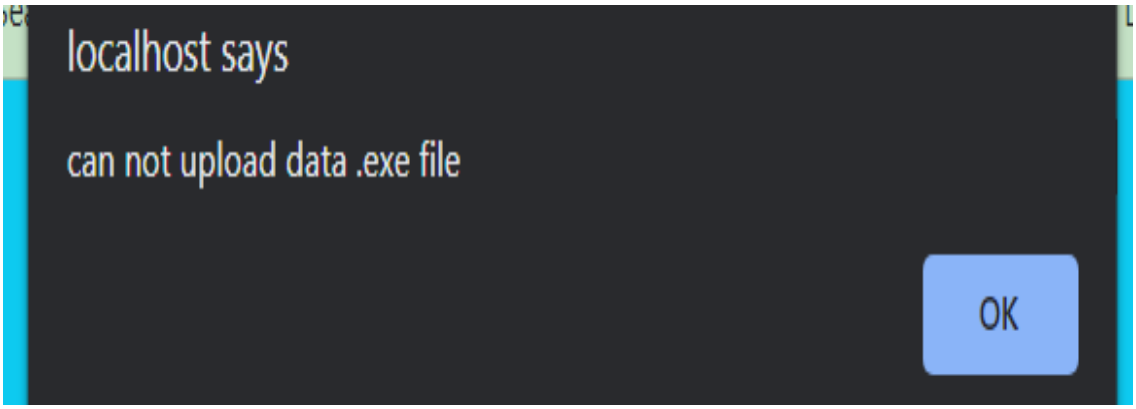


Figure 4.9 Rejecting Alert Message

Figure 4.10 shows the error message when a patient uploads an abnormal file link.

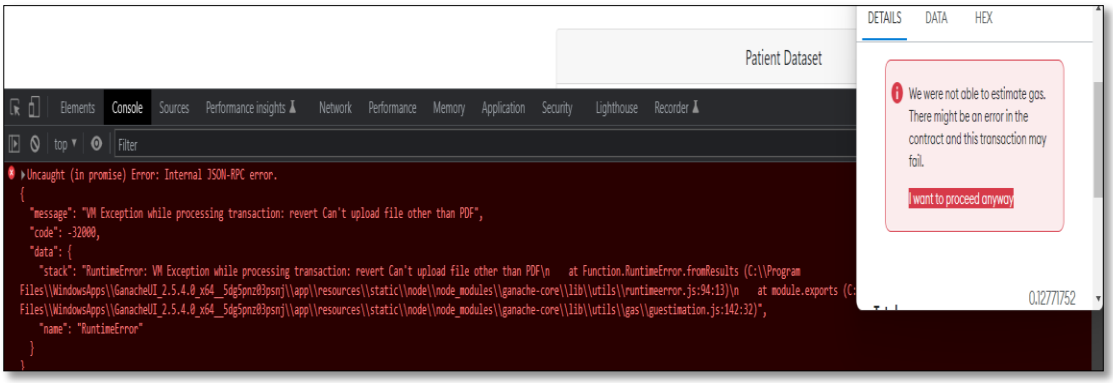


Figure 4.10 Error Message When Patient Uploads Abnormal File Link

4.3.2 Step-by-step Process of the System (Back-end Part)

The Back-End includes some basic parts as follows:

4.3.2.1 Results of Ganache UI

Ganache has been used to simulate a fully functional Ethereum Blockchain network. In this section, we display the ganache result when adding Patients transactions. Figure 4.11 shows the block of Ganache before deploying the smart contract. Figure 4.12 after running the smart deploy contract and Figure 4.13 the blocks on ganache after uploading transactions.

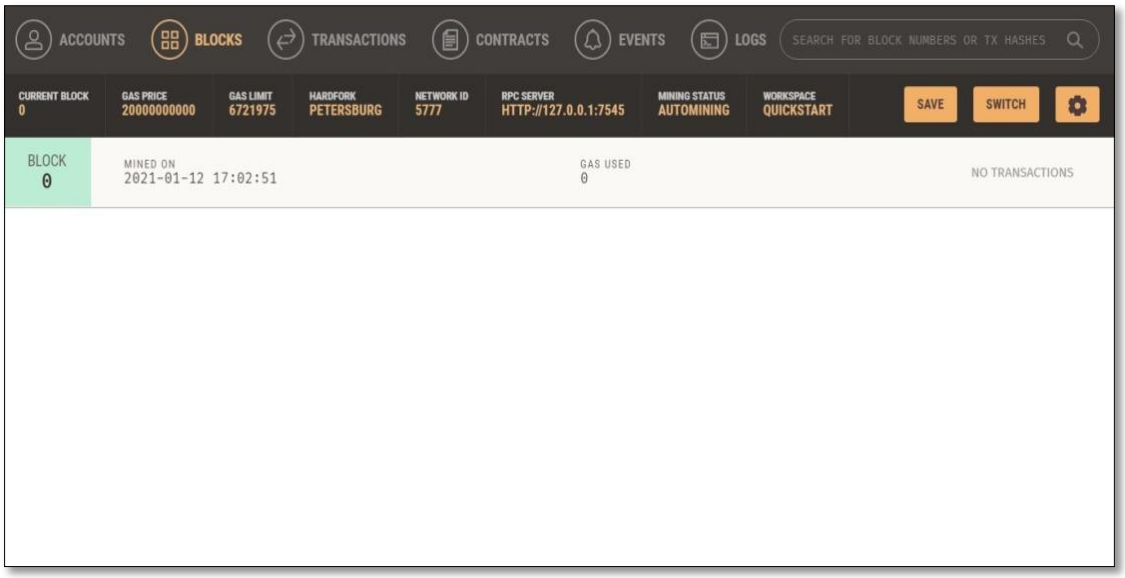


Figure 4.11 Block of Ganache before Deploy Smart Contract

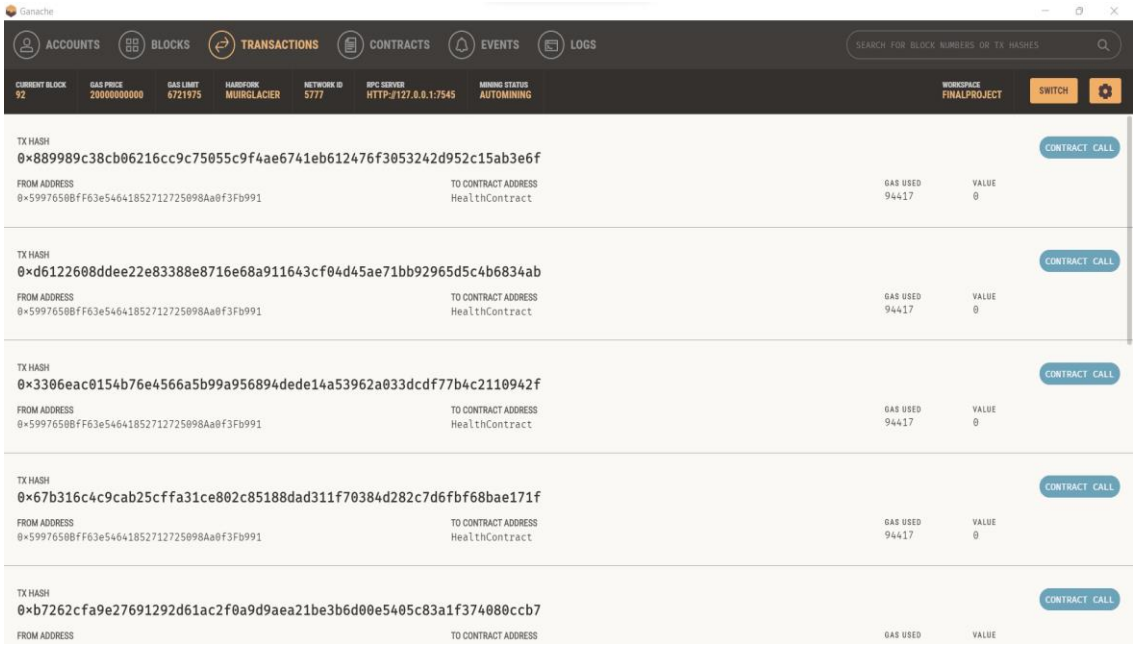


Figure 4.12 Block of Ganache after Deploy Smart Contract

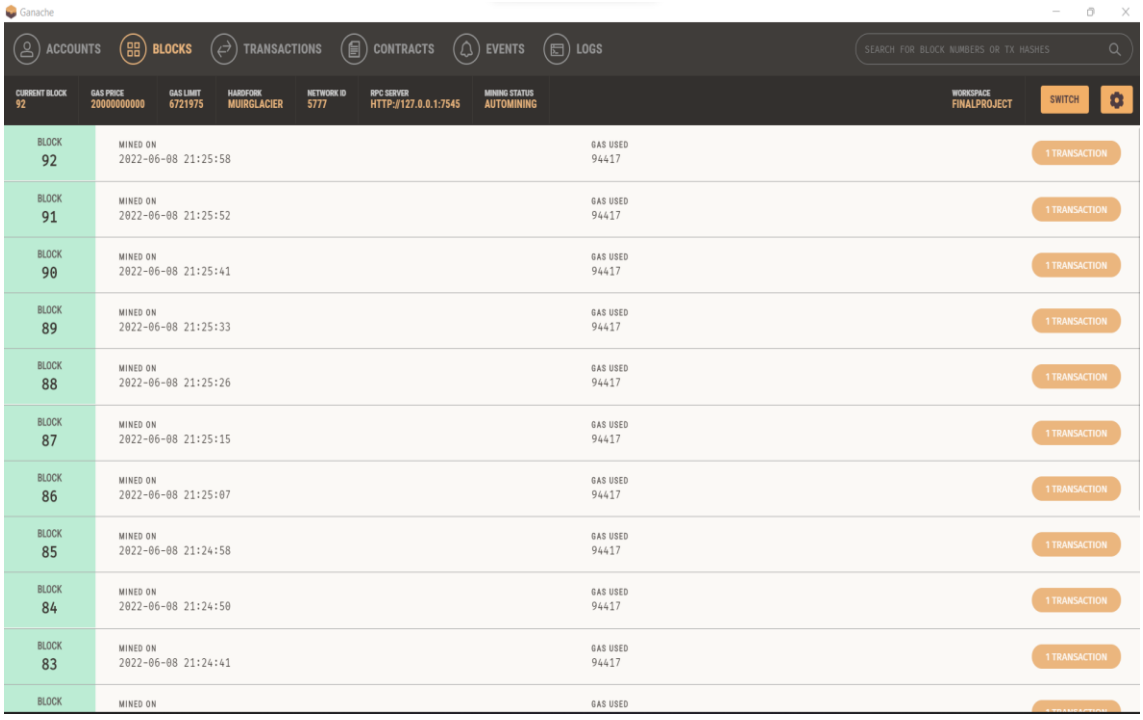


Figure 4.13 Block of Ganache after Uploading Dataset

4.3.2.2 Compiling and Migrations Contracts

To compile the smart contract, change to the directory root where the source code is located and type the following in the terminal:-truffle compile. The output is in Figure 4.14.

```
HP@noosha MINGW64 /c/xampp/htdocs/heath
$ truffle migrate --reset

Compiling your contracts...
===========================
> Compiling .\contracts\HealthContract.sol
> Compiling .\contracts\HitchensUnorderedAddressSet.sol
> Compiling .\contracts\HitchensUnorderedKeySet.sol
> Compiling .\contracts\Migrations.sol
> Compiling solidity-util\lib\Strings.sol
> Compilation warnings encountered:
```

Figure 4.14 Output Compile Contracts

Migrations are JavaScript files that help to deploy contracts to the Ethereum Blockchain. To run your migration, type the following in the terminal:- truffle migrate. The output is shown in Figure 4.15.

```
Starting migrations...
======================
> Network name:    'development'
> Network id:      5777
> Block gas limit: 6721975 (0x6691b7)


1_initial_migration.js
======================

   Replacing 'Migrations'
   ----------------------
   > transaction hash:    0xee57eae3d394d1b0df44addca46928d36f7ade9fe10fe0f552895e24a5714d18
- Blocks: 0            Seconds: 0
   > Blocks: 0            Seconds: 0
   > contract address:    0x99045a38557CFDdA2B620D8F1b7f63B26f8EE41f
   > block number:        88
   > block timestamp:     1657791963
   > account:             0x078c116744E66d669c40eBe0c40caA4908e0D2f5
   > balance:             99.77463898
   > gas used:            191943 (0x2edc7)
   > gas price:           20 gwei
   > value sent:          0 ETH
   > total cost:          0.00383886 ETH


   Replacing 'HealthContract'
   --------------------------
   > transaction hash:    0xded0272740111a873709cf2952151beb9c5d5fe219f02d1ab7b463617810350a
- Blocks: 0            Seconds: 0
   > Blocks: 0            Seconds: 0
   > contract address:    0x9F97e10250CA87D40208B6B04E7a1cbFB1EDA11f
   > block number:        89
   > block timestamp:     1657791963
   > account:             0x078c116744E66d669c40eBe0c40caA4908e0D2f5
   > balance:             99.74240424
   > gas used:            1611737 (0x1897d9)
   > gas price:           20 gwei
   > value sent:          0 ETH
   > total cost:          0.03223474 ETH


- Saving migration to chain.
   > Saving migration to chain.
   > Saving artifacts
   -------------------------------------
   > Total cost:           0.0360736 ETH
```

Figure 4.15 Output Migrations Contracts

4.4 Simulation of Ransomware Attacks

A simulator simulates the workplace environment of the Ransomware attack has been developed, specifically the TeslaCrypt Ransomware attack. First, the executive file is sent to the doctor's email account in the form of an image depicting the patient's medical analyses and examinations. In other words, the attacker sends an email to the victim containing the attack link. Finally, when the victim downloads and executes the file, the Ransomware begins to perform. The simulation of a Ransomware attack is separated into four main stages:

- It hides the console interface that appears when running any executable file.
- It encrypts all files inside the path of a Ransomware executable file.
- It changes the extension of all encrypted files to make them unreadable or recoverable.
- After completing the encryption process, the payment process instruction interface appears.

Figure 4.16 shows the interface of files after encryption by a Ransomware attack.

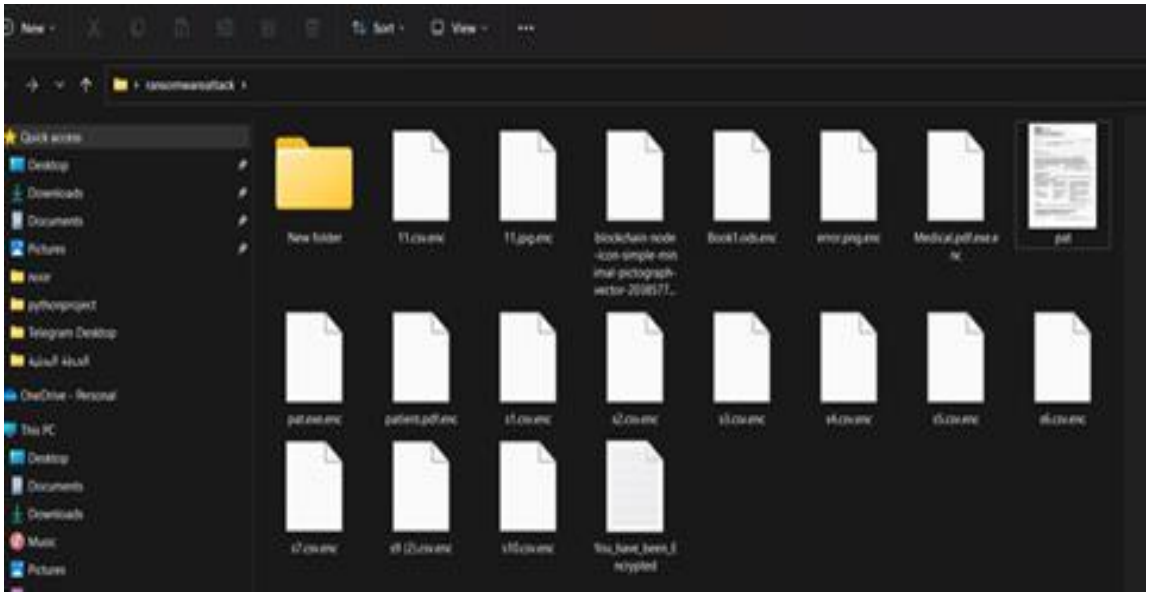


Figure 4.16 Encrypted Files By Ransomware Attack

After the encryption process, the victim notices an interface README.txt as shown in Figure 4.17, a file with instructions on getting his encrypted files back by paying a ransom in bitcoin currency.

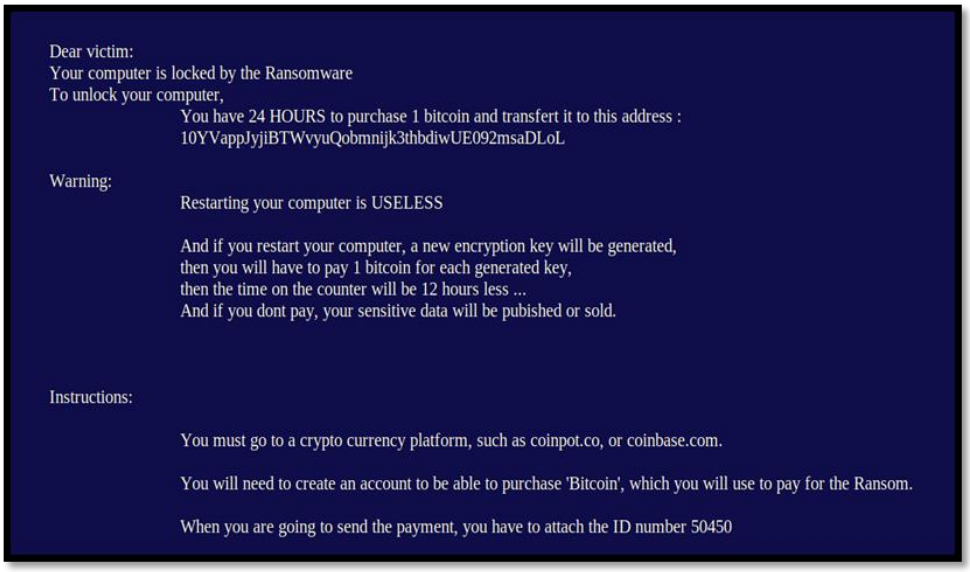


Figure 4.17 Alert Message for Victim

This process results when the attacker's privacy is protected, and his identity and location cannot be tracked. Also, the ransom must be sent to the Ransomware attacker's address within a specific time. If not, he will delete all the encrypted files. After paying the ransom, there are two ways to generate and save the decryption key to decrypt all encrypted files:

- ***Online decryption key*:** When the encryption, the attacker gets an email with the decryption file and a unique ID, which indicates a random number representing the victim's serial number. This keeps the decryption key from falling into the wrong hands (See Figure 4.18).

Figure 4.18 Online Decryption Key

- ***Offline decryption key*:** After the ransom is paid, the attacker has an executable that stores the decryption file so that they can send it to the victim, who can then use it to decrypt the files and get their data back. Figure 4.19 shows the offline decryption key.

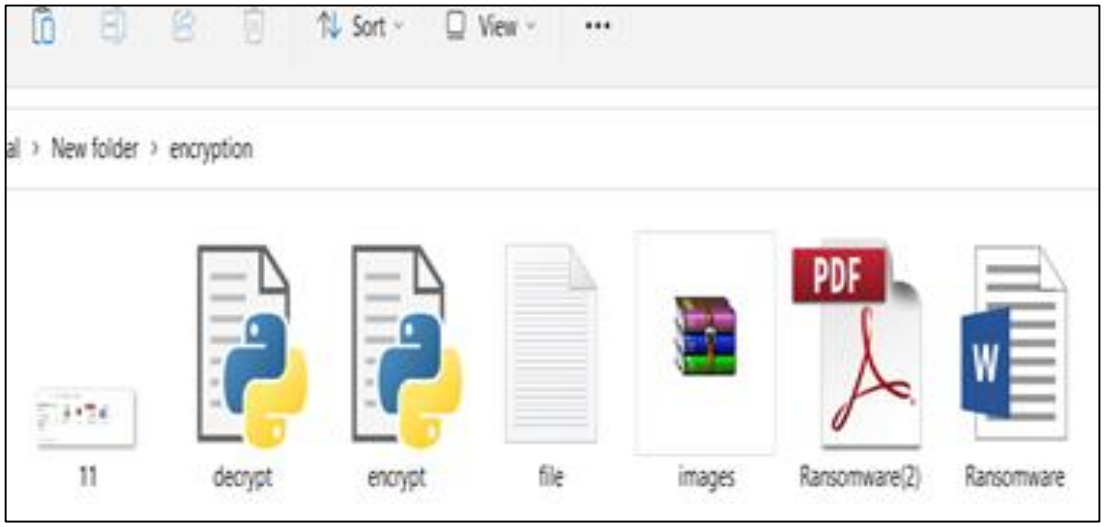


Figure 4.19 Offline Decryption Key

4.5 Deploy Smart Contract to Ethereum Network

The proposed system will use the Ganache Ethereum test network to deploy smart contracts, record results, and evaluate system performance based on them. The following steps are to deploy a smart contract on the Ganache Ethereum test network to validate the smart contract.

1- The following are the configuration of the Ethereum network.
   - Host Name:**127.0.0.1**
   - Port number: **7545**
   - Network Id: **5777**
   - Account Default Balance:100 Ether

2- Open the MetaMask wallet and submit the amount of Crypto-currency required to deploy a smart contract over the network for each Patient (see Figure 4.20, for example).

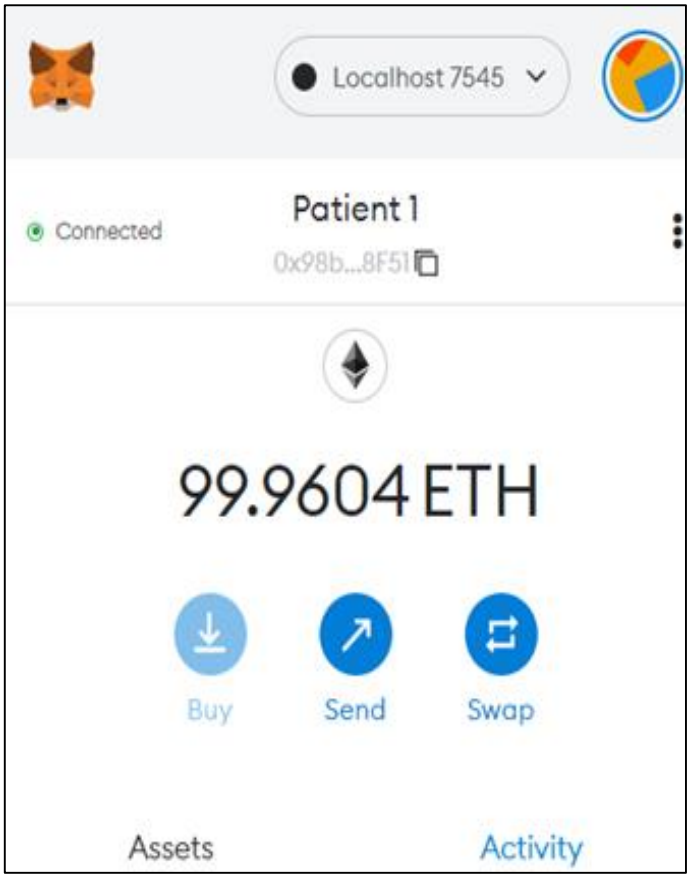


Figure 4.20 Patient Account in MetaMask

3- The next step is deploying a smart contract from Visual Studio Code to the Ganache Ethereum local test network (See Figure 4.21).

Figure 4.21 Deploy Smart Contract on Ganache Ethereum Network

4- A smart contract address is created to make transactions and call smart contract functions on the Ganache Ethereum network (see Figure 4.22).

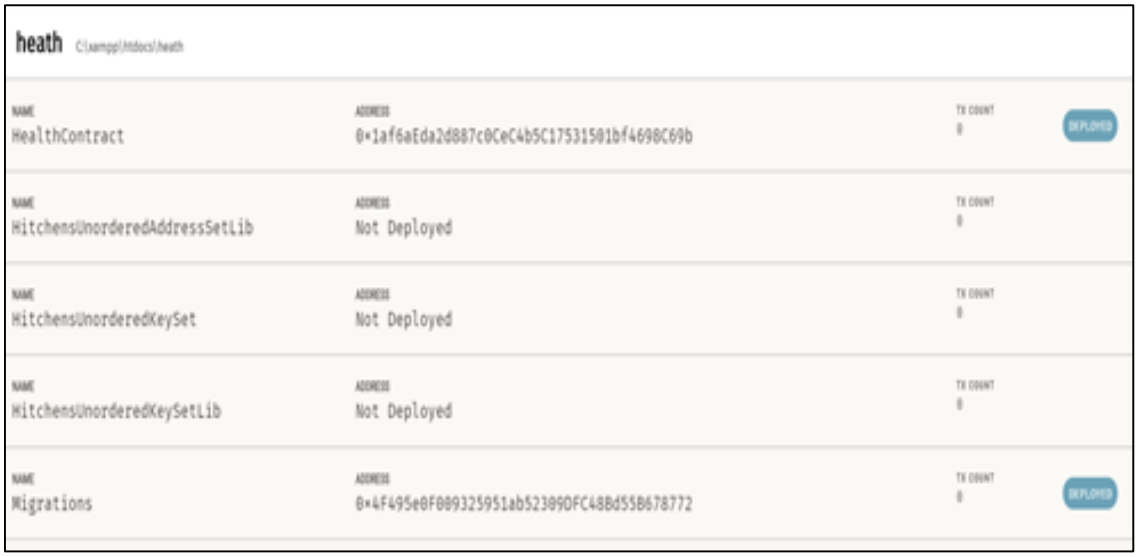


Figure 4.22 Blocks creation after Deploying a Smart Contract

5- Git Editor has been used for deploying the healthcare contract. This is run by executing the script (see Figure 4.23-4.24):

Truffle migrate –reset// Reset the Deployment of the smart contract

```
Starting migrations...
======================
> Network name:    'development'
> Network id:      5777
> Block gas limit: 6721975 (0x6691b7)


1_initial_migration.js
======================

   Replacing 'Migrations'
   ----------------------
   > transaction hash:    0x17f096fe931506ea9ba3f55b52ba11ecdbb58646465ca9afcc11
96b68c642c52
- Blocks: 0            Seconds: 0
   > Blocks: 0            Seconds: 0
   > contract address:    0x85DaE3c2e6760a86952e4507de4B2fD9D6Ca1449
   > block number:        4
   > block timestamp:     1654593676
   > account:             0x5Bd6A6217B328Ce61a63832e64BAF930bF2e7eC0
   > balance:             99.95924078
   > gas used:            191943 (0x2edc7)
   > gas price:           20 gwei
   > value sent:          0 ETH
   > total cost:          0.00383886 ETH
```

Figure 4.23 Deploying the Healthcare Contract

Figure 4.24 Deploy the Migration Contract

Then as shown in the below Figure (4.25), calculate the total cost of deploying the healthcare and migration contracts.

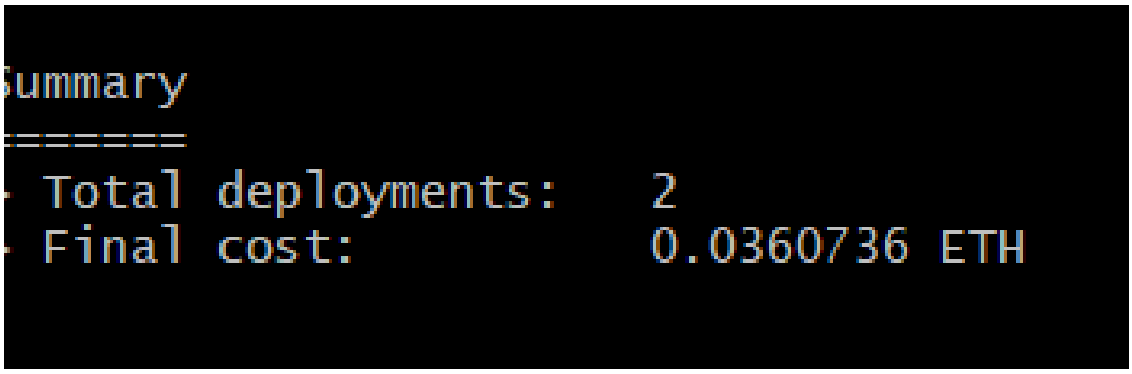


Figure 4.25 Cost of Deployment Smart Contract

4.6 Failure Node Backup: Python Flask

When a node in the Blockchain network fails or gets hacked by Ransomware. So we proposed a secure backup strategy to restore the failed node data.

We built a simulation that simulates the environment of the Blockchain network and restores a backup of the lost data from other nodes in the network. Nodes URL can begin from:

http://127.0.0.1:5001 and http://127.0.0.1:5002, etc.

While clients' URLs can begin from: http://127.0.0.1:8081 and http://127.0.0.1:8082, etc.

The node dashboard has two tabs in the navigation bar:

- Mine: To see information about transactions and the Blockchain, as well as to find new blocks of transactions (see Figure 4.26)

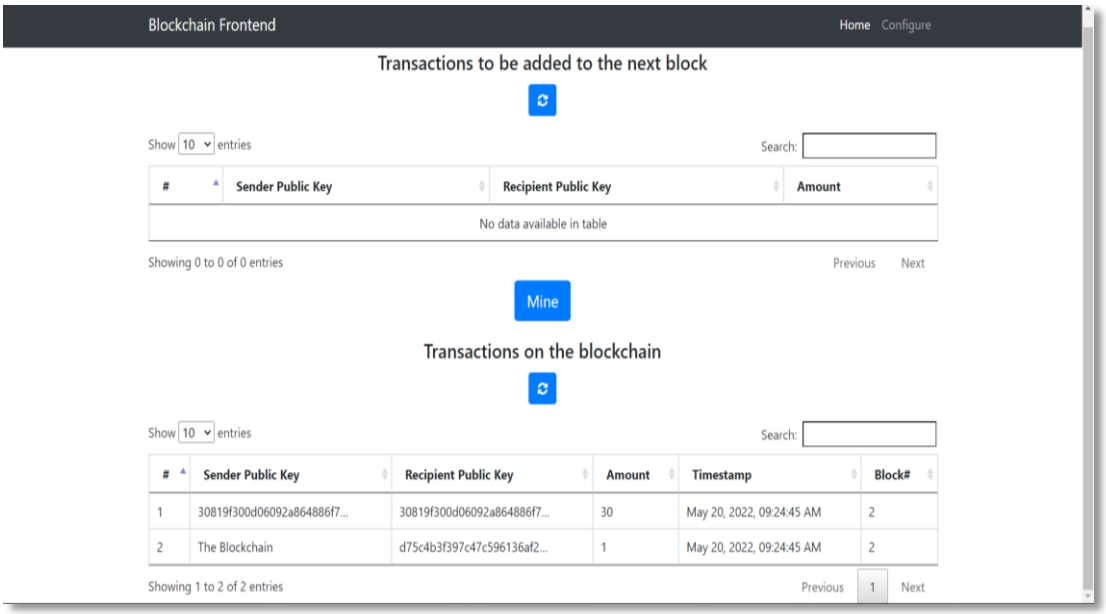


Figure 4.26 Interface of Node Mining Tab

- Configure: Set up links between the different Blockchain nodes (see Figure 4.27).

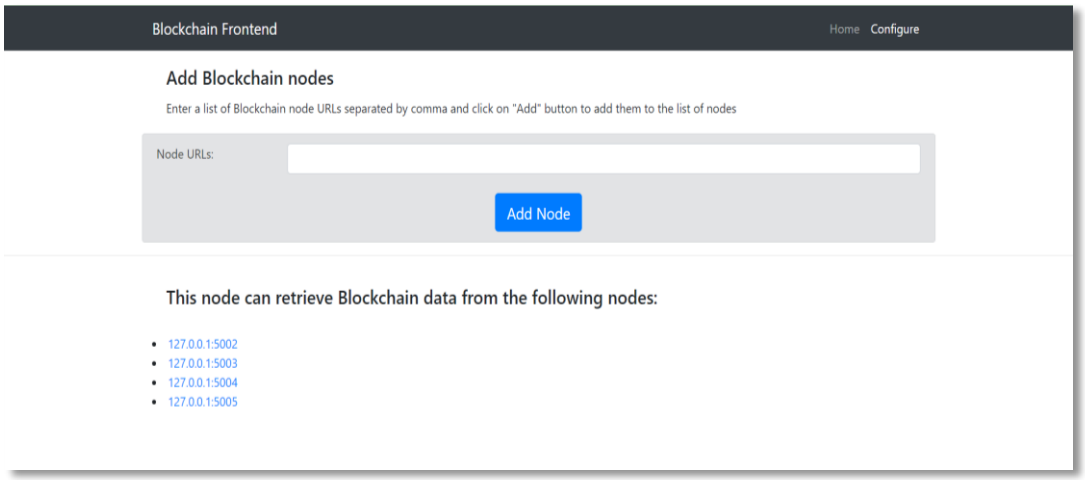


Figure 4.27 Interface of Node Configuration Tab

Figure 4.28 below illustrates the node's terminal normal state once it has been started.

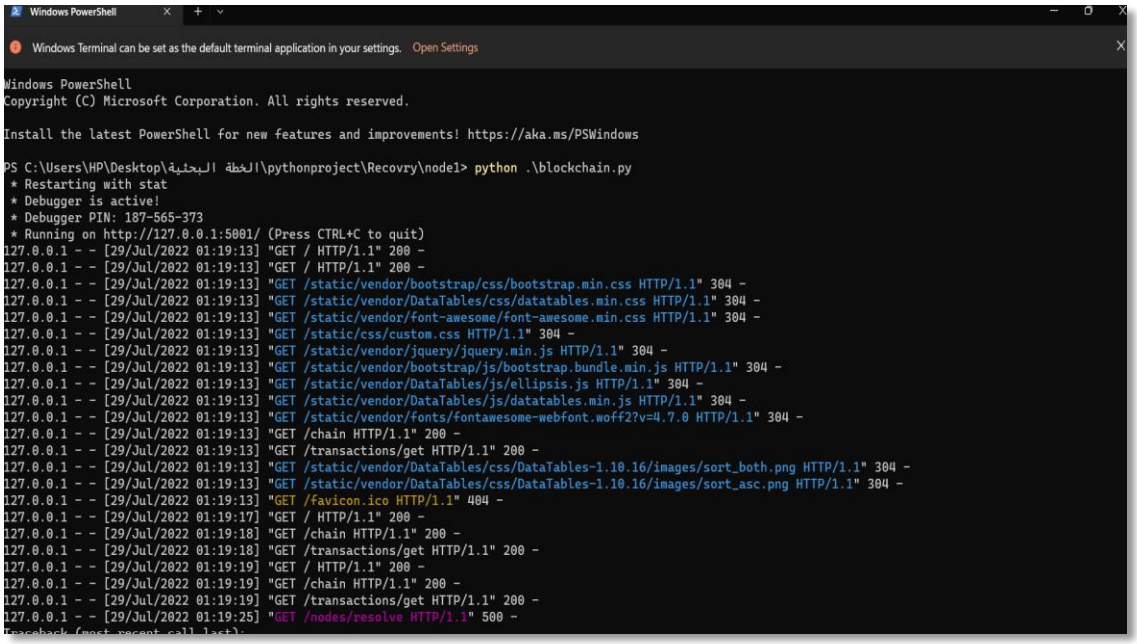


Figure 4.28 Node's Normal State

When a node fails, it sends a direct HTTP request to the remaining nodes to retrieve the lost node transaction. Moreover, randomly recovered the data from the node, as shown in Figure 4.29.

Figure 4.29 Retrieve the Backup of Transaction from another Node

4.7 Ethereum Gas Test

This section shows the performance test results regarding usage costs, as shown in Table 4.1. The amount of gas used in every procedure that requires a transaction to be sent to the Blockchain is recorded using Ganache. Execution of the Solidity code is deterministic, and the gas uses are calculated as the total gas used by the implemented EVM operating codes.

Table 4.1 Ethereum Gas Test

Behavior	Gas Used	Ether Cost	U.S. Dollar Cost
Deploy Smart Contract	**21.60**	**0.0360736 ETH**	**65.19$**

4.8 Performance Evaluation of Proposed System

In this section, the proposed system is evaluated according to the metrics that have been adopted (see Section 2.13.1 in Chapter Two) as well as the selected dataset (see Section 2.13.2 in Chapter Two).

4.8.1 Cost Results

Table 4.2 shows the cost of all patients' records of the dataset, which contains all the records, including the Ransomware attack link, where each reading represents a transaction, before using the proposed system and preventing the Ransomware attack link, and how these costs have been reduced.

Table 4.2 Cost of the All Patient Records before Using the Ransomware Protection System

No. Patient	No. Readings	Cost in Wei	Cost in Iraq Currency
Patient 1	31	697376	0.00000123762768490336

Patient 2	35	787780	0.0000013980669504158
Patient 3	21	472668	0.00000083884017024948
Patient 4	17	382636	0.00000067906109020196
Patient 5	20	450160	0.0000007988954002376
Patient 6	20	450160	0.0000007988954002376
Patient 7	39	877812	0.00000155784603046332
Patient 8	19	427652	0.00000075895063022572
Patient 9	27	607716	0.00000107850879032076
Patient 10	22	485276	0.00000086121548837236
Patient 11	14	315112	0.000000867655219984

For example, we have assumed that the Seventh patient is a Ransomware attack, the second record of its records contains the link to a Ransomware attack, and when the proposed system is executed, all records of this patient will be rejected, and the cost will be reduced by 855304, as shown in Table 4.3.

Table 4.3 Cost of the All Patient Readings after Using the Ransomware Protection System

No. Patient	No. Readings	Cost in Wei	Cost in Iraq Currency
Patient 1	31	697376	0.00000123762768490336
Patient 2	35	787780	0.0000013980669504158
Patient 3	21	472668	0.00000083884017024948
Patient 4	17	382636	0.00000067906109020196

Patient 5	20	450160	0.0000007988954002376
Patient 6	20	450160	0.0000007988954002376
Patient 7	1	22508	0.000000061975372856
Patient 8	19	427652	0.00000075895063022572
Patient 9	27	607716	0.00000107850879032076
Patient 10	22	485276	0.00000086121548837236
Patient 11	14	315112	0.000000867655219984

4.8.2 Immutability Results

In this section, the number of peers is 2, ***n*** is the number of miners, 4 is the maximum block can attacker to be attacked, and ***z*** is the number of blocks. Hence, the result of the Immutability for the proposed system is:

- Each reading represented a transaction
- Each transaction represented a block
- Each reading was distributed to multiple peers
- Number of readings based Dataset = 256
- Immutability = 1 - Pr (attack) = 1 - $(2/n)^{4z}$

Immutability = 1 - Pr (attacker)
Pr (attacker) = $(2/265)^{4*265}$
Immutability = 1 - $(2/265)^{4*265}$ = 1

4.8.3 Estimated Time Results

From the observation of the obtained results according to the equations below, the estimated time of the attacker to perform an attack increases as the number of blocks increases and miners.in our proposed system, we assume that the number of miners is the same number of blocks.

E (time) = T * (number of miner/number of pairs) ^{2z}

E (time) =12 * $(1/2)^{2*1}$

E (time) = 3s

E (time) =T * $(n/2)^{4z}$

E (time) =12 * $(265/2)^{4*265}$

E (time) = 4.24631507235234183065478243 1489e+2250s

4.8.4 Data Storage Results

According to the model proposed in this thesis, it is not possible to know if the Ransomware attack in which accounts for any of the known patients, so we assumed that the attack was carried out by the seventh patient, who has 39 records and the Ransomware attack link in the second record. After using the smart contract algorithm, it will store only 227 records. The cost is also reduced by 855304 Wei, as shown in the bellow Figure 4.30.

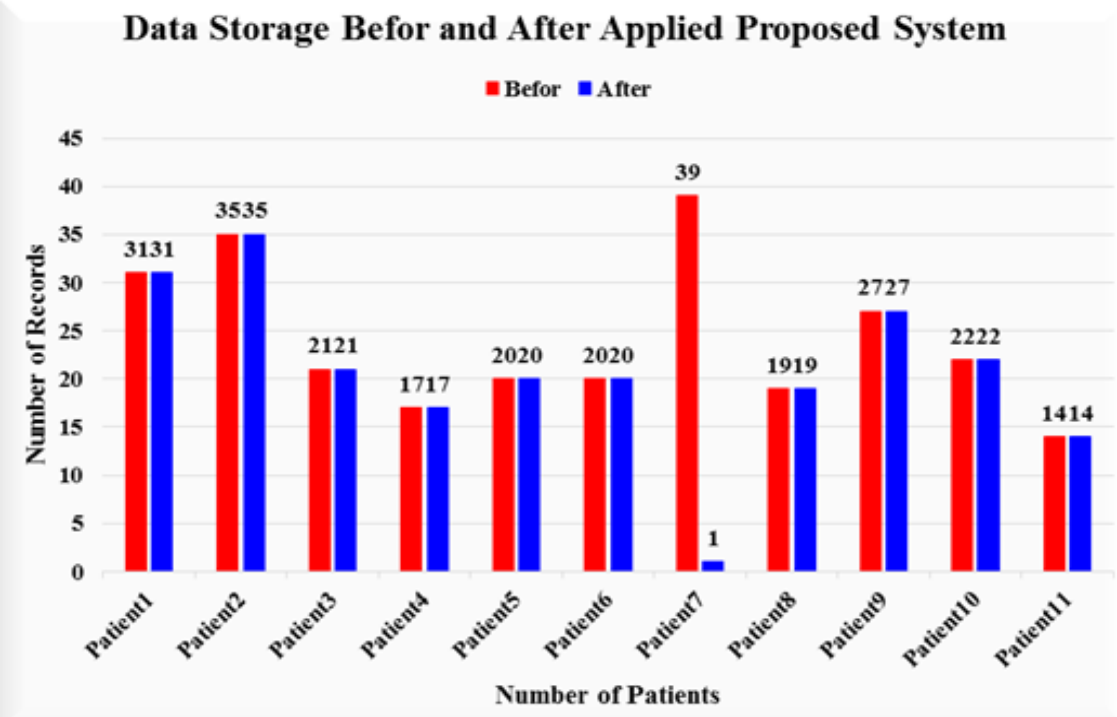


Figure 4.30 Data Storage

If the Ransomware program's attack link could happen in a certain record, that record might be 17 from 39 records. In this case, when the amount of space needed to store the data decreases, the cost also will be decreased and

become 495176 Wei. To calculate the probability of a Ransomware event in any record as follows:

If the selection record = 2, then the proposed system will block 37 record

If the selection record = 37, then the proposed system will block 1 record

Block-record = ***n*** - LinkedBlock + 1

Where ***n*** = sequence of attack record

x = number of transactions

z = number of reduced transaction

P(select-record) = ***x*** - ***n*** → ***z***

P(Record $_{number2}$) = 39 - 2 → 37 transactions are blocked

P(Record $_{number17}$) = 39 - 17 → 22 transaction are blocked

P(2) - P(17) = 37 - 22 transactions are blocked

= 15 transactions are blocked

This means the probability of blocked transactions in patient 7**.**

4.8.5 Recovery Time Results

It is the amount of time to retrieve the failed node lost transactions. We notice that the recovery time increase with the number of Blocks. Two methods were used to get the data from the failed node. The data was either taken from a random node on the network or from the closest node based on the shortest path. The results calculated by ***start time - end time for recover each recover blocks*****.** We assume to recover 10 blocks, the difference in how long it takes to get the block using the two methods is shown in Table 4.4 below.

Table 4.4 Comparison of the Two Methods Recovery Time for 10 Blocks

Number of Recovery Blocks	Time in Randomly Method	Time in Shortest Path Method
1	**0.015622139**	**0.03124404**

2	0.015622139	0.03124404
3	0.031243563	0.046867371
4	0.046900749	0.062488556
5	0.062525511	0.078111887
6	0.078128576	0.031244993
7	0.093786478	0.031244993
8	0.109409809	0.046865702
9	0.125005007	0.062488317
10	0.148600204	0.078072309

We have made a comparison between the two algorithms based on the number of blocks retrieved after the attack and during a time measured in seconds, as shown in Figure 4.31.

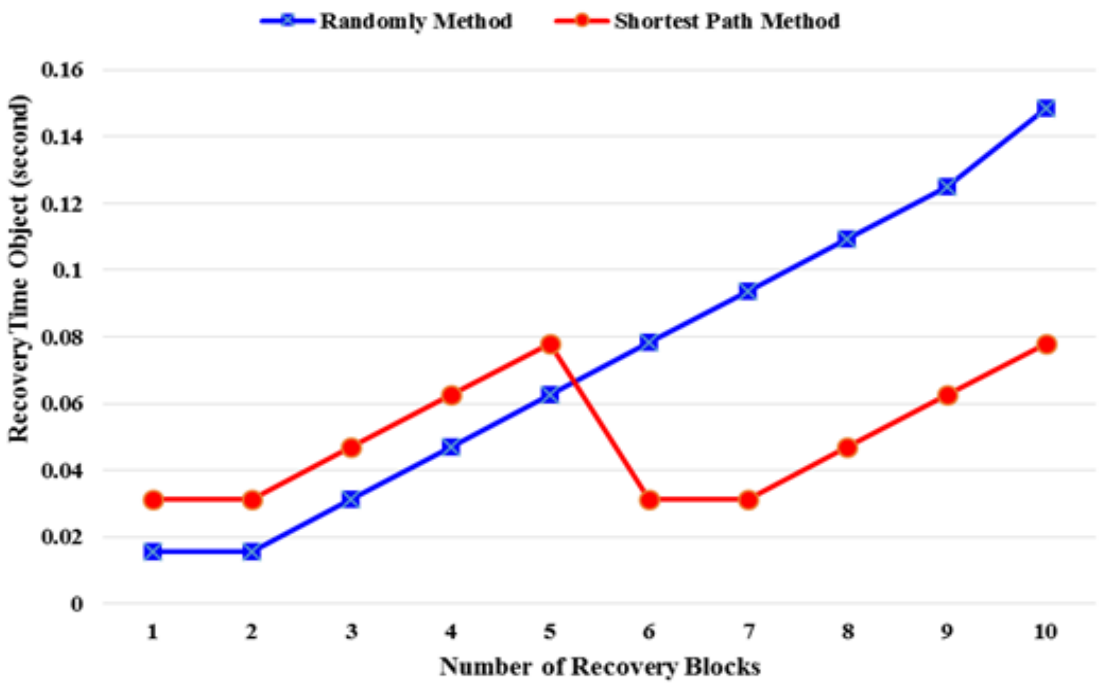


Figure 4.31 Recovery Time

Where it was found that the shortest path algorithm comes with slightly less time than the random Recovery, both methods yield typical values during the data retrieval rate.

4.8.6 Execution Time Results

The execution time to deploy smart contracts and run their tests. We checked how well the proposed system worked by measuring how long it took this smart contract to run on average from the time it was uploaded to the Ganache Network. This Blockchain simulator contains almost instant mining, which greatly reduces the time for testing execution. As a result, it was found that the execution time of transmitting patient records without the framework proposed will take time 9.5992984771728517 seconds. On the other hand, the execution time using the proposed framework, which took 2.625976563 seconds. In the end, we can show that the proposed smart contract-based model is possible because our model takes very little time and has very little overhead, which doesn't have a big effect on the Blockchain network or its users.

4.9 Setting up Development Environment for DAPPS

As explained in Chapter Two, Ethereum enables developers to create dApps, it is crucial in our project because it is the development platform and the Blockchain network used. Therefore, this section identifies the main elements of application architecture from Ethereum usage. Figure 4.32 shows the implementation platform and tools that are used to build Ethereum dApps, where Visual Studio IDE and Solidity development environment are used to write, compile and debug Solidity code. Truffle is an Ethereum framework and test environment. Ganache is a Blockchain private test platform, and the web3.js was used to interaction between the system interfaces and the Ethereum Blockchain network and MetaMask.

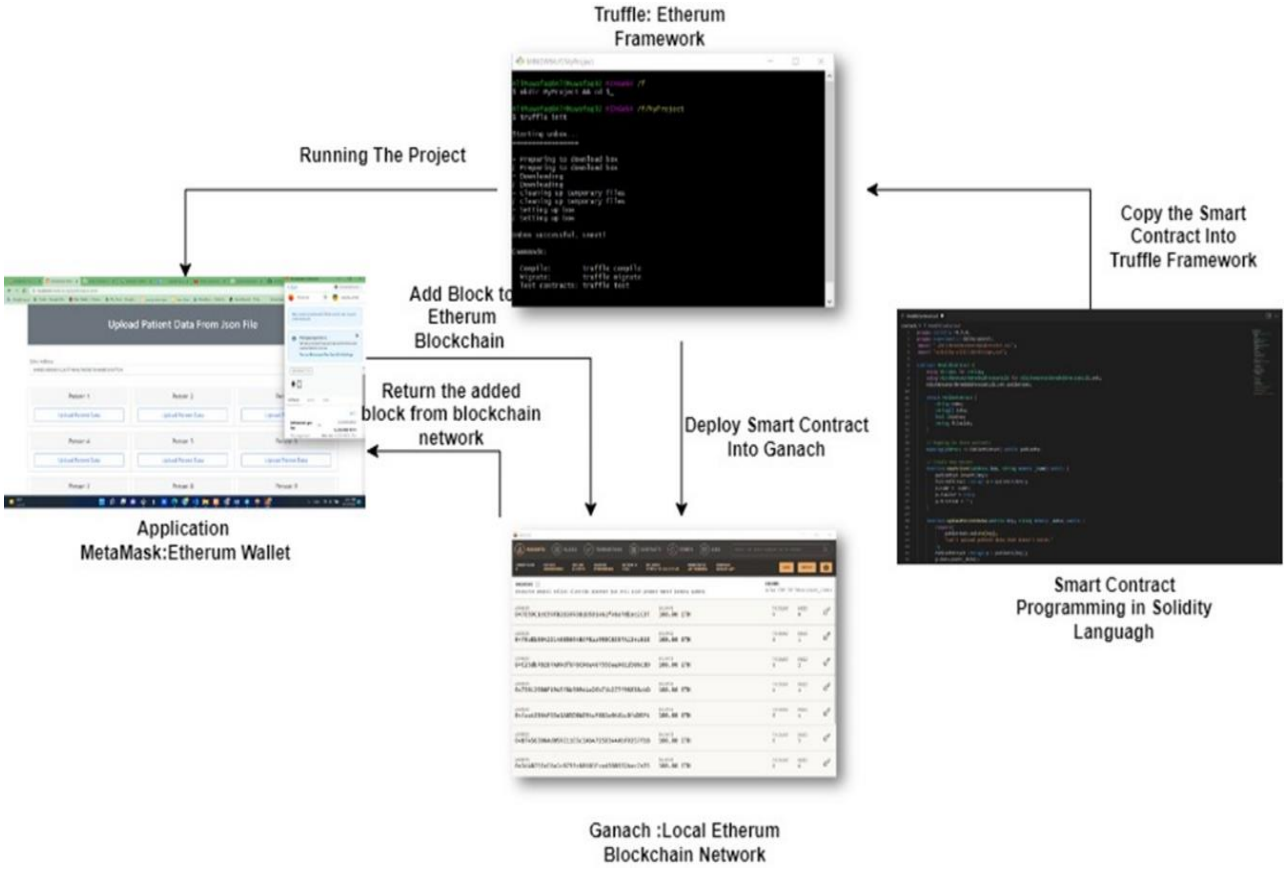


Figure 4.32 Ethereum Environments and its Tools

4.10 Connect Truffle to the Ganache

To connect truffle to the Ganache Ethereum network, improve the environment by trying to call network development and the host (URL) and port. Ganache is already listening on host URL: 127.0.0.1 and the port number: 7545 by using these settings to put the smart contract on the Ethereum. To get started, open truffle-config.js, a JavaScript file at the root of the project directory that can run any code needed to set up the project's configuration

5.1 Conclusions

Mostly in recent years, there have been a lot of Ransomware attacks and their alternatives. These attacks are now clearly targeting health facilities and other places that provide health care. In response to this change, this thesis provides a broad overview of Ransomware attacks in the healthcare industry. Although many studies, such as machine learning, SDN technology, Blockchain technology, etc., have looked at how to detect and prevent Ransomware in the healthcare sector in general, at the moment, Blockchain technology is receiving a lot of attention and research on a large scale. And there is some research on it, such as the consensus mechanism, post-quantum Blockchain technology, and building smart contracts. Also, we can see that Blockchain technology is the best technology that can be used to protect patient records from Ransomware. This is because Blockchain technology is secure, scalable, and immutable and stores information in a decentralized environment.

For this reason, our work is adopted Blockchain technology in order to develop a secure system against Ransomware attacks. Firstly, we simulated the behavior of Ransomware attack software based on the AES encryption algorithm to study and analyze the effect of this software on healthcare patient records. Secondly, we proposed a security system that has the ability to provide protect healthcare patient records from external and internal Ransomware attacks, as well as recover data when any node within the network is exposed to any damage that prevents it from sending its data and sharing in the network.

Each time when any patient sent own data (in our study, the IoT data) over the network, the smart contract checks the patient's own Ether address or/and the metadata of patient transaction to prevent attack links from being sent within the network, where they are immediately rejected. Moreover, the

simulation was made to simulate the Blockchain network when one of the network nodes may be attacked or fails, and it could not send its own transactions. In this situation, it can retrieve the data of these nodes in two ways: randomly selecting the backup copy of one of the network nodes or selecting the node that is nearest to the failed node.

According to the obtained results of the proposed system, it is noted that it reduced the cost of transactions by 855304 Wei by preventing (blocking) all the transmitted records from attackers after detecting it. Hence, the data storage was also decreased because the smart contract allows sending only the correct transactions. Furthermore, the proposed system over Blockchain technology increased the estimated attacker time by 98% compared to the other types of networks. The execution time for raising patient records on Ethereum Network is better than the standard system by 60%.

5.2 Limitation

In this section, some of the limitations are presented which had not been considered in the proposed system.

- The proposed system has not been considering the effect on the network's performance, Because of the focus on the security side
- The other type of attacks that may attack the Blockchain network is not addressed, such as DDOS, botnet and rootkit attacks.
- Difficulty in Implement the new build the smart contracts on the real Blockchain network, because of issues (cost and security).
- In addition, the proposed system has not been evaluated on multiple datasets of varying sizes and formats.

5.3 Future Works

This thesis presents an initial look at creating a multi-peer distributed system using Blockchain technology that can be used in various fields,

taking into consideration the specificity of each field. Below are some areas where it is suggested that the system be applied in future work.

- Implement the smart contracts on a real Blockchain network, for example, the Rinkeby network.
- Design a secure medical application by implementing the proposed system on a testbed (real data for IoT devices).
- Implement the proposed system on the Linux operation system via combining Ethereum with Hyperledger and IPFS technologies.
- Develop the proposed system to protect and prevent the MHRs from other types of attacks like a botnet and, rootkit, DDOS attacks.
- Fix the problem of the vulnerable node with a bigger and broader technology by making an algorithm for faster and better data retrieval and putting it on a real network like Ethereum.

REFERENCES

[1] R. ELGawish, M. Hashim, M. Abo-Rizka, and R. ELGohary, "Detecting Ransomware within Real Healthcare Medical Records Adopting Internet of Medical Things using Machine and Deep Learning Techniques," *Int. J. Adv. Comput. Sci. Appl.*, vol. 13, no. 2, pp. 591–597, 2022, doi: 10.14569/IJACSA.2022.0130270.

[2] R.Sangeetha, B.Harshini, A.Shanmugapriya, and T. K. P. Rajagopal, "Electronic Health Record System using Blockchain," *Int. Res. J. Multidiscip. Technovation*, no. March, pp. 57–61, 2019, doi: 10.34256/irjmt1927.

[3] B. L. Radhakrishnan and A. S. Joseph, "2019 5th International Conference on Advanced Computing and Communication Systems, ICACCS 2019," *2019 5th Int. Conf. Adv. Comput. Commun. Syst. ICACCS 2019*, pp. 699–703, 2019.

[4] N. Thamer and R. Alubady, "A Survey of Ransomware Attacks for Healthcare Systems: Risks, Challenges, Solutions and Opportunity of Research," *1st Babylon Int. Conf. Inf. Technol. Sci. 2021, BICITS 2021*, vol. 2021, no. Bicits, pp. 210–216, 2021, doi: 10.1109/BICITS51482.2021.9509877.

[5] Ayed Al Qartah, "Evolving Ransomware Attacks on Healthcare Providers," no. October, pp. 1–63, 2020, doi: 10.13140/RG.2.2.23202.45765.

[6] M. Humayun, N. Z. Jhanjhi, A. Alsayat, and V. Ponnusamy, "Internet of things and ransomware: Evolution, mitigation and prevention," *Egypt. Informatics J.*, vol. 22, no. 1, pp. 105–117, 2021, doi: 10.1016/j.eij.2020.05.003.

[7] S. Maniath, P. Poornachandran, and V. G. Sujadevi, *Survey on prevention, mitigation and containment of ransomware attacks*, vol. 969. Springer Singapore, 2019. doi: 10.1007/978-981-13-5826-5_3.

[8] S. Tanwar, K. Parekh, and R. Evans, "Blockchain-Based Electronic Healthcare Record System for Healthcare 4.0 Applications," *J. Inf. Secur. Appl.*, vol. 50, pp. 1--13, 2020, doi: 10.1016/j.jisa.2019.102407.

[9] S. Khezr, M. Moniruzzaman, A. Yassine, and R. Benlamri, “Blockchain Technology in Healthcare: A Comprehensive Review and Directions for Future Research,” *Appl. Sci.*, vol. 9, no. 9, pp. 1–28, 2019, doi: 10.3390/app9091736.

[10] N. A. and S. B. G. Ugochukwu, “Blockchain Transforming Cyber-attacks: Healthcare Industry.” University of Malaysia, p. 9, 2020. [Online]. Available: https://www.researchgate.net/publication/347966463_Blockchain_Transforming_Cyber-attacks_Healthcare_Industry

[11] M. M. Jaber *et al.*, “Remotely Monitoring COVID-19 Patient Health Condition Using Metaheuristics Convolute Networks from IoT-Based Wearable Device Health Data,” *Sensors*, vol. 22, no. 3, 2022, doi: 10.3390/s22031205.

[12] J. Scott, “How to Crush the Health Sector’s Ransomware Pandemic,” *Inst. Crit. Infrastruct. Technol.*, no. March, pp. 2–29, 2017, [Online]. Available: https://icitech.org/wp-content/uploads/2017/03/ICIT-Analysis-Artificial-Intelligene-in-the-Health-Sector.pdf

[13] A. O. Almashhadani, M. Kaiiali, S. Sezer, and P. O’Kane, “A Multi-Classifier Network-Based Crypto Ransomware Detection System: A Case Study of Locky Ransomware,” *IEEE Access*, vol. 7, no. c, pp. 47053–47067, 2019, doi: 10.1109/ACCESS.2019.2907485.

[14] M. Hirano and R. Kobayashi, “Machine Learning Based Ransomware Detection Using Storage Access Patterns Obtained from Live-forensic Hypervisor,” *2019 6th Int. Conf. Internet Things Syst. Manag. Secur. IOTSMS 2019*, pp. 1–6, 2019, doi: 10.1109/IOTSMS48152.2019.8939214.

[15] M. Akbanov, V. G. Vassilakis, and M. D. Logothetis, “Ransomware detection and mitigation using software-defined networking: The case of WannaCry,” *Comput. Electr. Eng.*, vol. 76, pp. 111–121, 2019, doi: 10.1016/j.compeleceng.2019.03.012.

[16] R. Kumar, X. Zhang, W. Wang, R. U. Khan, J. Kumar, and A. Sharif, “A

Multimodal Malware Detection Technique for Android IoT Devices Using Various Features," *IEEE Access*, vol. 7, no. c, pp. 64411–64430, 2019, doi: 10.1109/ACCESS.2019.2916886.

[17] D. Akarca, P. Xiu, D. Ebbitt, B. Mustafa, H. Al-Ramadhani, and A. Albeyatti, "Blockchain Secured Electronic Health Records: Patient Rights, Privacy and Cybersecurity," *Conf. Proc. 2019 10th Int. Conf. Dependable Syst. Serv. Technol. DESSERT 2019*, no. June, pp. 108–111, 2019, doi: 10.1109/DESSERT.2019.8770037.

[18] S. Chenthara, K. Ahmed, H. Wang, F. Whittaker, and Z. Chen, *Healthchain: A novel framework on privacy preservation of electronic health records using blockchain technology*, vol. 15, no. 12 December. 2020. doi: 10.1371/journal.pone.0243043.

[19] A. Wani and S. Revathi, "Ransomware protection in loT using software defined networking," *Int. J. Electr. Comput. Eng.*, vol. 10, no. 3, pp. 3166–3174, 2020, doi: 10.11591/ijece.v10i3.pp3166-3175.

[20] C. G. Akcora, Y. Li, Y. R. Gel, and M. Kantarcioglu, "Bitcoin heist: Topological data analysis for ransomware prediction on the bitcoin blockchain," *IJCAI Int. Jt. Conf. Artif. Intell.*, vol. 2021-Janua, pp. 4439–4445, 2020, doi: 10.24963/ijcai.2020/612.

[21] C. Sowthily, S. Senthil Kumar, and M. Brindha, *Detection and Classification of Faults in Photovoltaic System Using Random Forest Algorithm*, vol. 1176, no. Ficta. 2021. doi: 10.1007/978-981-15-5788-0_72.

[22] H. Natarajan, S. K. Krause, and H. L. Gradstein, "Distributed Ledger Technology (DLT) and Blockchain," *FinTech Note*, no. 1, pp. 1–60, 2017.

[23] M. Vatandsoost and S. Litkouhi, "The Future of Healthcare Facilities: How Technology and Medical Advances May Shape Hospitals of the Future," *Hosp. Pract. Res.*, vol. 4, no. 1, pp. 1–11, 2019, doi: 10.15171/hpr.2019.01.

[24] H. Kaur, M. A. Alam, R. Jameel, A. K. Mourya, and V. Chang, "A Proposed

Solution and Future Direction for Blockchain-Based Heterogeneous Medicare Data in Cloud Environment," *J. Med. Syst.*, vol. 42, pp. 1--12, 2018, doi: 10.1007/s10916-018-1007-5.

[25] S. Belfrage, G. Helgesson, and N. Lynøe, "Trust and digital privacy in healthcare: a cross-sectional descriptive study of trust and attitudes towards uses of electronic health data among the general public in Sweden," *BMC Med. Ethics*, vol. 23, no. 1, pp. 1–8, 2022, doi: 10.1186/s12910-022-00758-z.

[26] T. Graves, "A manual for Developing Countries.," in *Community Eye Health / International Centre for Eye Health*, vol. 15, 2002, pp. 64–64.

[27] N. Menachemi and T. H. Collum, "Benefits and drawbacks of electronic health record systems," *Risk Manag. Healthc. Policy*, vol. 4, pp. 47–55, 2011, doi: 10.2147/RMHP.S12985.

[28] AliveCor, "A Guide to Remote Patient Monitoring," *alivecor*, pp. 1–16, 2019, [Online]. Available: https://alivecor.in/images/clinician/AliveCor+Remote+Patient+Monitoring+Guide.pdf

[29] E. Spennato, "3 Key Data Challenges in Health Care Risk Management," *riskandinsurance*, 2019. https://riskandinsurance.com/3-key-data-challenges-in-health-care-risk-management/

[30] R. Agrawal and C. Nyamful, "Challenges of Big Data Storage and Management," *Glob. J. Inf. Technol.*, vol. 6, pp. 1--11, 2016, doi: 10.18844/gjit.v6i1.383.

[31] A. G. Alexandru, I. M. Radu, and M.-L. Bizon, "Big Data in Healthcare - Opportunities and Challenges," *Inform. Econ.*, vol. 22, no. 2/2018, pp. 43–54, 2018, doi: 10.12948/issn14531305/22.2.2018.05.

[32] Y. W. Chiu, Y. H. Weng, Y. Y. Su, C. Y. Huang, Y. C. Chang, and K. N. Kuo, "The Nature of International Health Security," *Asia Pac. J. Clin. Nutr.*, vol. 18, no. 4, pp. 679–683, 2009, doi: 10.6133/apjcn.2009.18.4.32.

[33] A. Jurcut, T. Niculcea, P. Ranaweera, and N. A. Le Khac, “Security Considerations for Internet of Things: A Survey,” *arXiv*, vol. 1, no. 4, pp. 1–19, 2020, doi: 10.1007/s42979-020-00201-3.

[34] S. Askarifar, N. A. Abd Rahman, and H. Osman, “A review of latest wannacry ransomware: Actions and preventions,” *J. Eng. Sci. Technol.*, vol. 13, no. Special Issue on ICCSIT 2018, pp. 24–33, 2018.

[35] A. Muhammad and A. S. Ejiyime, “Analysis of Ransomware, Origin, Threats and Economic Lost on Victims,” *Front. Knowl. J. Ser. | Int. J. Pure Appl. Sci.*, vol. 1, no. 1, pp. 2635–3393, 2017.

[36] S. H. Kok, A. Abdullah, N. Z. Jhanjhi, and M. Supramaniam, “Prevention of crypto-ransomware using a pre-encryption detection algorithm,” *Computers*, vol. 8, no. 4, pp. 1–15, 2019, doi: 10.3390/computers8040079.

[37] F. A. Antariksa, “Ransomware Attack using AES Encryption on ECB, CBC and CFB Mode,” *J. Ilmu Komput.*, vol. 12, no. 1, p. 8, 2019, doi: 10.24843/jik.2019.v12.i01.p06.

[38] H. Lee, K. Lee, and Y. Shin, “Implementation and performance analysis of AES-128 CBC algorithm in WSNs,” *Int. Conf. Adv. Commun. Technol. ICACT*, vol. 1, pp. 243–248, 2010.

[39] M. Andoni *et al.*, “Blockchain Technology in The Energy Sector : A systematic Review of Challenges and Opportunities,” *Renew. Sustain. Energy Rev.*, vol. 100, pp. 143–174, 2019, doi: 10.1016/j.rser.2018.10.014.

[40] Magnus Vitsø Bjørnstad and J. G. H. S. Krogh, “A study on blockchain technology as a resource for competitive advantage,” 2017. [Online]. Available: https://brage.bibsys.no/xmlui/bitstream/handle/11250/2472245/17527_FULLTEXT.pdf?sequence=1

[41] A. V. Aswin, K. Y. Basil, V. P. Viswan, B. Reji, and B. Kuriakose, “Design of AYUSH: A blockchain-based health record management system,” *Lect.*

Notes Networks Syst., vol. 89, pp. 665–672, 2020, doi: 10.1007/978-981-15-0146-3_62.

[42] W.-M. Lee, *Beginning Ethereum Smart Contracts Programming*. 2019. doi: 10.1007/978-1-4842-5086-0.

[43] S. Wang, Y. Zhang, and Y. Zhang, "A blockchain-based framework for data sharing with fine-grained access control in decentralized storage systems," *IEEE Access*, vol. 6, no. c, pp. 38437–38450, 2018, doi: 10.1109/ACCESS.2018.2851611.

[44] V. Kopylash, "An Ethereum-based Real Estate Application with Tampering-resilient Document Storage," 2018.

[45] R. Xu, L. Zhang, H. Zhao, and Y. Peng, "Design of Network Media's Digital Rights Management Scheme Based on Blockchain Technology," *Proc. - 2017 IEEE 13th Int. Symp. Auton. Decentralized Syst. ISADS 2017*, pp. 128–133, 2017, doi: 10.1109/ISADS.2017.21.

[46] Hasil-E-hayaat, A. Priya, A. Khatri, and P. Dixit, "Rise of blockchain technology: Beyond cryptocurrency," *Commun. Comput. Inf. Sci.*, vol. 899, pp. 286–299, 2019, doi: 10.1007/978-981-13-2035-4_25.

[47] Z. Zheng, S. Xie, H. Dai, X. Chen, and H. Wang, "An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends," *Proc. - 2017 IEEE 6th Int. Congr. Big Data, BigData Congr. 2017*, no. June, pp. 557–564, 2017, doi: 10.1109/BigDataCongress.2017.85.

[48] K. Salah, A. Alfalasi, and M. Alfalasi, "A Blockchain-based System for Online Consumer Reviews," *INFOCOM 2019 - IEEE Conf. Comput. Commun. Work. INFOCOM WKSHPS 2019*, pp. 853–858, 2019, doi: 10.1109/INFCOMW.2019.8845186.

[49] B. K. Mohanta, D. Jena, S. S. Panda, and S. Sobhanayak, "Blockchain technology: A survey on applications and security privacy Challenges," *Internet of Things (Netherlands)*, vol. 8, p. 100107, 2019, doi:

10.1016/j.iot.2019.100107.

[50] Y. Xu, S. Zhao, L. Kong, Y. Zheng, S. Zhang, and Q. Li, “ECBC: A High Performance Educational Certi fi cate Blockchain with Ef fi cient Query,” *Springer Int. Publ.*, vol. 1, pp. 288 – 304, 2017, doi: 10.1007/978-3-319-67729-3.

[51] P. Zhang and M. Zhou, “Security and Trust in Blockchains: Architecture, Key Technologies, and Open Issues,” *IEEE Trans. Comput. Soc. Syst.*, vol. 7, no. 3, pp. 790–801, 2020, doi: 10.1109/TCSS.2020.2990103.

[52] R. Alubady and R. Mohammed, “Blockchain-base Healthcare Applications A Survey,” no. May, 2021, [Online]. Available: https://dl.acm.org/doi/10.1145/3376915

[53] S. Seang and D. Torre, “Proof of Work and Proof of Stake Consensus Protocols: a Blockchain Application for Local Complementary Currencies,” *Fr. Univ. Cote d’Azur-GREDEG-CNRS. Str 3.4*, pp. 1–21, 2018.

[54] Zhang and Ren, “Analyzing and Improving Proof-of-Work Consensus Protocols,” no. November, 2019, pp. 1–211.

[55] C. Ganesh, C. Orlandi, and D. Tschudi, “Proof-of-Stake Protocols for Privacy-Aware Blockchains,” vol. 00169, no. 669255, pp. 1–21, 2020.

[56] W. Li, “Securing Proof-of-Stake Blockchain Protocols,” *Data Priv. Manag. Cryptocurrencies Blockchain Technol. Springer, Cham, 2017*, pp. 297–315, 2017, doi: 10.1007/978-3-319-67816-0.

[57] S. De Angelis, L. Aniello, and R. Baldoni, “PBFT vs Proof-of-Authority : Applying the CAP Theorem to Permissioned Blockchain,” *Univ. Southampt.*, pp. 1--12, 2017.

[58] P. Ekparinya and G. Jourjon, “The Attack of the Clones Against Proof-of-Authority,” *arXiv Prepr.*, pp. 1--14, 2020.

[59] H. Baskaran, S. Yussof, and F. A. Rahim, “A Survey on Privacy Concerns in Blockchain Applications and Current Blockchain Solutions to Preserve Data

Privacy," *Commun. Comput. Inf. Sci.*, vol. 1132 CCIS, pp. 3–17, 2020, doi: 10.1007/978-981-15-2693-0_1.

[60] X. Fu, H. Wang, and P. Shi, "A survey of Blockchain consensus algorithms: mechanism, design and applications," *Sci. China Inf. Sci.*, vol. 64, no. 2, pp. 1–15, 2021, doi: 10.1007/s11432-019-2790-1.

[61] S. S. Sarmah, "Understanding Blockchain Technology," *Comput. Sci. Eng.*, vol. 8, no. 2, pp. 23–29, 2018, doi: 10.5923/j.computer.20180802.02.

[62] N. Masinde and K. Graffi, *Peer - to - Peer - Based Social Networks : A Comprehensive Survey*. Springer Singapore, 2020. doi: 10.1007/s42979-020-00315-8.

[63] and H. Weifeng Hao1, Jiajie Zeng1, Xiaohai Dai1, Jiang Xiao1(B), Qiangsheng Hua1, Hanhua Chen1, Kuan-Ching Li2, "BlockP2P: Enabling Fast Blockchain Broadcast with Scalable Peer-to-Peer Network Topology," *Gpc 2019*, vol. 1, pp. 208–222, doi: 10.1007/978-3-030-19223-5.

[64] O. Levasseur, M. Iqbal, and R. Matulevičius, "Survey of Model-Driven Engineering Techniques for Blockchain-Based Applications," *CEUR Workshop Proc.*, vol. 3045, pp. 11–20, 2021.

[65] W. Wang *et al.*, "A Survey on Consensus Mechanisms and Mining Strategy Management in Blockchain Networks," *IEEE Access*, vol. 7, no. c, pp. 22328–22370, 2019, doi: 10.1109/ACCESS.2019.2896108.

[66] N. Masinde and K. Graffi, *Peer-to-Peer-Based Social Networks: A Comprehensive Survey*, vol. 1, no. 5. Springer Singapore, 2020. doi: 10.1007/s42979-020-00315-8.

[67] M. Ball, A. Rosen, M. Sabin, and P. N. Vasudevan, "Average-case fine-grained hardness," *Proc. Annu. ACM Symp. Theory Comput.*, vol. Part F1284, pp. 483–496, 2017, doi: 10.1145/3055399.3055466.

[68] M. F. Sallal, G. Owenson, and M. Adda, "Proximity Awareness Approach to Enhance Propagation Delay on the Bitcoin Peer-to-Peer Network," *Proc. - Int.*

Conf. Distrib. Comput. Syst., pp. 2411–2416, 2017, doi: 10.1109/ICDCS.2017.53.

[69] J. Passerat-Palmbach *et al.*, "Blockchain-orchestrated machine learning for privacy preserving federated learning in electronic health data," *Proc. - 2020 IEEE Int. Conf. Blockchain, Blockchain 2020*, pp. 550–555, 2020, doi: 10.1109/Blockchain50366.2020.00080.

[70] A. Rezvanian and M. R. Meybodi, "Sampling algorithms for weighted networks," *Soc. Netw. Anal. Min.*, vol. 6, no. 1, pp. 1–22, 2016, doi: 10.1007/s13278-016-0371-8.

[71] M. Gong, G. Li, Z. Wang, L. Ma, and D. Tian, "An efficient shortest path approach for social networks based on community structure," *CAAI Trans. Intell. Technol.*, vol. 1, no. 1, pp. 114–123, 2016, doi: 10.1016/j.trit.2016.03.011.

[72] P. Jaillet, "Shortest path problems with node failures," *Networks*, vol. 22, no. 6, pp. 589–605, 1992, doi: 10.1002/net.3230220607.

[73] Y. Shahsavari, K. Zhang, and C. Talhi, "Toward Quantifying Decentralization of Blockchain Networks With Relay Nodes," *Front. Blockchain*, vol. 5, no. February, pp. 1–11, 2022, doi: 10.3389/fbloc.2022.812957.

[74] S. Peyrott, "An Introduction to Ethereum and Smart Contracts," 2017, p. 68. [Online]. Available: https://auth0.com/e-books/intro-to-ethereum

[75] A. T. Pãnescu and V. Manta, "Smart Contracts for Research Data Rights Management over the Ethereum Blockchain Network," *Sci. Technol. Libr.*, vol. 37, no. 3, pp. 235–245, 2018, doi: 10.1080/0194262X.2018.1474838.

[76] K. Delmolino, M. Arnett, A. Kosba, A. Miller, and E. Shi, "Step by Step Towards Creating a Safe Smart Contract : Lessons and Insights from a Cryptocurrency Lab," *International conference on financial cryptography and data security. Springer, Berlin, Heidelberg, 2016*. pp. 79–94, 2015.

[77] J. Jiao, S. Kan, S. W. Lin, D. Sanan, Y. Liu, and J. Sun, "Semantic

understanding of smart contracts: Executable operational semantics of solidity," *Proc. - IEEE Symp. Secur. Priv.*, vol. 2020-May, pp. 1695–1712, 2020, doi: 10.1109/SP40000.2020.00066.

[78] Q. Xu, Z. Song, R. S. M. Goh, and Y. Li, "Building an Ethereum and IPFS-Based Decentralized Social Network System," *Proc. Int. Conf. Parallel Distrib. Syst. - ICPADS*, vol. 2018-Decem, pp. 986–991, 2019, doi: 10.1109/PADSW.2018.8645058.

[79] C. Dannen, "Introducing Ethereum and Solidity," in *Introducing Ethereum and Solidity*, 2017, pp. 139–147. doi: 10.1007/978-1-4842-2535-6_7.

[80] R. Tas and O. O. Tanriover, "Building A Decentralized Application on the Ethereum Blockchain," *3rd Int. Symp. Multidiscip. Stud. Innov. Technol. ISMSIT 2019 - Proc.*, pp. 1–4, 2019, doi: 10.1109/ISMSIT.2019.8932806.

[81] S. K. Panda and S. C. Satapathy, "An Investigation into Smart Contract Deployment on Ethereum Platform Using Web3.js and Solidity Using Blockchain," no. July, pp. 549–561, 2021, doi: 10.1007/978-981-16-0171-2_52.

[82] Q. Wang, R. Li, Q. Wang, S. Chen, M. Ryan, and T. Hardjono, "Exploring Web3 From the View of Blockchain," vol. 2, pp. 1–38, 2022, [Online]. Available: http://arxiv.org/abs/2206.08821

[83] E. Albert, J. Correas, P. Gordillo, G. Román-Díez, and A. Rubio, "GASOL: Gas Analysis and Optimization for Ethereum Smart Contracts," *Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics)*, vol. 12079 LNCS, no. April, pp. 118–125, 2020, doi: 10.1007/978-3-030-45237-7_7.

[84] H. S. Kim and K. Wang, "Immutability measure for different blockchain structures," *2018 IEEE 39th Sarnoff Symp. Sarnoff 2018*, no. February, pp. 1–6, 2018, doi: 10.1109/SARNOF.2018.8720496.

[85] E. Politou, F. Casino, E. Alepis, and C. Patsakis, "Blockchain Mutability:

Challenges and Proposed Solutions," *IEEE Trans. Emerg. Top. Comput.*, vol. 9, no. 4, pp. 1972–1986, 2021, doi: 10.1109/TETC.2019.2949510.

[86] A. Demichev and A. Kryukov, "COMPLETE DECENTRALIZATION of DISTRIBUTED DATA STORAGES BASED on BLOCKCHAIN TECHNOLOGY," *CEUR Workshop Proc.*, vol. 3041, pp. 96–100, 2021, doi: 10.54546/mlit.2021.77.48.001.

[87] X. Chen, S. Tian, K. Nguyen, and H. Sekiya, "Decentralizing private blockchain-iot network with olsr," *Futur. Internet*, vol. 13, no. 7, pp. 1–14, 2021, doi: 10.3390/fi13070168.

[88] A. A. Monrat, O. Schelen, and K. Andersson, "Performance Evaluation of Permissioned Blockchain Platforms," *2020 IEEE Asia-Pacific Conf. Comput. Sci. Data Eng. CSDE 2020*, pp. 1–8, 2020, doi: 10.1109/CSDE50874.2020.9411380.

[89] E. Zhou *et al.*, "Security Assurance for Smart Contract," *2018 9th IFIP Int. Conf. New Technol. Mobil. Secur. NTMS 2018 - Proc.*, vol. 2018-Janua, pp. 1–5, 2018, doi: 10.1109/NTMS.2018.8328743.