# BLOCKCHAIN: A PANACEA FOR HEALTHCARE CLOUD-BASED DATA SECURITY AND PRIVACY

S.Monika, Sujana G N, Supriya.K ,Varshini .N, Prashanth H.S
K.S.Institute of Technology,Bangalore

**ABSTRACT**

*The main objective of this project is securely store and maintain the patient records in the healthcare. Healthcare is a data-intensive domain where a large amount of data is created, disseminated, stored, and accessed daily. The blockchain technology is used to protect the healthcare data hosted within the cloud. The block that contain the medical data and the timestamp. Cloud computing will connect different healthcare providers. It allows healthcare provider to access the patient details more securely from anywhere. It preserve data from attackers. The data is encrypted prior to outsourcing to the cloud. The healthcare provider have to decrypt the data prior to download*

**Keyword :** *Block Chain, Healthcare ,security, privacy ,cloud, etc*

## 1. INTRODUCTION

Cloud computing offers an opportunity for individuals and companies to offload to powerful servers the burden of managing large amounts of data and performing computationally demanding operations. Due to the increasing popularity of cloud computing, more and more Data owners are motivated to outsource their data to cloud servers for great convenience and reduced cost in data management. Data owners offer services to a large number of businesses and companies, they stick to high security standards to improve data security by following a layered approach that includes data encryption, key management, strong access controls, and security intelligence. Healthcare is a data-intensive domain where a large amount of data is created, disseminated, stored, and accessed daily. It is clear that technology can play a significant role in enhancing the quality of care for patients (e.g. leveraging data analytics to make informed medical decisions) and potentially reduce costs by more efficiently allocating resources in terms of personnel, equipment, etc. Generally, Electronic Medical Records (EMRs) contain medical and clinical data related to a given patient and stored by the responsible healthcare provider. This facilitates the retrieval and analysis of healthcare data. To better support the management of EMRs, early generations of Health Information Systems (HIS) are designed with the capability to create new EMR instances, store them, and query and retrieve stored EMRs of interest.2 HIS can be relatively simple solutions, which can be schematically described as a graphical user interface or a web service. These are generally the front-end with a database at the back-end, in a centralized or distributed implementation. With patient mobility (both internally and externally to a given country) being increasingly the norm in today's society, it became evident that multiple stand-alone EMR solutions must be made interoperable to facilitate sharing of healthcare data among different providers, even across national borders, as needed. For example, in medical tourism hubs such as Singapore, the need for real-time healthcare data sharing between different providers and across nations becomes more pronounced. To facilitate data sharing or even patient data portability, there is a need for EMRs to formalize their data structure and the design of HIS. Electronic Health Records (EHRs), for example, are designed to allow patient medical history to move with the patient or be made available to multiple healthcare providers (e.g. from a rural hospital to a hospital in the capital city of the country, before the patient seeks medical attention at another hospital in a different country).3 EHRs have a richer

data structure than EMRs. There have also been initiatives to develop HIS and infrastructures that are able to scale and support future needs, as evidenced by the various national and international initiatives such as the Fascicolo Sanitario Elettronico (FSE) project in Italy, the epSOS project in Europe, and an ongoing project to standardize sharing of EHRs. Recently, the pervasiveness of smart devices (e.g. Android and iOS devices and wearable devices) has also resulted in a paradigm shift within the healthcare industry. Such devices can be user-owned or installed by the healthcare provider to measure the well-being of the users (e.g. patients) and inform/facilitate medical treatment and monitoring of patients. For example, there is a wide range of mobile applications (apps) in health, fitness, weight-loss, and other healthcare related categories. These apps mainly function as a tracking tool, such as registering user exercises/workouts, keeping the count of consumed calories, and other statistics (e.g. number of steps taken), and so on. There are also devices with embedded sensors for more advanced medical tasks, such as bracelets to measure heartbeat during workouts, or devices for self-testing of glucose. The data (e.g. user's vital signs) can be continuously gathered and sent in real-time to a smart device, before being sent to a remote healthcare cloud for further analysis. Another example is Ambient Assisted Living solutions for healthcare designed to realize innovative telehealth and telemedicine services, in order to provide remote personal health monitoring. These developments have paved the way for Personal Health Records (PHR), where patients are more involved in their data collection, monitoring of their health conditions, etc, using their smart phones or wearable devices (e.g. smart shirts and smart socks). Blockchain was originally designed to record transaction data, which is relatively small in size and linear. In other words, one only concerns itself about whether the current transaction can be traced backwards to the original ―deall.

## 2. OBJECTIVE

- The main objective of this project is securely store and maintain the patient records in the healthcare. Healthcare is a data-intensive domain where a large amount of data is created, disseminated, stored, and accessed daily
- The blockchain technology is used to protect the healthcare data hosted within the cloud. The block that contain the medical data and the timestamp.
- Cloud computing will connect different healthcare providers.
- It allows healthcare provider to access the patient details more securely from anywhere.
- It preserve data from attackers. The data is encrypted prior to outsourcing to the cloud. The healthcare provider have to decrypt the data prior to download.
- Finally our model ensure the data security for accessing the patient record over the cloud.

## 3. LITERATURE SURVEY

**Outsourced symmetric private information retrieval S. Jarecki, C. Jutla, H. Krawczyk, M. Rosu, and M. Steiner**

Outsourcing is the process of contracting an existing business process which an organization previously performed internally to an independent organization, where the process is purchased as a service. The data owner enables SSE Scheme and outsources a document or collection of files to a remote server in encrypted form. And also the data owner authorizes clients (third parties) to search the database to learn. The remote server still does not learn about the data or queried values as in the basic SSE setting. We extend the OXT protocol of Cash et al. to support arbitrary Boolean queries in all of the above models while withstanding adversarial non-colluding servers (Data owner and remote server) and arbitrarily malicious clients to preserve the remarkable performance of the protocol.

**Dynamic search-able symmetric encryption S. Kamara, C. Papamanthou, and T. Roeder**

Searchable symmetric encryption (SSE) allows a client to encrypt data in such a way that it can later generate search tokens to send as queries to a storage serve. We propose the first SSE scheme to satisfy all the properties like sub-linear search time and so-on. Extends the inverted index approach in several non-trivial ways and introduces new

techniques for the design of SSE. We implement our scheme and conduct a performance evaluation, showing that our approach is highly efficient and ready for deployment

**Highly-scalable searchable symmetric encryption with support for Boolean queries D. Cash, S. Jarecki, C. Jutla, H. Krawczyk, M. Rosu, and M. Steiner**

The design, analysis and implementation of the first searchable symmetric encryption (SSE) protocol that supports conjunctive search and general Boolean queries on outsourced symmetrically-encrypted data and that scales to very large databases and arbitrarily-structured data including free text search. Our solution provides a realistic and practical trade-off between performance and privacy by efficiently supporting very large databases at the cost of moderate and well-defined leakage to the outsourced serve.

**Parallel and Dynamic Searchable Symmetric Encryption S. Kamara and C. Papamanthou**

Searchable symmetric encryption (SSE) enables a client to outsource a collection of encrypted documents in the cloud and retain the ability to perform keyword searches without revealing information about the contents of the documents and queries. Although efficient SSE constructions are known, previous solutions are highly sequential. This is mainly due to the fact that, currently, the only method for achieving sub-linear time search is the inverted index approach which requires the search algorithm to access a sequence of memory locations, each of which is unpredictable and stored at the previous location in the sequence. Motivated by advances in multi-core architectures, we present a new method for constructing sub-linear SSE schemes. Our approach is highly parallelizable and dynamic.

## 3. EXISTING SYSTEM

Existing system doesn't maintain and process the data securely. It doesn't provides the more accurate search result. Incorrect and misleading of data will produce the wrong analysis result. Low search Efficiency. The search delay of the scheme is proportional to the size of the database. It is not suitable for the large scale databases.

DISADVANTAGES

- Low search Efficiency
- The search delay of the scheme is proportional to the size of the database.
- It is not suitable for the large scale databases.
- Doesn't support verification upon file update.
- Data Integrity attacks.

## 4. PROPOSED SYSTEM

To overcome the security problems that are occurred in the existing system and effectively store the data over the cloud we introduce this system. The data user outsources the encrypted documents to the cloud. The Data user get the each result, the proof and the public verification key, they itself or others can verify the freshness, authenticity, and completeness of the search result even without decrypting them.

ADVANTAGES

- Efficient Search Result.
- Prevents data freshness attacks and data integrity attacks.
- It provides High Security.
- Files can be easily updated.

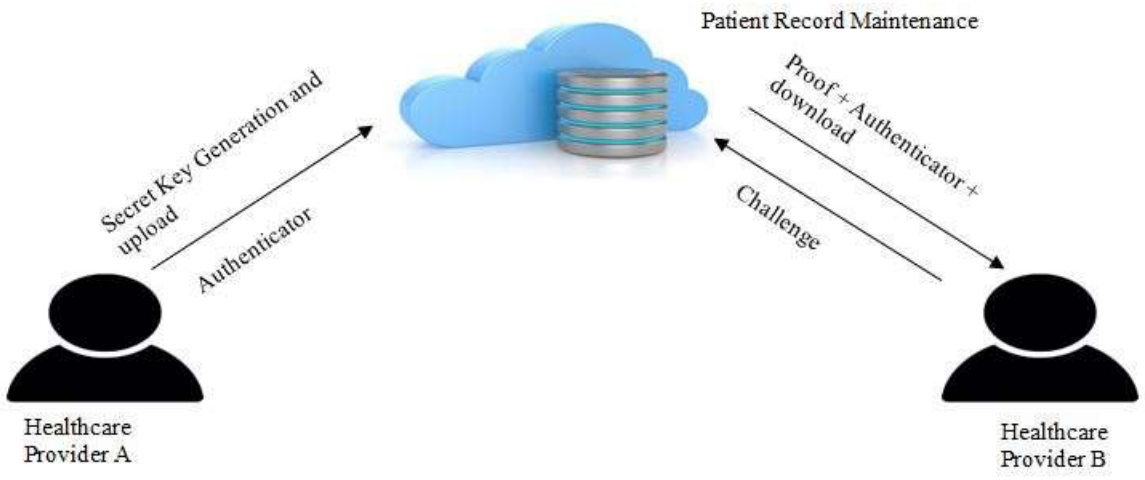


Fig: Architechture diagram

.

## 5. CONCLUSIONS

It's more securely maintain all the patient records and it will be easily accessible by any healthcare providers. By building block chain, it provides efficient search result verification, while preventing data freshness attacks and data integrity attacks in SSE**.**

## 6. ACKNOWLEDGEMENT

We would like to express our special thanks to Mr. Prashanth H S sir, for their guidance and support during the planning and development of this project. We would also like to thank all the professors of KSIT for their continuous support and encouragement**.**

## 6. REFERENCES

[1]. M. Steward, ―Electronic Medical Records,‖ Journal of Legal Medicine, vol. 26, no. 4, 2005, pp. 491–506
[2]. K. Häyrinena et al., ―Definition, Structure, Content, Use and Impacts of Electronic Health Records: A Review of the Research Literature,‖ Int'l Journal of Medical Informatics, vol. 77, no. 5, 2008, pp. 291–304.
[3]. M. Ciampi et al., ―A Federated Interoperability Architecture for Health Information Systems,‖ Int'l Journal of Internet Protocol Technology, vol. 7, no. 4, 2013, pp. 189– 202.
[4]. M. Moharra et al., ―Implementation of a CrossBorder Health Service: Physician and Pharmacists' Opinions from the epSOS Project,‖ Family Practice, vol. 32, no. 5, 2015,
[5]. S.H. Han et al., ―Implementation of Medical Information Exchange System Based on EHR Standard,‖ Healthcare Informatics Research, vol. 16, no. 4, 2010, pp. 281–289.
[6]. D. He et al., ―A Provably-Secure CrossDomain Handshake Scheme with SymptomsMatching for Mobile Healthcare Social Network,‖ IEEE Transactions on Dependable and Secure Computing, vol. PP, no. 99, 2016; doi.org/DOI: 10.1109/TDSC.2016.2596286.
[7]. F.Y. Leu et al., ―A Smartphone-Based Wearable Sensors for Monitoring Real-Time Physiological Data,‖ Computers and Electrical Engineering, 2017