

*Republic of Iraq*

*Ministry of Higher Education and Scientific Research*

*University of Babylon*

*College of Information Technology*

*Department of Information Security*

***Medical health care Using Blockchain***

*A Project*

*Submitted to the University of Babylon / College of information technology / Department of Information Security in Partial Fulfilment of the Requirements of the bachelor’s degree in information Security.*

زينب جمال هاشم

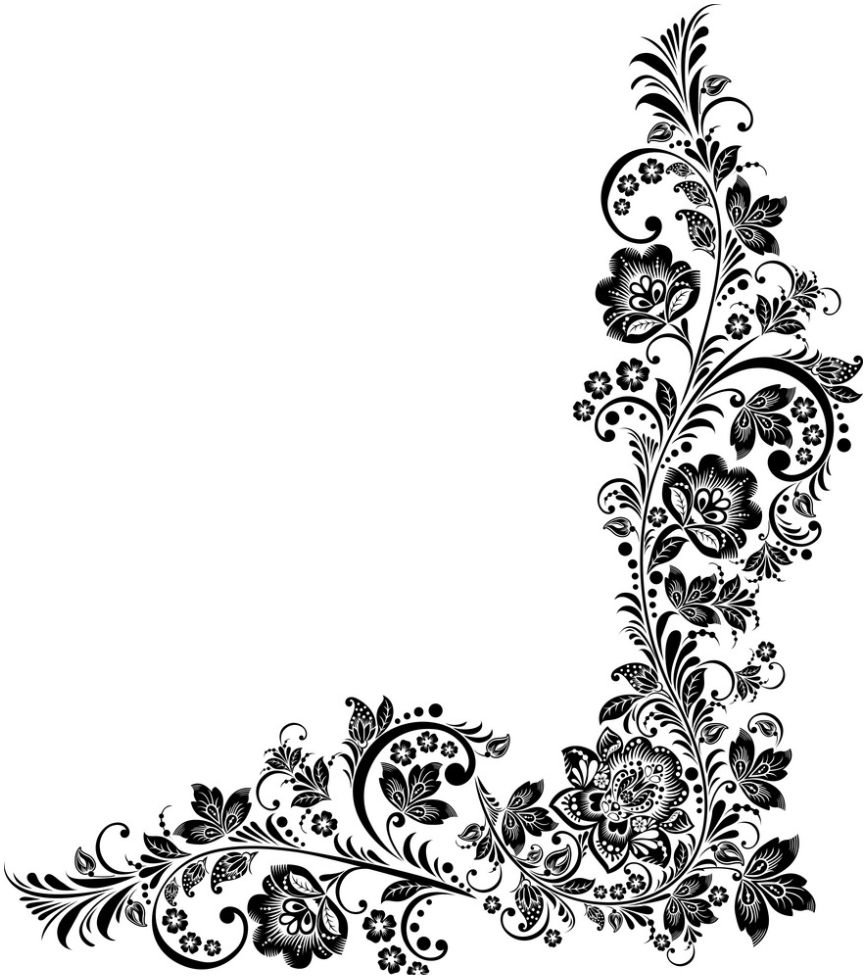
بدور خضير شمير

***بإشراف***

أ. م. د. امنه عطية داوود

**2023 A.D 1444 A.H**

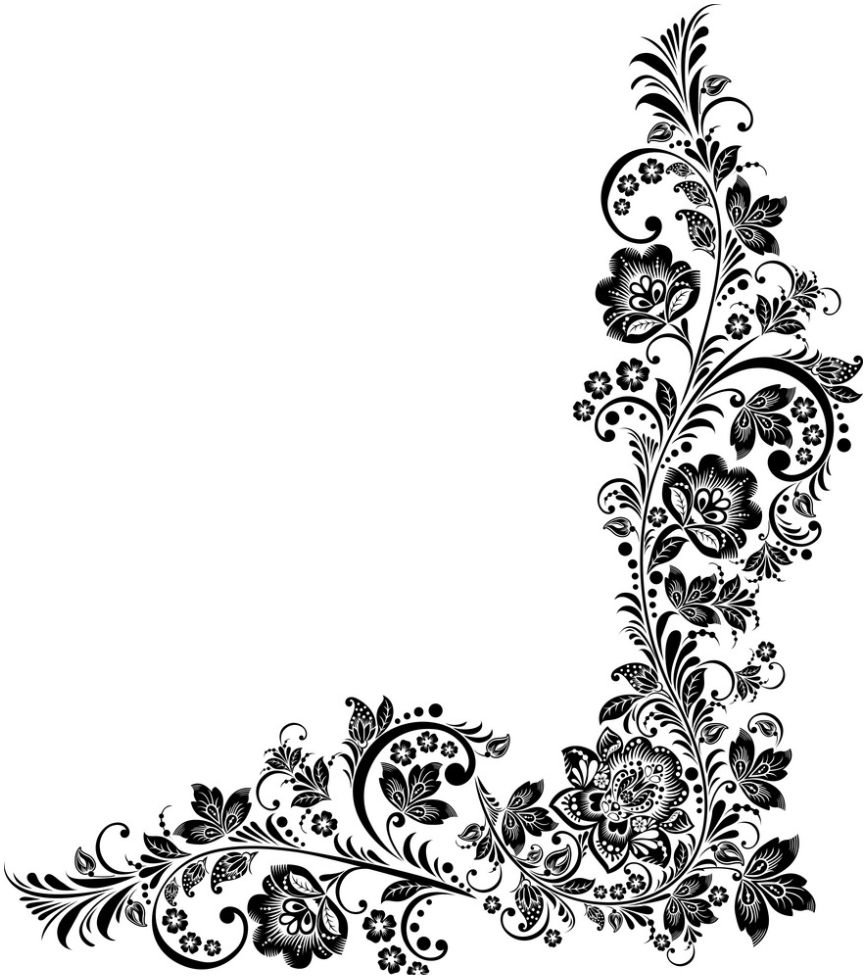






**Dedication**

This study is wholeheartedly dedicated to my beloved parents, who have been my source of inspiration. They gave me the strength when I thought of giving up, and continually provided moral, emotional, and financial support. I wish them all the love and happiness in the world.





**Acknowledgments**

I would like to Express My Gratitude for Everyone Who Helped me during the Graduation Project Starting with Endless Thanks for My Supervisor Dr. Amna Atya, Who does Keep any Effort in encouraging us to do a Great Job, providing me with Valuable Information and Advices to be Better Each Time. Thanks for the Continuous Support and Kind Communication Which Had a Great Effect on me.

Thanks are extended to University of Babylon, College of information technology and Department of Information Security for the Beneficial Lectures Provided Which Facilitated Many Things in our Projects.

Thanks are extended to all Instructors and Doctors Who helped us During the Study Stages.

**Supervisor Certification**

I certify that the Project entitled “Medical health care Using Blockchain” was prepared under my supervision at the Department of information Security / information technology college / University of Babylon , by the students: zainab Jamal , Bedoor Khudaier as partial fulfillment of the requirements of the bachelor's degree in Information Security.

Signature:

Name: Dr. Amna Atya

Date: / / 2023

**The Head of Department Certification**

In view of the available recommendation, I forward the Project entitled “Medical health care Using Blockchain “ for debate by the examination committee.

Signature:

Name: Dr. Alharith A. Abdullah (Prof.)

Date: / / 2023

**Table of Contents**

**Chapter One** ……………………………………………………………………………………………………......1

[1.1 **Introduction** 1](#_Toc45983847)

[1.2 **Background** 1](#_Toc45983848)

[1.3 **Aim of project** 1](#_Toc45983850)

[1.4 **Outline** 1](#_Toc45983851)

**Chapter Two** ……………………………………………………..………….2

[2.1 **Cryptography** 2](#_Toc45983853)

[2.2 **AES** 2](#_Toc45983854)

[2.3 **SHA 256** 3](#_Toc45983855)

[2.4 **Blockchain** 4](#_Toc45983856)

[2.5 **History of Blockchain** 5](#_Toc45983857)

[2.6 **Chaining Blocks** 5](#_Toc45983858)

[2.7 **Medical Health Care Confidentiality** 6](#_Toc45983859)

2.8 **Blockchain And Medical Healthcare Data Security**.......................7

[2.9 **Ways Blockchain Can Secure Health Data** 7](#_Toc45983861)

**Chapter Three**...…………………………………………………………….8

[3.1 **Introduction** 8](#_Toc45983863)

[3.2 **Main design** 8](#_Toc45983864)

[3.3 **Diagram** 9](#_Toc45983865)

**Chapter Four** ……………………………………………………..……….10

[4.1 **Implementation and Results** ...10](#_Toc45983868)

**Chapter Five** …………………………………………………………...….12

[5.1 **Conclusion** 12](#_Toc45983870)

[5.2 **Future** **work** 12](#_Toc45983871)

**Abstract**

The confidentiality and integrity are the important factors in data security. Patients’ medical record is containing on sensitive information which relative to patient. Such as name, address, age, diseases, assurance and so on. To secure and protect this data, there is a need for developing method for this purpose. This project focused on confidentiality and integrity of electronic healthcare records (EHRs). As these two factors in EHR is a critical issue for patients and providers. The patients’ data store in centralized database, which generate weakness and attract hackers’ attention. When attack happened, then the sensitive data will expose. This project focuses on provide confidentiality and integrity for EHR by using blockchain algorithms. Using blockchain in this study will provide decentralized data for patients’ data to prevent the issues which result from centralized data storage. The model adapted blockchain techniques based on The Advanced Encryption Standard (AES) and Secure Hash Function (SHA). This model was built to contribute to the healthcare management systems to allow only the authorized individuals to reach sensitive data.

**Chapter One**

**Overview**

## **1.1 Introduction**

This system is count on in information security, cause it focus on save patients information encrypted completely and can’t be altered. Also it can be separated easily when need to transfer cross network, and also can be reconstruct the blocks with unloosy ways.

## **1.2 Background**

Blockchain were used in this project because it considers a modern way and continues in development in projects that required information security.

And it provides complete needed to all block to get the information.

## **1.3 Aims of project.**

That project aims to provide a secure environment for private medical health care information for patients inside hospitals and connect it all with distributed central database .

## **1.4 Outline**

Chapter Two is going to discuss the theory part of the project.

Chapter Three is about the practical part of the project.

Chapter Four demonstrates the implementations and how to get the results.

Chapter Five is the conclusion of the research and the future work for the project.

**Chapter Two**

**Theory Part**



**2.1 Cryptography**

Cryptography is the science of using mathematics to encrypt and decrypt data. Cryptography enables you to store sensitive information or transmit it across insecure networks (like the Internet) so that it cannot be read by anyone except the intended recipient.

While cryptography is the science of securing data, cryptanalysis is the science of analyzing and breaking secure communication. Classical cryptanalysis involves an interesting combination of analytical reasoning, application of mathematical tools, pattern finding, patience, determination, and luck. Cryptanalysts are also called attackers.

* ‘Cryptography is the science of using mathematics to encrypt and decrypt data’ Phil Zimmermann
* ‘Cryptography is the art and science of keeping messages secure’ Bruce Schneier

**2.2** **AES**

AES is one of the widely accepted encryption algorithms used for encryption. AES holds its own unique structure for encryption and decryption. AES can deal with three different key sizes such as AES 128, 192 and 256 bit and each of these ciphers has 128-bit block size. The number of rounds is based on the key length. The size of the key decides the number of rounds such as AES uses 10 rounds for 128-bit keys, 12 rounds for 192-bit keys and 14 rounds for 256-bit keys. From Fig.1, we can infer that AES encryption algorithm is more mathematically efficient and elegant cryptographic algorithm and exponentially stronger than the DES encryption algorithm [1]

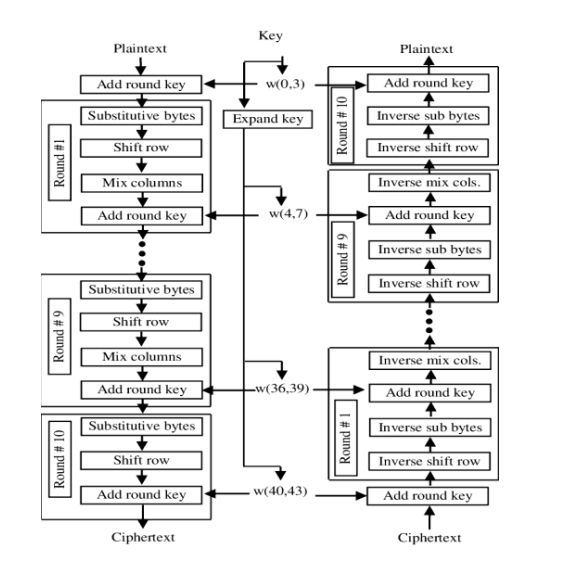
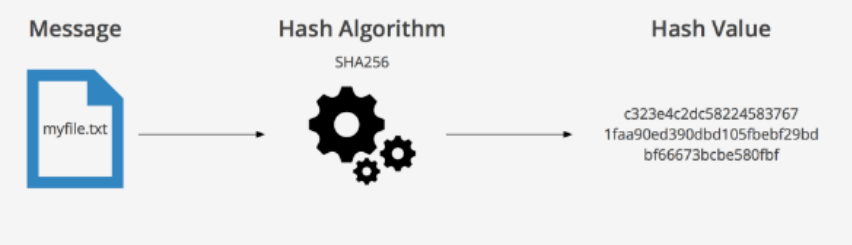


Fig 2.1

**2.3** **SHA 256**

SHA 256 is the cryptography encryption algorithm, which is the advancement of SHA-1 and it is one of the strongest hash functions available. It has not compromised by others till date. It provides a unique 256-bit hash code, also known as signature for a text or a data file. By comparing the calculated "hash value" to a known and expected hash value, data's integrity can be determined. The hash value as in Fig.2 is a one-way code generated from the sender’s side and it cannot secure the file or data in the file. The hash code generated from the hash function is used only for authentication purpose and not for the encryption or security purposes. The hash code can only guarantee the integrity but not the confidentiality of the data or the file that is transferred.

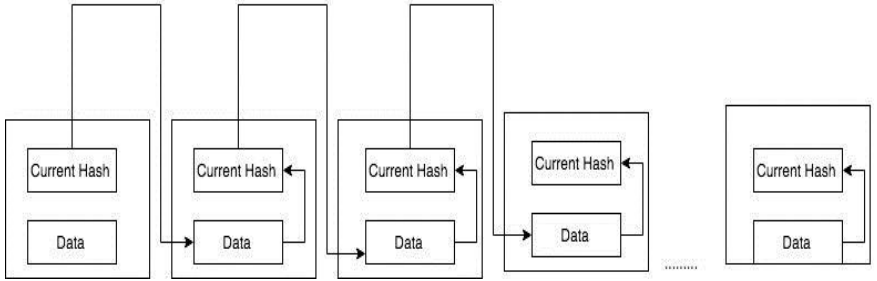


**Fig 2.2**

**2.4** **Blockchain**

In recent times, blockchain technology has been a growing technology and it is in use in various applications like bitcoin transactions, file transfer, record keeping and in many other applications. Blockchain uses a hash function to get the hash codes which is used to link two blocks in the blockchain. In a large network, the hash codes are difficult to compromise but in smaller networks, the hacker always finds a way to hack the network. In such cases, the data can be secured by using the more popular and widely used encryption algorithm, AES before hashing a file.[2]

A blockchain, as in Fig.3 is a chain of blocks or is a growing list of data, called blocks, which are linked together with the help of cryptography. Each data blocks contains a cryptographic hash code of the block before it, a timestamp, and the data to be transmitted. Modification of data in the blockchain is not allowed. When a data in a block is changed, it affects the upcoming blocks and hence the whole blockchain changes.



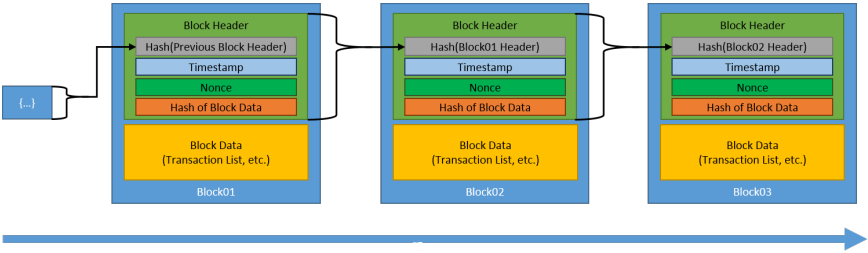
**Fig 2.3**

**2.5 History of Blockchain**

The core ideas behind blockchain technology emerged in the late 1980s and early 1990s. In 1989, Leslie Lamport developed the Paxos protocol, and in 1990 submitted the paper The Part Time Parliament [3] to ACM Transactions on Computer Systems; the paper was finally published in a 1998 issue. The paper describes a consensus model for reaching agreement on a result in a network of computers where the computers or network itself may be unreliable. In 1991, a signed chain of information was used as an electronic ledger for digitally signing documents in a way that could easily show none of the signed documents in the collection had been changed [4]. These concepts were combined and applied to electronic cash in 2008 and described in the paper, Bitcoin: A Peer to Peer Electronic Cash System [5], which was published pseudonymously by Satoshi Nakamoto, and then later in 2009 with the establishment of the Bitcoin cryptocurrency blockchain network. Nakamoto’s paper contained the blueprint that most modern cryptocurrency schemes follow (although with variations and modifications). Bitcoin was just the first of many blockchain applications.

**2.6** **Chaining Blocks**

Blocks are chained together through each block containing the hash digest of the previous block’s header, thus forming the blockchain. If a previously published block were changed, it would have a different hash. This in turn would cause all subsequent blocks to also have different hashes since they include the hash of the previous block. This makes it possible to easily detect and reject altered blocks. Fig.4 shows a generic chain of blocks.



**Fig 2.4**

**2.7 Medical Health Care Confidentiality**

The quantity and type of health care information now collected has also increased dramatically in recent years. The participation in health care delivery of many different individuals and groups of providers exerts strong pressures to document in ever greater detail. The expanding numbers of available technologies for diagnosis and therapy mean that details that a provider could at one time recall must now be recorded and thus become available for inspection by others. Further, information on lifestyle (e.g., use of tobacco or alcohol), family history, and health status have become of greater interest and relevance as we learn more about the relationship of these factors to overall health and well-being. In addition, genetic data are becoming more readily available, not only for prenatal testing but also for assessing an individual's degree of risk for an inherited condition [6]

**2.8** **Blockchain and Medical Healthcare Data Security**

Keeping medical data safe and secure is the most popular blockchain healthcare application now, which isn’t surprising. Security is a major issue in the healthcare industry. There were 692 large healthcare data breaches reported between July 2021 and June 2022. The perpetrators stole credit cards and banking information, as well as health and genomic testing records.

Blockchain’s ability to keep an incorruptible, decentralized, and transparent log of all patient data makes it a technology ideal for security applications. Additionally, while blockchain is transparent, it is also private, concealing the identity of any individual with complex and secure codes that can protect the sensitivity of medical data. The decentralized nature of the technology also allows patients, doctors, and healthcare providers to share the same information quickly and safely.

**2.9 Ways Blockchain Can Secure Health Data**

* Decentralized data logs that are incorruptible and transparent
* Complex codes that protect individuals’ identities and data
* Quick transfers reduce the window in which data is vulnerable.

**Chapter Three**

**Practical Part**



**3.1 Introduction**

In this chapter we will walk you through the process of making the system module from start to finish and include the source code parts and give a simple explanation of that code. We will also provide a simple diagram of the functions of the system.

**3.3 Main design**

1. The first screen that appears is asking the user of two Operation he can do either want to enter information about new patient and save it or want to search throw database about one specific.
2. If user choose to Add information the system asked him to provide some info
3. The information that comes from the user go to Class to be process to form can be used in blockchain, first splits into Blocks then encrypted by AES algorithm and become ready to save to database.
4. The blockchain that has been created saved to SQLite database with unique identifier called UUID (Universally Unique IDentifier).
5. The identifier and patient name saved in SQLite database called **DataCenter**.
6. When user want to search about patient need just to type his/her name to present the information that saved in his/her database.

**3.3 Diagram**

**Add New Information**

**User**

**Information splits into Blocks**

**Encrypt The Blocks**

**Blocks padded into AES Block**

**Save The identifier of patient database in central Database.**

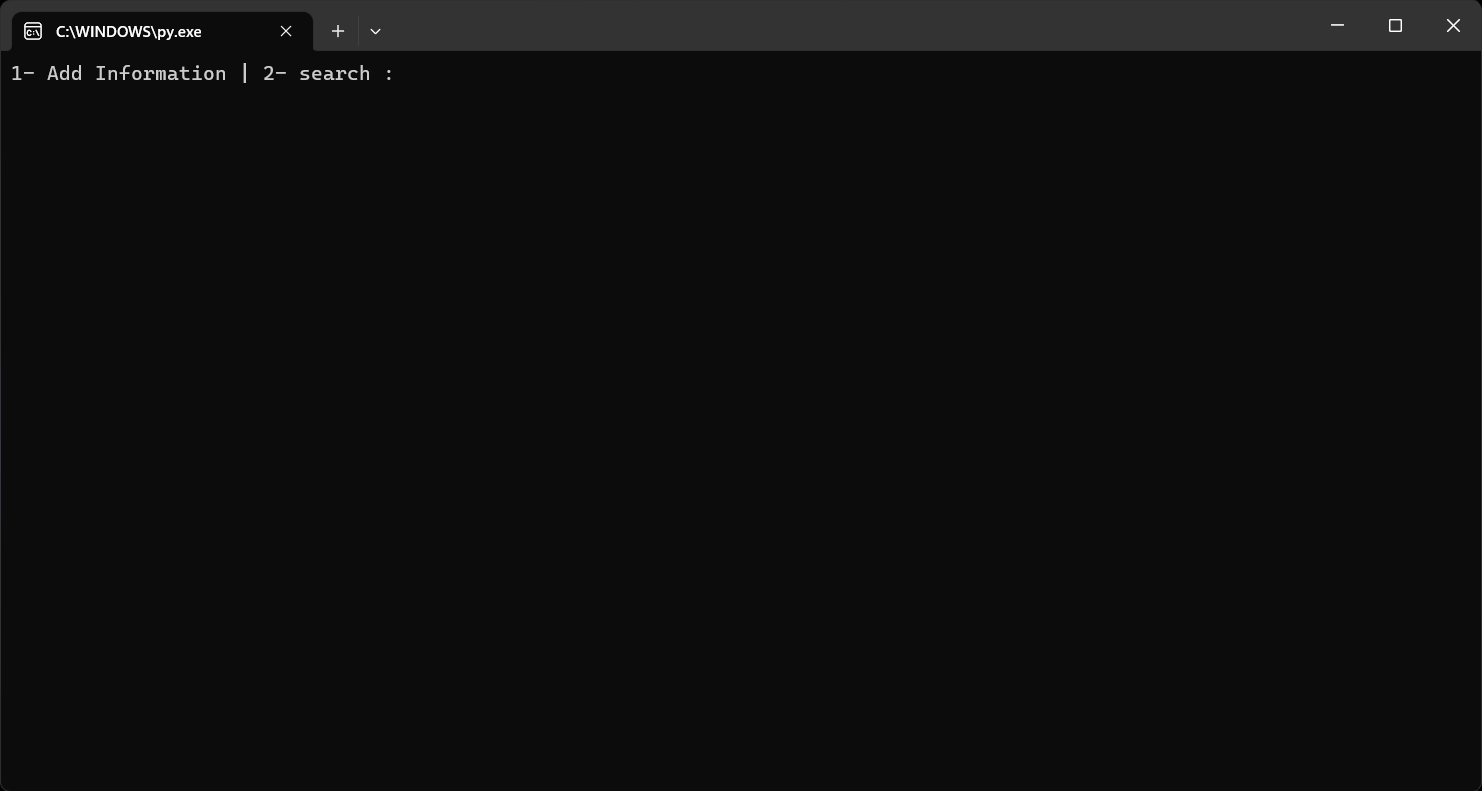
**Create Database for the patent.**

**Chapter Four**

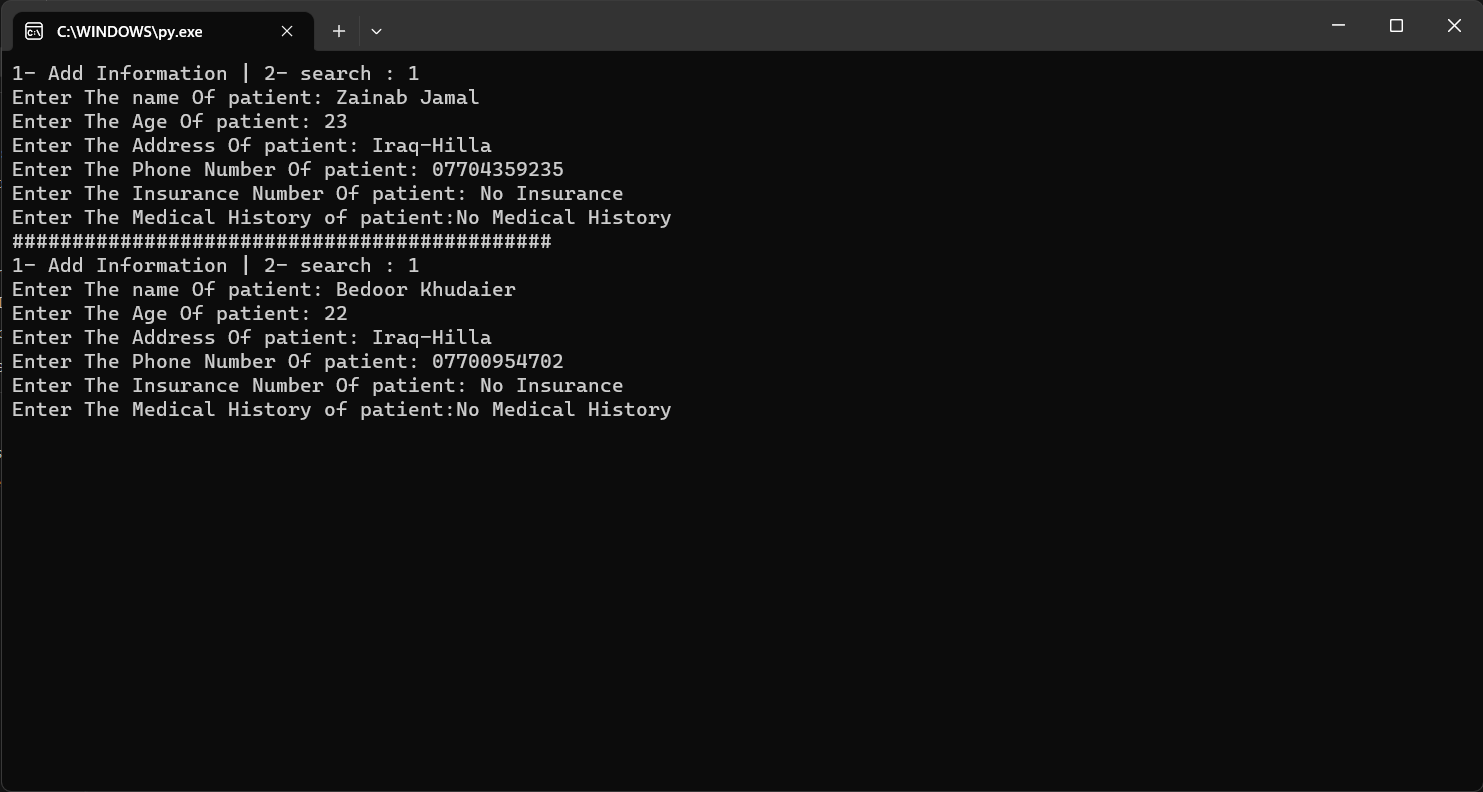
**Implementation and Results**



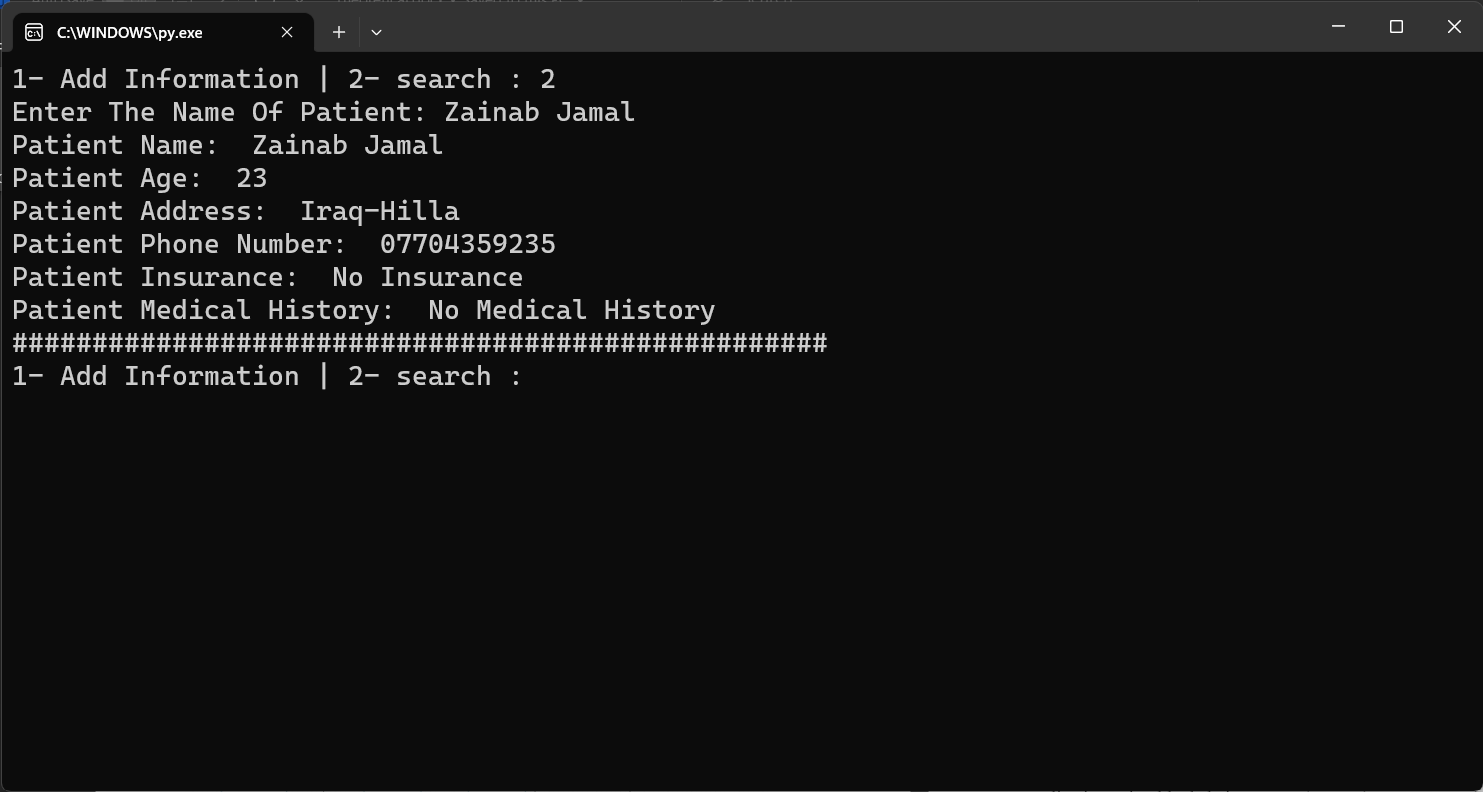
**4.1 Implementation and Results**



1. **The first step is opening the program with python interpreter.**



1. **Choosing first Choice to add Information of patients.**



1. **Choosing second choice to search about patients and show the information.**

**Chapter five**

**Conclusion and Future work**



**5.1 Conclusion**

The purpose of this project was to build an easy-to-understand system that has all the information the user needs about the data of patients.

The privacy of patients information is the most important thing cause it maybe leads to problems if it’s disclosure. With the use of Blockchain we can avoid that.

**5.2 Future work**

In a future not so far ahead, I’d like to do these following things to the project to make it much better than now:

* Add Interactive GUI to the project.
* Make It online Project So it can be used anywhere with specific permissions.

**References**

[1] AkoMuhamad Abdullah,” Advanced Encryption Standard (AES) Algorithm to Encrypt and Decrypt Data” 2017.

[2] SriBalaji, Vignesh Mohan, Soundarya, “Secure and decentralized file transfer application using blockchain”, ISSN (PRINT): 2393-8374, (ONLINE): 2394-0697, VOLUME-4, ISSUE-4, 2017.

[3] Lamport, Leslie. “The Part-Time Parliament.” ACM Transactions on Computer Systems, vol. 16, no. 2, Jan. 1998, pp. 133–169.,

[4] Narayanan, A., Bonneau, J., Felten, E., Miller, A., and Goldfede, S., Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction, Princeton University Press, 2016.

[5] Nakamoto, S., “Bitcoin: A Peer-to-Peer Electronic Cash System,” 2008.

[6] An IOM report on assessing genetic risk explores these issues in considerable detail and develops a strong pro-privacy stance (IOM, 1993b).