HiPPRule: Hippocratic Rule-based Privacy Preservation Contract Scheme for Healthcare 5.0 Ecosystems

Submitted By

PATEL MANASHRI DHARESH

20MCEI19

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

INSTITUTE OF TECHNOLOGY

NIRMA UNIVERSITY

AHMEDABAD-382481

May 2022

HiPPRule: Hippocratic Rule-based Privacy Preservation Contract Scheme for Healthcare 5.0 Ecosystems

Major Project

Submitted in partial fulfillment of the requirements

for the degree of

Master of Technology in Computer Science and Engineering

Submitted By

PATEL MANASHRI DHARESH

(20MCEI19)

Guided By

Prof. Vivek Prasad

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

INSTITUTE OF TECHNOLOGY

NIRMA UNIVERSITY

AHMEDABAD-382481

May 2021

Certificate

This is to certify that the major project entitled ***HiPPRule*: Hippocratic Rule-based Privacy Preservation Contract Scheme for Healthcare 5.0 Ecosystems** submitted by **Prof. Vivek Prasad (20MCEI19)**, towards the partial fulllment of the requirements for the award of degree of Master of Technology in Computer Science and Engineering of Nirma University, Ahmedabad, is the record of work carried out by him under my supervision and guidance. In my opinion, the submitted work has reached a level required for being accepted for examination. The results embodied in this Major Project, to the best of my knowledge, haven't been submitted to any other university or institution for award of any degree or diploma.

Prof. Vivek Prasad
Internal Guide & Associate Professor
CSE Department
Institute of Technology
Nirma University, Ahmedabad

Dr Sharada Valiveti
Professor & PG Coordinator (M.Tech - INS)
CSE Department
Institute of Technology
Nirma University, Ahmedabad

Dr Madhuri Bhavsar
Professor & Head
CSE Department
Institute of Technology
Nirma University, Ahmedabad

Dr Rajesh Patel
Director
Institute of Technology
Nirma University, Ahmedabad

Statement of Originality

I, **PATEL MANASHRI DHARESH**, **20MCEI19**, give undertaking that the Major Project entitled ***HiPPRule*: Hippocratic Rule-based Privacy Preservation Contract Scheme for Healthcare 5.0 Ecosystems** submitted by me, towards the partial fulfillment of the requirements for the degree of Master of Technology in **Computer Science & Engineering** of Institute of Technology, Nirma University, Ahmedabad, contains no material that has been awarded for any degree or diploma in any university or school in any territory to the best of my knowledge. It is the original work carried out by me and I give assurance that no attempt of plagiarism has been made.It contains no material that is previously published or written, except where reference has been made. I understand that in the event of any similarity found subsequently with any published work or any dissertation work elsewhere; it will result in severe disciplinary action.

____

Signature of Student
Date:
Place:

Endorsed by
Prof. Vivek Prasad
(Signature of Guide)

Acknowledgements

It gives me immense pleasure in expressing thanks and profound gratitude to **Prof. Vivek Prasad**, Assistant Professor, Computer Science and Engineering Department, Institute of Technology, Nirma University, Ahmedabad for his valuable guidance and continual encouragement throughout this work. The appreciation and continual support he has imparted has been a great motivation to me in reaching a higher goal. His guidance has triggered and nourished my intellectual maturity that I will benefit from, for a long time to come.

It gives me an immense pleasure to thank **Dr Madhuri Bhavsar** , Hon'ble Head of Computer Science And Engineering Department, Institute of Technology, Nirma University, Ahmedabad for her kind support and providing basic infrastructure and healthy research environment.

A special thank you is expressed wholeheartedly to **Dr Rajesh Patel**, Hon'ble Director, Institute of Technology, Nirma University, Ahmedabad for the unmentionable motivation she has extended throughout course of this work.

I would also thank the Institution, all faculty members of Computer Science and Engineering Department, Nirma University, Ahmedabad for their special attention and suggestions towards the project work.

-Patel Manashri Dharesh
20MCEI19

Abstract

Medical technology has advanced dramatically as a result of technological advancements. With the help of medical technology, accurate medical data on patients may be acquired, resulting in an increase in the amount of medical information collected. The patient's records contain sensitive information that, when shared with other hospital employees, hospitals, or insurance companies, should maintain the privacy of the patient without disclosing it. The publication of sensitive data by data providers is frequently limited to specific users for specific objectives. As a result, when the data is disclosed, maintaining the privacy of the sensitive data about the patient is a must. The Hippocratic database was created to ensure privacy in relational database systems where access decisions are made based on privacy policies and authorization tables. Purpose trees are intended to capture purpose hierarchies so that information can be delivered to users according to purposes, providing more data access options. SQL was employed for searching and constructing relationships between multiple data entries. To authenticate the other party before sending the sensitive data, we use a smart contract.

List of Figures

List of Tables

Contents

Chapter 1

Introduction

In recent years, the health-care industry has begun to emphasise the customization of products with unique and distinctive requirements for patients with various diseases or ailments. We need to think about a human-centric approach that incorporates IoT and AI in healthcare, especially in light of the COVID era's *New Normal*. Patients' and healthcare professionals' tailored needs can be met in Industry 5.0, often known as the fifth industrial revolution. Industry 4.0 allowed for mass customization, while industry 5.0 requires healthcare professionals to move according to a user's specific needs. Interconnected machines in Industry 5.0 have a lot of potential for customisation, which can cater to the needs of the users. With there being digital transformation, there will be great enhancement in terms of quality, safety, and waste reduction. We require better designed studies to examine healthcare research effectively. Design studies are becoming more prominent as a type of problem-solving research. We've found a unique design study technique that will help us incorporate the Healthcare 5.0 research into our study.

According to Coughlin *et al* [1] in a report published in the Internal Medical Journal, the healthcare sector was chosen because it will generate at least 6 percentage more data annually than other data-generating industries such as manufacturing, financial services, and media-entertainment. Healthcare data comprises sensitive information about the patient which the patient might not want to release. These sensitive attributes must be hidden from entities such as doctors, nurses, laboratories, and so on. One of the most important considerations for users when choosing a healthcare database system is ensuring privacy. The degree of privacy has a direct impact on a user's usage and trust. The

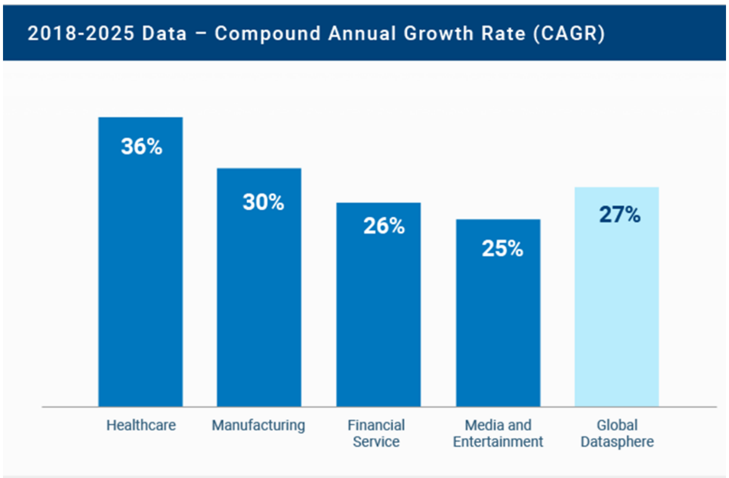

Figure 1.1: Source - Coughlin *et al* [1] Internal Medicine Journal article

application of the ”Hippocratic Databases (HDB’s)” concept can solve the challenges listed above, which are generally based on the Hippocratic Oath’s basic principles and can be applied to the databases to ensure data privacy and confidentiality.

Every hospital and clinic maintains its own medical records. Healthcare 5.0 enhanced performance, precision, and accessibility without being cumbersome. When it comes to safeguarding patients’ sensitive data, who has access to what information is crucial. The ten HBD principles and standards are then used to implement the HBD principles for healthcare systems and specific components. When considering the environment, the HBD method improves privacy and security. Query-Restriction and Data-Perturbation are the two most common privacy policies used in HBD during its processing. The application first sends a query to the database and then retrieves the response. The application then examines the resulting records and filters out any information that is banned. However, if no privacy methods are applied to the sensitive features of the data, various sensitive data can be disclosed. As a result, to address issues that develop as a result of query input, privacy preservation methods are sometimes used to improve privacy and security. In the earlier paper [2], we worked on improving the capabilities of privacy preservation methods. By combining these two policies of privacy, the tables that are released become more customizable, and sensitive data disclosure can be regulated.

The tables that are being shared are both safe and do not reveal any important information about the patients. The following step is to ensure that data transmission from one hospital to another is secure. There are several methods for ensuring secure data transmissions, including encrypting the data before sending it, or authorising the opposite party before transmitting the data only if the user is certified. The second method is to employ the most recent and widely used mechanism known as a smart contract. Smart contracts are self-contained, secure, dependable, efficient, and accurate. If, a smart contract is deployed before sending a patient's data to another hospital, it creates transparency and ensures that the other party cannot violate the conditions of the agreement. When employing a smart contract, the other party's verification and authorization process is crucial. Patients' trust in the data, as well as its integrity, must be assured. As a result, we employ smart contracts to transfer the gathered healthcare data, which strengthens security by only delivering the data to approved individuals.

Based on the foregoing discussion, we have identified four significant challenges. The first is to protect the healthcare database from linking and inference attacks (using multiple query sets). The second goal is to reduce data loss so that the user can get precise results. The third is that if someone impersonates a real user, the database views will be blocked as well. The fourth requirement is that authorization is obtained before data is transmitted to the other party. To overcome these challenges, we have introduced the HiPPRule by integrating two promising privacy control techniques (query-set-size restriction and KADP) with the generated rule set to achieve a sufficient privacy level and satisfactory data usefulness. We deployed a smart contract in HiPPRule to further authorize the user before delivering the released table to another party. HiPPRule filters healthcare data and manages how different people see it. Because healthcare data must be given publicly for research purposes, this technique was developed expressly for consumers. No other sensitive data is released for public use. When compared to other sensitive data, these forms of data leaks can have a more obstructive social impact (full identity theft) and can be utilized in a variety of ways. As a result, we've introduced the HiPPRule approach to keep healthcare data private.

1.0.1 Hippocratic Database

Databases should include accountability for privacy as a core component, where efficiency is no longer a top priority. Previously, healthcare relied heavily on traditional storage systems, with the quality of the data being the primary concern. Later, as the industrialization age began, the responsiveness of databases to end-to-end services became increasingly important. Various automated procedures were added in health 3.0, which improved database access control and responsiveness efficiency. The key focus areas for databases during the digitization age were their uniqueness, mass personalization, and proactive healthcare. This was the era when numerous EHR and EMR systems were introduced, each offering the highest level of database security possible. The primary focus of databases has shifted in the current internet era as people and users choose privacy and personalization over other benefits. The Hippocratic Databases are introduced here to assist users in obtaining what they require.

In the 5.0 scenario, the internet and all of its services enable the collection and storage of client information. The process can be completely automated and without the knowledge or approval of the data source (corporate users, students, patients, or normal web users). These facts address privacy and security concerns early in the process of analysing, designing, and implementing modern information systems. Privacy, security, and data access control were formerly reserved for ”big databases” and special-purpose systems. Those are the requirements and standards that every database system must meet.

- Privacy - Every individual has the right to decide when, how, and how much information is available for storage and communication between systems.

- Access control - a method with only two goals: to prevent resource misuse and to obtain complete facts about an event. Access control rights and operations defined in access control matrices are used to define functionality. In a nutshell, access control determines who gets access to what resources and how.

Hippocratic databases (HDBs) are a type of database that accepts responsibility for the data’s privacy and security while allowing approved access and dissemination. The following are the guidelines for developing hippocratic databases. These are largely based on the Privacy Act of 1974 in the United States and comparable legislation in other countries. Fair information practises are what they're called. They apply to any information about individuals that is collected:

1. Purpose Specification: The purpose for which the data is being gathered should be stated.
2. Consent: The data collection must have been approved by the donor of data.
3. Limited Collection: Only as much information as is required should be gathered.
4. Limited Use: Only the information collected should be used for the intended purpose.
5. Limited-Disclosure: Without the donor's permission, the information should not be shared with others.
6. Limited Retention: Information should only be kept for as long as it is needed.
7. Accuracy: The information kept on an individual should be accurate and current.
8. Safety: The data collection agency should ensure data security and prevent unwanted access.
9. Openness: The donor must be able to see and modify his information.
10. Compliance: Donors should be able to check whether their data is being kept private.

Solutions and current trends put the issue of privacy on the back burner and leave it to the company's security policy to address it. Examples of privacy violations demonstrate how this can be accomplished. To protect and maintain data privacy, technology should include access control and security procedures.

Privacy preservation Methods

Discovering safe ways to give the public access to a private dataset, like the medical dataset, is what privacy preservation entails. Privacy Preservation is vital when dealing with any variety of sensitive information that is obtained by the users. There are a variety of reasons why we need to protect and privatise data. In today's society, a variety of measures are employed to ensure that users' privacy is protected. Some of these strategies are listed below, which assist the users in determining what measures are to be taken if their privacy has been violated or how to improve the efficiency of their data privatisation.

There have been numerous privacy-preserving methods developed, but the majority of them rely on the anonymization of data. The following is a list of privacy-preserving strategies [1].

Table 1.1: Privacy Preservation Methods

Method Name	**Definition**	**Attack name**	**Drawback**
K-anonymity	Data modified before submitting for data analytics, preventing de-identification and resulting in K indistinguishable records	Homogeneity and Background knowledge attacks	Identity disclosure
L-diversity	Each equivalence class must have L well-represented values for the sensitive attribute (disease).	Skewness and similarity attacks	Implementation not possible when there is a variety of data
T-closeness	The distance between the sensitive attribute distributions in the equivalence class is less than a threshold.	Similarity and distribution-based attacks	Does not give a proper distribution of data every time.
Randomization	Adding noise to the data which is generally done by probability distribution	Random data injection	Large datasets is not possible because of time complexity and data utility

1. **K-anonymity** is a security paradigm that is typically used to protect data subjects in data sharing cases, and it guarantees that data is anonymized using k-anonymity. The ultimate goal of various security and privacy preservation mechanisms is anonymity for unlabeled data subjects. When completely trusted, the intention is to remain anonymous. If the information contained in the release cannot be distinguished from at least k-1 individuals whose information also appears in the release,

2. **L-diversity** is a security preservation technique in which homogeneity attacks are aimed at data similarity. It's absurd to think that L-diversity can be applied to any kind of dataset. To get around the limitations of k-anonymity, L-diversity was proposed. They have proposed a novel technique as an extension to k-anonymity that can guarantee information security even without knowing the adversary's experience with

avoiding property disclosure.

3. **T closeness**: a T-closeness strategy, which reduces the unprocessed of the deciphered content, is an advancement of the L-diverse. The degree of detail available to the spectator on explicit information is restricted, but the information is not limited to the general table containing the datasets. In this way, the semi-identifier parameter's relationship with the sensitive properties is weakened

4. **Randomization**: We suggested a randomised reaction model (k-mix), which introduces possible deniability using a combination of emissions attributed by the real data reconstruct method, rather than using normal activities (e.g., hypothesis, concealment, or added material clamor).

Some of the solutions described above are not practical to apply in the current scenario. As a result, when choosing a privacy preservation approach among the different methods stated above [2], we took into consideration its practicality and efficiency.

1.0.2 Block-chain Smart contract

Block-Chain Technology is a relatively new technology that has recently become a hot topic in the computer and network security area. Several studies are being conducted in this area to see if block-chain can aid in the privacy preservation of medical datasets. There are a variety of applications for block-chain technology, including privacy and security.

Basically, data sharing between parties necessitates the use of a trusted third party. As a result, it ensures each entity's security (confidentiality, integrity, and availability), privacy, and authentication. We employ the block-chain network or block-chain technology in the system for third-party assurance. While existing traditional sharing structures such as information bases and distributed storage (cloud) can provide an adequate ability to exchange test information in a suitable way, they cannot secure information integrity or licence innovation privileges of exploration outcomes. For example, COVID-19 has been spreading rapidly in recent days, with no vaccines available. At the time, each government was doing vaccine development. Data sharing across research departments, clinics, governments, patients, and hospitals is lacking.

As a result, we may create a block-chain network to aid in data sharing and communication among all entities. From the above discussion, we can deduce that authentication prior to data exchange can also be accomplished via block-chain and smart contracts. Smart contracts are essentially programmes that run when certain criteria are satisfied and are stored on a blockchain. Smart contracts' usage is to automate the execution of an agreement so that all parties can know the conclusion immediately without the need for middlemen or lost time.

Typically, a patient seeking medical help from another healthcare facility acquires all of his or her records from various institutions and makes them available to the new facility. This method of collecting and transmitting data may result in data loss or inconsistencies. The data in smart contracts is maintained on a blockchain, which is a distributed ledger.

Another healthcare organisation can access the information directly. Because each member of the chain has a complete copy of each individual's whole medical record, malicious assaults or data corruption on one system or location do not result in data loss, and data can be retrieved and restored from another block on the blockchain. Any changes to the records are also propagated throughout the network. As a result, smart contracts can better safeguard the integrity of patient data.

1.1 Motivation

Healthcare is a field that deals with a great deal of personal data. This sensitive information must be carefully stored, maintained, and retrieved. As we've seen, Hippocratic privacy preservation is critical for big data, especially in the healthcare industry [1]. Despite our knowledge of data protection, sensitive data is compromised when insufficient data preservation methods are followed. In this paper, we discuss how Hippocratic databases are used, as well as privacy protection mechanisms that can be applied to big data sets. We identify current weaknesses in data-sets and provide strategies to overcome privacy concerns.

1.2 Contribution

The following is the key contribution of our work:

1. A strategy based on query set size restrictions was proposed to protect sensitive

data from inference attacks.

2. Using KADP, this approach additionally protects the data from linking attacks.
3. A rule set for view control has been recommended to preserve the privacy of the authorised user's sensitive data if an impersonation attack is carried out.
4. This method also reduces processing time while minimising data loss.
5. When smart contracts are used for authentication, there is an increase in user trust.

1.3 Organization

The paper here-by follows the following schema. Section 2 contains the existing state-of-the-art approaches related to our research.Section 3 portrays the issues and challenges that exist in the present mechanism for the Healthcare 5.0 ecosystem. In Section 4, we have talked about why it is advantageous to use the proposed solution that has been modeled in Section 5. There is an in-depth working of the architectural model HiPPRule, that is presented in this paper. Finally, we have described the analysis delivered by the HiPPRule framework.

Chapter 2

Literature Survey

We present the existing state-of-the-art approaches in the Hippocratic approach for privacy-preserving healthcare ecosystems in this subsection. The existing techniques are listed in Table I. For example, Kundalwal *et al.* [3] offered an improvement in the preservation of cloud-based healthcare data. They developed a hybrid query set size restriction and k-anonymity technique that improved the privacy of healthcare data. Hartman *et al.* [4] introduced an ontology-based access control architecture that allowed web service users to access data at various levels. To guarantee that users do not exceed their power, they are assigned particular roles and goals. Bhatia *et al.* [5] presented a healthcare scenario in which they explained why Privacy Preserving Access Control (PPAC) should be used. They shared sensitive information in the realm of web services and introduced their unique framework for privacy-aware access in the domain of web services using PPAC, which was of great assistance. Wang *et al.* [6] presented PGuide, a privacy-preserving approach for clinical healthcare guiding and self-diagnosis and recommendation services with high risk prediction accuracy. The patient's sensitive attributes are preserved using a single-attribute encryption approach. Kundalwal *et al.* [7] suggest a hybrid technique based on query size restriction and inference control. The technique guarantees a k-anonymity model, which reduces inference and linkage attacks.

Similarly, Nortey *et al.* [8] used blockchain technology to ensure that the data they collected was kept private. They deployed the blockchain technology for data management as well as data distribution for EHR (Electronic Health Record) systems. Li *et al.* [9] suggested a network data set approach based on the Distributed Privacy Preservation technique. For the verification process, they integrated two techniques: smart contracts and Intel Software Guard Extensions (SGX). This was accomplished by looking at the user's properties and previous actions. With the support of the Blockchain system and user needs, Liu *et al.* [10] established a methodology and produced satisfactory results for the multimedia data collection. They analysed user needs and merged them with blockchain technology for authentication in their study. The authentication was performed on the multimedia data, resulting in a safer multimedia improvement. Li *et al.* [11] proposed FAPS, a strategy that ensures fairness in big-data exchange between buyers and sellers by eliminating third-party intermediaries. Smart contracts are presented as a way to ensure system justice and autonomy while also allowing friction-less transactions between cooperating entities. Some of the ideas listed above aren't feasible in the current situation. As a result, when picking between the several solutions outlined above, we weighed the Hippocratic privacy protection strategy's viability and efficiency.

Table 2.1: Comparative analysis of the state-of-the-art schemes

No	Years	Application	Dataset
Hartman *et al.* [4]	2016	Ontology based access control model → access data at different levels for web service users(WSU) + WSU may have different roles and purposes.	healthcare
Bhatia *et al.* [5]	2017	1. Privacy Preserving Access Control for sharing sensitive information in the arena of web services + reasons why privacy aware access control technologies are needed + comprehensive review of the existing work in this arena + novel framework for privacy aware access to web services	healthcare
Wang *et al.* [6]	2019	1. Privacy-Preserving Comparison Protocol (PPCP) in Patient Guide → to improve the accuracy of disease risk prediction 2. Single Attribute Encryption technique for privacy-preserving hospital recommendation service in Patient Guide → to choose from hospital list after self-diagnosis	healthcare
Nortey *et al.* [7]	2019	Use the blockchain technology for privacy preservation during the collection , management and distribution for EHR data	healthcare
Imtiaz *et al.* [8]	2020	Design and implement an end-to-end pipeline using DP and FL, use clustering to find similarities and increase the prediction accuracy	healthcare
Puri and Haritha [9]	2020	When stream data is collected, L-diversity occurs due to reputation Sol: HASH(L-diverse group + find similarity)' Result: reduce in data loss	healthcare
Li *et al.* [10]	2020	Distributed PP based on smart contracts + Intel Software Guard Extensions (SGX) → To verify by checking the user's properties and history behaviour.	network
Suneetha *et al.* [11]	2020	1. k-anonymization + L-diversity → to mask Personal Sensitive Information (PSI) 2. Apache Spark is used for faster and effective Big-Data process 3. shared data wont disclose original data by segregating Sensitive-Data and move it to HDFS	healthcare
Randa Aljably [12]	2021	Collect specific points from the user's behaviour patterns instead of the entire data stream and fed into Local Differential Privacy (LDP), after statistical data anonymization, reconstruct the original points using nonlinear techniques.	healthcare
Wu *et al.* [13]	2021	Collects SingleData[SD] (of all players → OtherData[OD]), check influence of OD on SD	game
Liu *et al.* [14]	2021	Block-Chain system + user needs → authenticated data by enhancing the safety of multimedia	multimedia
Irene *et al.* [15]	2021	1. fisher score, pearson correlation, information gain calculated(via. avg of it taken) 2. feature selection(eucledian distance) 3. clustered using(DAFCM) 4. classification done(entropy) 5. apply privacy preservation for better results than original	healthcare
Xu *et al.* [16]	2021	Review for federated learning technologies, particularly within the biomedical space.	healthcare
Kundalwal *et al.* [17]	2021	Hybrid technique (including 2 inference control techniques, query set size restriction and k-anonymity) to ensure individuals' privacy	healthcare
Li *et al.* [18]	2021	Use a Smart-Contract to exchange Data between Buyer and Seller w/o a 3rd party	Any generic Big-Data

Chapter 3

Identification of issues and challenges

People's use of mobile phones has expanded in recent years, and they now have a variety of applications to record their daily activities. They can use a variety of applications to keep track of their medical records. These apps are essentially EHRs (Electronic Health Records), which keep track of and save health-related information. They also send out reminders for prescriptions and regular examinations, as well as advice and information from doctors and nurses if they are consulted. As a result, keeping these medical records safe and confidential has become a major problem, because even a small breach in information might jeopardise a person's life.

Based on our survey of various journals and papers, we discovered the importance of preserving sensitive information provided by users. Users will be able to relax since their information will be protected, and they will be able to rely on them because their privacy will be protected. If they are unable to reach a neighbouring hospital, they can rely on the app, which may save more lives in a timely manner.

It's critical to recognise the problems that have arisen as a result of insufficient privacy protection. Here are some of the important topics we've discussed.

1. Users' personal information may be exposed.

2. During a data breach, a person with malicious intent can use the exposed data to

harm the patient.

3. Data can be lost, stolen, or tampered with, resulting in the patient not receiving timely and appropriate medication

When a person's health and life are taken into consideration, there are numerous options. As a result, sensitive data should be safeguarded and adequately protected from prying eyes.

As technology advances, so does the ability of those with nefarious intentions to mess with and harm innocent people. As technology evolves, the amount of data generated grows tremendously, as does the necessity for privacy. When people's hopes are placed in developers and scientists, there should be technology or methods in place to ensure that people's privacy is protected. Users can relax and feel better about themselves if their privacy is protected, which is excellent for their health.

Chapter 4

Proposed solutions and methodology used

4.1 Proposed Solution

In this section, we present the solution of the challenges mentioned above with system model and entities involved in the proposed scheme.

In our scheme, *HiPPRule*, which integrates based hippocratic databases (RBHD) and authentication based smart contract (ABSC) that allows dual benefits of rule control and privacy preservation. In the scheme, we consider N healthcare setups, denoted as $\{H_1, H_2, \ldots, H_n\}$. Any H_n is further categorized as $\{E_H, E_{PD}, E_{DR}\}$, where E_H means data available from hospitals, E_{PD} represents the public available healthcare datasets, and E_{DR} presents the datasets available from drug research labs. The collected data from $\{E_H, E_{PD}, E_{DR}\}$, collectively represented as D_H is prepossessed and cleaned. The modified data, represented as D_{HM} is shared between k healthcare users, represented as entities $E = \{E_p, E_d, E_a, E_n, E_ia\}$ respectively. E_p means patients, E_d represent doctors, E_a represents hospital admin, E_n denotes nursing staff, and E_ia denotes the insurance agents.

As data is shared among k entities in distributed manner, to preserve privacy, the scheme applies hippocratic databases (HDBs) to enforce query set restriction and data perturbation on D_{HM}. In the HBD engine, we apply q rule sets, $\{R_1, R_2, \ldots, R_q\}$ that forces the access constraints among k users through a many-to-many relationship. The domain for this rule set is R_H, which is the final set created after combining the multiple rule sets in the HBDs engine. Each entity consists of unique attributes which are then used in HBDs to secure data. The E_p entity consists of the following attributes $E_p = \{P_{id}, P_{floor}, P_{name}, P_{gender}, P_{age}, P_{address}, P_{Dname}, P_{disease}\}$. While the E_d, E_n and E_a consists the following attributes $E_d = \{D_{id}, D_{name}, D_{department}\}$, $E_n = \{N_{id}, N_{name}, N_{floor}\}$ and $E_a = \{A_{id}, A_{name}, A_{designation}, A_{rights}\}$ respectively. These rules set R_H are applied on these attributes to create a more secure database. Also KADP is applied on E_p so as to keep the records safe and viewable to only the necessary entities.

We get to the stage where we need to exchange the data around the various healthcare setups after safeguarding the data with rules and KADP. When sharing data among the multiple E_H, the particular hospital must be authenticated. For authorization and authentication of the healthcare provider, we employ a smart contract that validates according to a certain rule set. For the purpose of validation we employ f rule sets in the SC engine, $R_C = \{R_1, R_2, \dots, R_f\}$ to enforce authorization requirements among k users. While R_C is applied to some of the attributes of E_H such as $\{H_{code}, H_{name}\}$ which are checked with the attributes of A_R. A_R is the registration authority which already has the data of various E_H, which at the time of SCs execution checks whether the E_H is authenticate or not.

4.2 Methedology Used

In this research, we used three methodologies, the findings of one of which were combined with the results of the other to produce a higher efficiency than when they were used alone. This section provides a full discussion of how to use and benefit from these strategies.

4.2.1 Rule based Hippocratic Database

The following rule set has been proposed to control an authorised person's complete visibility of data to safeguard the data or table from impersonation attacks. The complete dataset will be visible if the user's input matches the saved values; otherwise, the data will be viewed in KADP format.

- $R_1: E.Type = \{reg\_E\} \bigwedge QR = \{Any\} \bigwedge Operation = \{R, W\} \bigwedge Resource = \{E_p\} \longrightarrow Permission = \{True\} \cup View.\mathrm{E}_p = \{\text{Complete}\}$

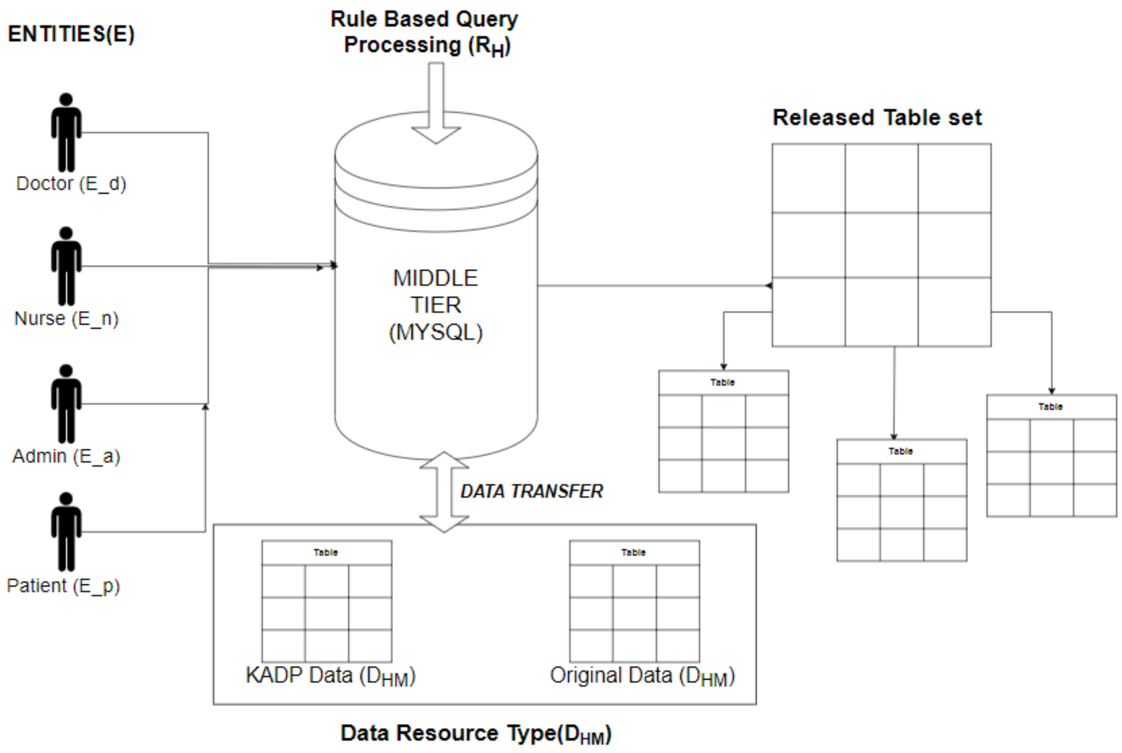

Figure 4.1: Rule Based Hippocratic Database

Rule Interpret : The registered entity of E of any type will be able to read or write the resource data E_p and they will be able to view the complete original data.

- R_2 : $E.Type = \{unreg\_E\} \bigwedge QR = \{Any\} \bigwedge Operation = \{R\} \bigwedge Resource = \{E_p.(P_{gender}, P_{floor}, P_{disease})\} \longrightarrow Permission = \{True\} \cup View.\mathrm{E}_p = \{\mathrm{KADP}\}$

Rule Interpret : The un-registered entity of E of any type will be able to read only the selected attributes $(P_{gender}, P_{floor}, P_{disease})$ from resource data E_p and they will be able to view only the KADP form of original data.

- R_3 : $E.Role = \{E_a\} \bigwedge QR = \{Any\} \bigwedge Operation = \{M\} \bigwedge Resource =\{E_p.(P_{gender}, P_{floor}, P_{disease})\} \longrightarrow Permission = \{True\} \cup View.\mathrm{E}_p = \{\mathrm{Complete}\}$

Rule Interpret : The E_a entity of E will be able to execute any query for maintaining the healthcare data from resource data E_p and they will be able to view the full form of original data.

- R_4 : $E.Type = \{unreg\_E\} \bigwedge Operation = \{W\} \longrightarrow Permission = \{False\}$

Rule Interpret : The un-registered entity of E of any type wants to execute any query in healthcare data they will not be allowed to execute it.

- R_5 : $E.Type = Any \bigwedge Operation = \{M\} \longrightarrow Permission = \{False\}$

Rule Interpret : The any entity of E of any type wants to modify healthcare data they will not be allowed to execute it.

Here, the above mentioned rules are the part of the set R_H which has been defined earlier. Thus, we can say that $R_H = \{R_1, R_2, R3, R4, R_5\}$ where f=5 are the rules that are set over the D_{HM} data that is being shared among k entities. In the next section we will in detail understand what is the KADP method that has been been mentioned earlier.

KADP Module

If one individual's information cannot be discriminated against by at least x other persons in the dataset, the data will have the k-anonymity property. We developed k-anonymity on the dataset to protect health-cloud databases against data linkage attacks. Here, some data will be encrypted and replaced using k-anonymity's generalisation and suppression methods, making the data non-identifiable.

1. **Suppression:** The "*" symbol can be used to replace some attribute values as well as some column values."Name" attribute to "*" can be used instead.
2. **Generalization:** In some cases, individual values can be substituted with broader categorical values. "age": "19" or "26" can be used represented as " $\leqq 40$"

Today, vast datasets are available, many of which include quasi-identifying information like P_disease, P_gender, and P_age, which, when combined, may identify over 86 percent of the US population. Thus, we may add noise to the dataset by using the Laplace and Gaussian methods of diffrenential privacy and make it practically difficult to identify a person. Differential privacy's claim is that it will be nearly impossible for anyone to extract private information about a person from a dataset.

A differentially algorithm takes a dataset as input and adds noise to the identifying data points. Statistical distributions such as Laplace and Gaussian approaches will be used to generate the noise at random. As a result, identifying information will be obscured by noise, ensuring the privacy of those whose identifying information is stored in the dataset. A graphical representation of the use of differential privacy may be seen here. Laplace and Gaussian methods are used in statistical distribution of differential privacy.

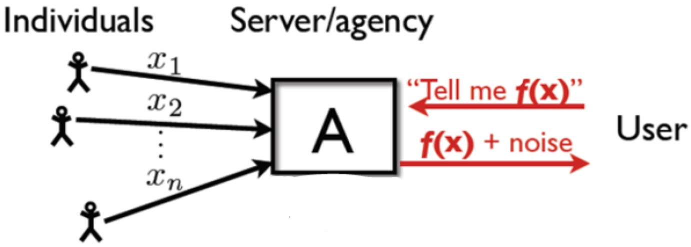

Figure 4.2: Working of Diffrential Privacy

When implementing and achieving the results in this work, we applied the Laplace theorem. As laplace allows us to employ the random factor, which is very beneficial in boosting the efficacy of privacy protection. When k-anonimity and differential privacy are combined, we get better results than when they are used separately. These findings will be presented in the next sections of this paper.

4.2.2 Authorization Based on Smart contract

In this situation, we chose to deliver the D_HM data via a smart contract because it contains sensitive information about the users. We must first authenticate the other entity before delivering the data to the other entities of the E_H collection; this is where SC comes into play. To begin, the E_H entities must register with the A_R, the registration authority, which houses all hospital data as well as other attributes with the exception of the D_HM data. The A_R demands attribute such as $\{AR_{Hid}, AR_{Hcode}, AR_{Hname}, AR_{Hspeciality}, P_{Haddress}, AR_{HcontactNo}\}$ from the registering hospital during the registration process. This information is gathered by the A_R in smart contract for the purpose of authenticating and authorising the E_H while transacting the smart contract. Entity E_H also has attributes which will be compared and mapped to some of the A_R attributes which will be the deciding attributes in this entire smart contract. The attributes of E_H are $\{H_{code}, H_{name}\}$, which will be checked with the A_R sets attributes to know whether the hospital is authenticate or not.

Smart contracts have the unique feature of being executed as soon as the requirements are met. There is no third-party interception while the execution process is in progress, giving users peace of mind. Here when the smart contracts conditions are meet, the execution process begins. There are two mapping conditions that are being executed in this smart contract which is used for authorisation purposes. The conditions of mapping are as follows: $M_1 : E_{Hid} \rightarrow U_{id}$ and $M_2 : A_{Rhid} \rightarrow U_{id}$. The mapping shown above depicts a situation where the user id is mapped to the hospital entities id and also to the registration authorities hospital id. This is the main condition that has to be full-filed during the authentication process of the hospital.

While executing the smart contract for authenticating the E_H set, we compare its attribute to the A_R entities. If the values while comparing them are the same then the authenticating procedure has been done and the D_HM data can be transferred to the entity that has been authenticated. The comparison takes place between the A_R attributes $\{AR_{Hcode}, AR_{Hname}\}$ and E_H attributes $\{H_{code}, H_{name}\}$. When $\{H_{code} == AR_{Hcode}\}$ and $\{H_{name} == AR_{Hname}\}$, then it is said that the E_H is authentic and the transfer of sensitive data i.e. D_{HM} can take place. Once the authentication process is over, the E_H and A_R data transactions are maintained as transactional ledgers in IPFS, and meta-information is chronologically recorded in the blockchain. This transaction information is maintained in a consortium blockchain, and the available usage and regulations are reflected on all authorised nodes in the chain. This maintains process transparency and reduces the risk of cooperation among malicious bidder nodes.

Chapter 5

Implementation

5.1 Architecture

In this section, we present the suggested reference architecture's layered approach, which handles the issue of privacy preservation methods in 5.0 healthcare ecosystem. The specifics are shown in Figure . The following are the details of a three-layered design that we consider.

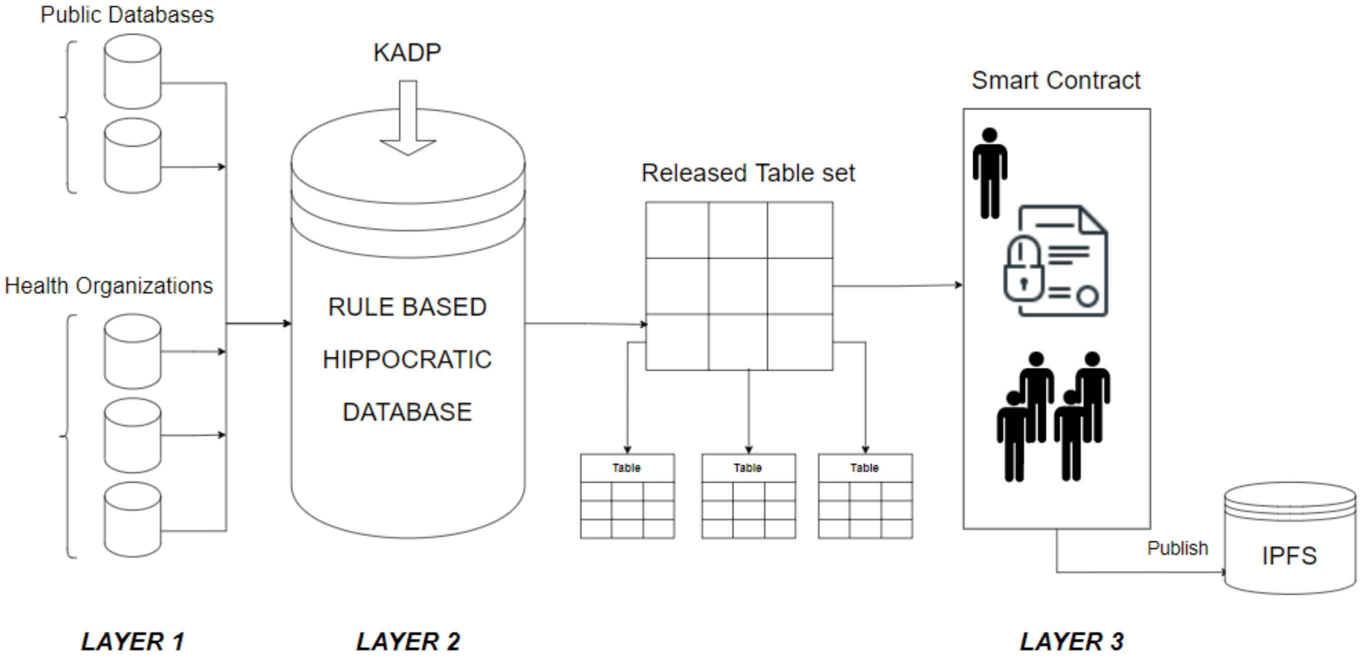

Figure 5.1: Layered Architecture Deployment

Layer 1: Organizational Layer

At *Layer 1*, we assume the D_{HM} and E details are present, which are a cluster of the modified data and the set of entities who have the access to D_{HM} data respectively. The D_{HM} data is the modified version of D_H data after it is cleaned and pre-processed. This layer serves as a storage house where all the data is stored and organised so that it is easily and efficiently available to the later layers.

Layer 2: Rule Based Hippocratic Database layer

At *Layer 2*, the pre-processed data is then given as input and once the rules of this layer are applied, the result is protected released tables that are ready for transmission. With the rules R_H which have been introduced and enforced this layer gets more secured while the query processing, which helps to maintain the privacy of the patients. The privacy of patients is being maintained from E entities with the help of KADP module that has been introduced. This module makes it so that when it is incorporated with the R_H set the E_p records are safeguarded and privatised. The D_HM which is the set of released tables are then sent to the next layer as an intput.

Layer 3: Contract Layer

At *Layer 3*, To break the shackles imposed by a centralised environment, the E_p requires a mechanism that can automate the process of making informed judgments. We use smart contacts for this. Smart contracts are self-executing programmes that do not require the intervention of a third party (such as humans). In the proposed model, smart-contracts ensure the storage of authorised E_H and A_R data published on IPFS. IPFS access is controlled by identity authorization and the IPFS key.

5.2 Dataset Description and Results

The original dataset D_{HM} which is a set of data that has been collected over various healthcare scenarios is a collection of big data. The E_H data that we have shown results from consists of bias and unbiased data forms. The bias data has a total of ten thousand rows and seven columns. Country, condition or disease, age, gender, name, patient ID, and date of birth are the column names. Where as the unbiased data-set gathered has 4 different entities which are E_d, E_n, E_a, E_p which further has their own attributes. The E_p consists of 8 attributes which are P_{id}, P_{floor}, P_{name}, P_{gender},P_{age}, $P_{address}$, P_{Dname}, $P_{disease}$. There are a total of 1100 rows in the E_p entity. This collection contains information about 15 different areas of Ahmedabad city. The age factor is having the maximum variation which is why it is identified as an attribute to privatize the most. The other entites of the E dataset are used for the R_H rule set, for checking the various data and also for querying purpose. Here we have shown results of two queries on which the R_H rule set was applied, along with the KADP form of the E_p dataset.

Query 1:

EXISTS{ (SELECT D_{id} FROM Doctors WHERE $P_{disease} = D_{speciality}$ U_{id}=$Doctors.(D_{id}))$};

Explanation: by the word "EXIST" we emphasize that is the following condition of query is not fulfilled, then the query will not show any results. Here firstly the D_{id} is matched with the U_{id}, which is the current users id. If both the values are same it will check the condition of $P_{disease}$ to the $D_{speciality}$, if and only if these condition match do we show the data. Now to know what type of data will be shown D_{id} plays an important role. If the condition is matched with U_{id} then it shows that the doctor which is the current user is registered. Thus the result shown will be Complete data, which is shown in following table.

Table 5.1: Query Result Rule 1

Pid	Pname	Pgender	Page
P0072	SHIROMANI JAIN	Female	25
P0076	SOHAM DAVE	Male	23
P0092	JASHRATH BHAI	Male	36
P0098	DIPAK BHAI	Male	28
P0119	VIJAY BHAI	Male	22
P0124	SEEMA	Female	45
...	...	...	...
P0751	MONIK BHAI	Male	25
P0833	NANDINI BEN	Female	45
P0846	SEEMA	Female	45
P0847	BHAVYA	Male	16
P0854	VISHAL BHAI	Male	50
P0857	PRIYA	Female	25

Query 2:

EXISTS{ SELECT N_{id} FROM Nurses WHERE $P_{floor} = N_{floor}$ U_{id}=$Nurses.(N_{id}))$};

Explanation: Here firstly the N_{id} is matched with the U_{id}, which is the current users id. Here the match has not been made which suggest us that the user that tried to enter is not a registered user. Thus the result shown will KADP data, which is shown in following table. The next condition to check is whether P_{floor} is equal to N_{floor}, if and only if this condition matches the data will be shown in KADP form, otherwise the user will not be allowed to view any data.

Table 5.2: Query Result Rule 3

Pid	Pgender	Pdisease	Pfloor
P0033	*	****AL	3
P0045	*	****AL	3
P0059	*	****AL	3
P0060	*	****AL	3
P0065	*	****AL	3
P0066	*	****AL	3
...	...	...	...
P1080	*	****AL	3
P1084	*	****O	3
P1088	*	****AL	3
P1091	*	****O	3
P1093	*	****AL	3

Table 5.3: Result of KADP

Pid	Paddress	Pdisease	Page	Pgender	Pname	PDname	Pfloor
P0001	******pur	***N	26.91888	*	*	HIRAL BEN	2
P0002	******pur	***N	57.4659	*	*	HIRAL BEN	2
P0003	******pur	***N	32.42079	*	*	SUNIL DESAI	2
P0004	******pur	***N	39.24621	*	*	SUNIL DESAI	2
P0005	******pur	***N	57.41649	*	*	HIRAL BEN	2
...	...	...	...	...	...	...	...
P1095	***a	**N	69.81247	*	*	FORAM BEN	4
P1096	******ev	****EN	52.69321	*	*	DHARMESH BHAI	5
P1097	******dia	******R.	31.04915	*	*	HIMANSHU BHAI	5
P1098	******pur	******R.	48.12593	*	*	HIMANSHU BHAI	5
P1099	******ar	****Y	34.92575	*	*	HIMANSHU SHAH	5

KADP: The original data set is subsequently converted to an anonymised version using k-anonymity, for which we deployed algorithm-1. Because people's sensitive information can be easily recognised if a hostile person knows their country and age, we utilise the Laplace theorm as shown in algorithm-2. Due to the laplace theorm of differential privacy, statistical content such as age will have erroneous values, making it more difficult for a hostile individual to identify the patient. The outcomes obtained after combining these two tactics are shown in the KADP table.

5.3 Flowchart

Here the workflow of layer 2 and layer 3 has been proposed, which explains to us how those layers work. As we can see firstly we have to open the web portal, than login to the portal with the identities provided in option and then according to the identity the data will be retrieved.

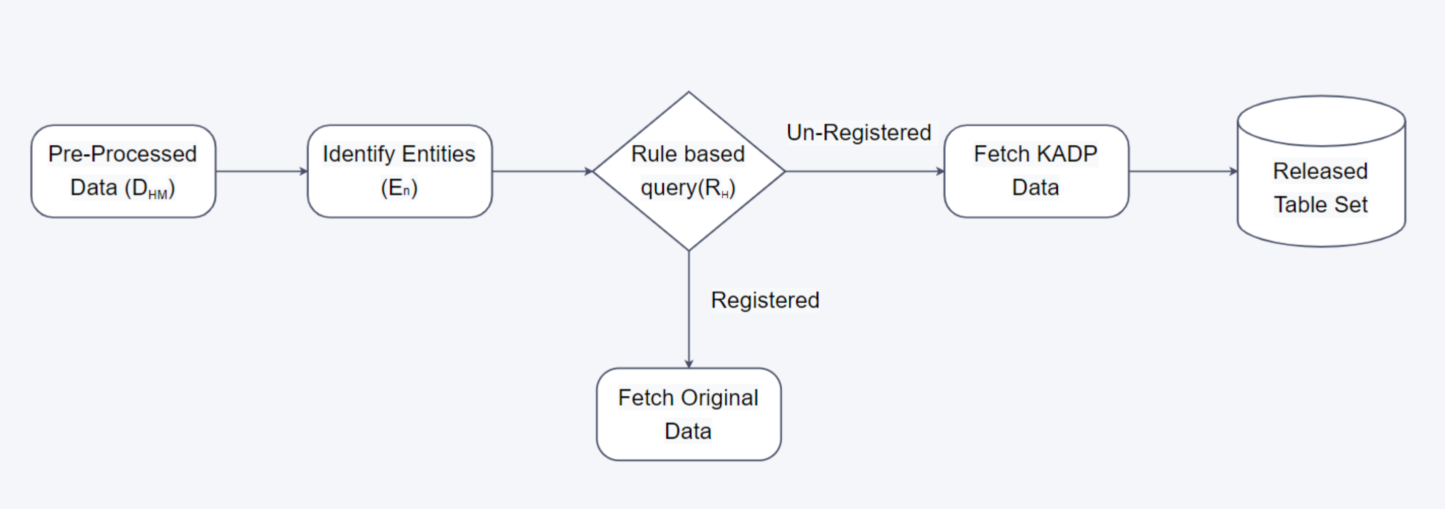

Figure 5.2: Flowchart of RBHD

Layer2 and Layer3: After applying the rules of this layer2 to the pre-processed data, the result is secured released tables that are ready for transmission. The rule most vital point is the condition check of registered and un-registered user. If the user is not register that the data shown is the KADP data while registered user can have the full view of the data. During releasing the tables we use smart contacts to free the users from the constraints of centralised systems. Smart contracts are self-executing programmes that do not require third-party interaction (such as humans). Smart-contracts ensure the storage of authorised E_H only. This authorisation is checked by the Authorization registration party after satisfying the conditions provided by the smart contract.

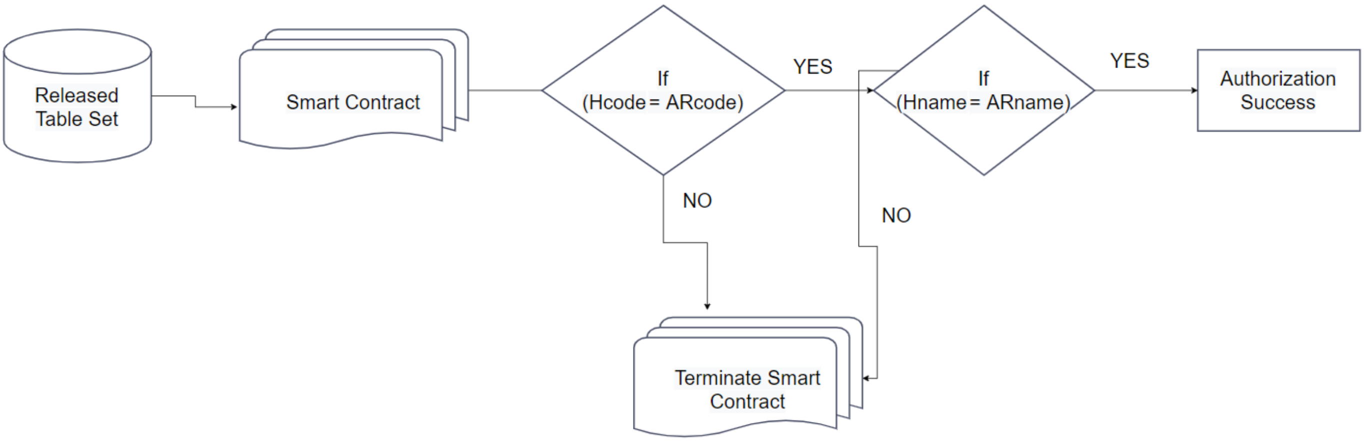

Figure 5.3: Flowchart of ABSC

5.4 Algorithms

Here we have provided with the algorithm that is being used for obtaining the desired results.

Algorithm 1 The k-anonymize algorithm

```
procedure ANONYMIZE($Ds$, $Cs$)
    $AnDs \leftarrow Ds.copy()$
    repeat
        for $C \leftarrow Cs$ do
            $CL \leftarrow C['L']$
            if $C['type'] ==' suppressed'$ then
                for $x \leftarrow AnDs[CL]$ do
                    $x \leftarrow *$
                    $AnDs[columnLabel] \leftarrow x$
                end for
            end if
            if $C['type'] ==' semi-suppressed'$ then
                $AnDs[CL] \leftarrow AnDs[CL].astype(str)$
                for $x \leftarrow AnDs[CL]$ do
                    $x \leftarrow *(0.Y\text{OfTotalLen})$
                    $AnDs[CL] \leftarrow x$
                end for
            end if
            if $C['type'] ==' generalized'$ then
                for $i \leftarrow range(len(AnDs[CL]))$ do
                    $AnDs[CL] \leftarrow AnDs[CL].astype(str)$
                    $x = int(float(AnDs[CL][i]))$
                    if $x <= a$ then
                        $AnDs[CL][i] \leftarrow " < a"$
                    end if
                    if $x > a\& \ x <= b$ then
                        $AnDs[CL][i] \leftarrow "a - b"$
                    end if
                    if $x > b\& \ x <= max$ then
                        $AnDs[CL][i] \leftarrow " > b"$
                    end if
                end for
            end if
        end for
    until $\neg AnDs$
end procedure
=0
```

Algorithm 2 The Differential Privatization(Laplace) algorithm

```
procedure DP($Ds$, $Cs$)
    $sensitivity \leftarrow a$
    $epsilon \leftarrow b$
    Use Laplace Truncated and Place Required Values.
    $LpDs \leftarrow Ds.copy()$
    for $x \leftarrow LpDs[CL]$ do
        $x \leftarrow randomise[CL]$
        $LpDs[CL] \leftarrow x$
    end for
end procedure=0
```

Algorithm 3 Authorization In Smart contract algorithm

```
procedure SMART-CONTRACT($H_C$, $H_N$, $RA_C$, $RA_N$, $SC$)
    if $SC \leftarrow TRUE$ then
        if $H_C == RA_C$ then
            if $H_N == RA_N$ then
                $Show \leftarrow success$
            end if
        end if
    end if
end procedure=0
```

Chapter 6

Performance evaluations

According to the algorithms and rules the D_{HM} and E_p were experimented on and there were some satisfactory results that were obtained. After the adaption of HiPPRule the results that were obtained are compared to the previous results and some analysis are provided based on them. During the analysis we found that the disease data has been distributed in a downward curve graph with GENERAL disease having the highest number of records while GBC disease having the lowest amount of entries.

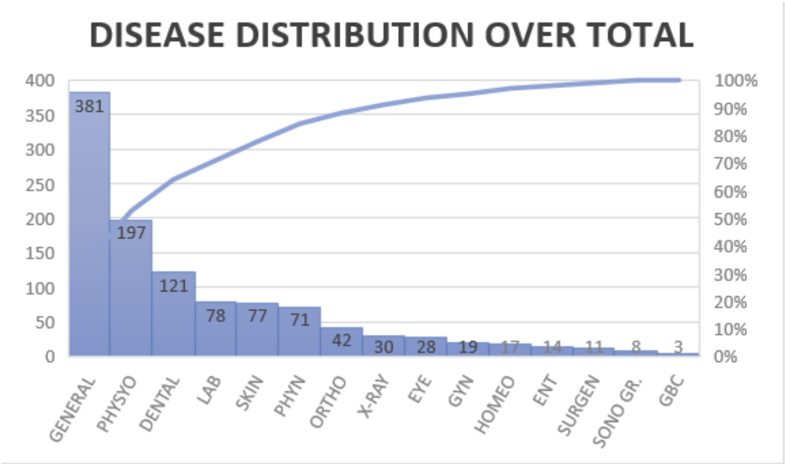

Figure 6.1: Analysis of E_p dataset

Here we have identified certain scenarios which are based on the query implementation that has been shown before. There are basically 2 main scenarios that have been implemented and whose comparison in an evaluation form has been shown here. The scenarios are as follow:

Scenario 1: When the Doctor type user is unregistered and the disease type is searched, we obtain the P_{id}, and P_{floor} as it is, while the other attributes such as $P_{address}$, P_{gender}, P_{name} and P_{age} will be anonymised. By knowing some background knowledge regarding the patient such as P_{age} the search of the user with malicious intention gets narrowed down. Thus, we adapt KADP methodology along with the defined rules so as the information of P_{age} is hidden away by adding noise to that entity.

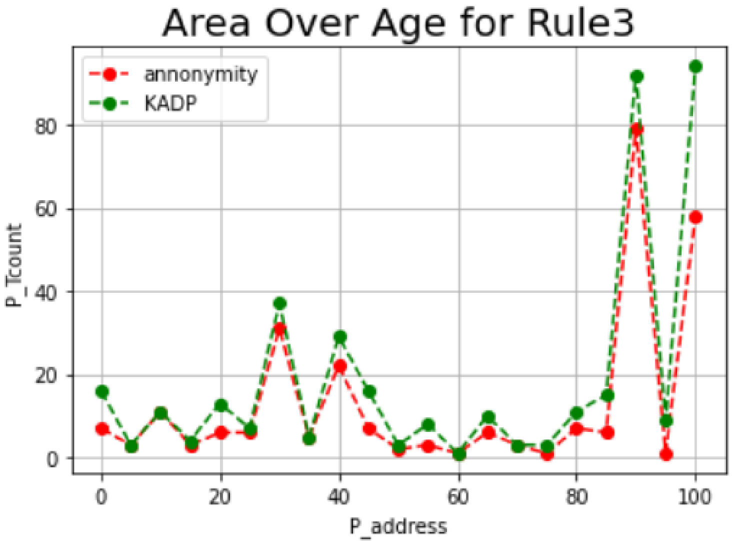

Figure 6.2: Result of Scenario 1

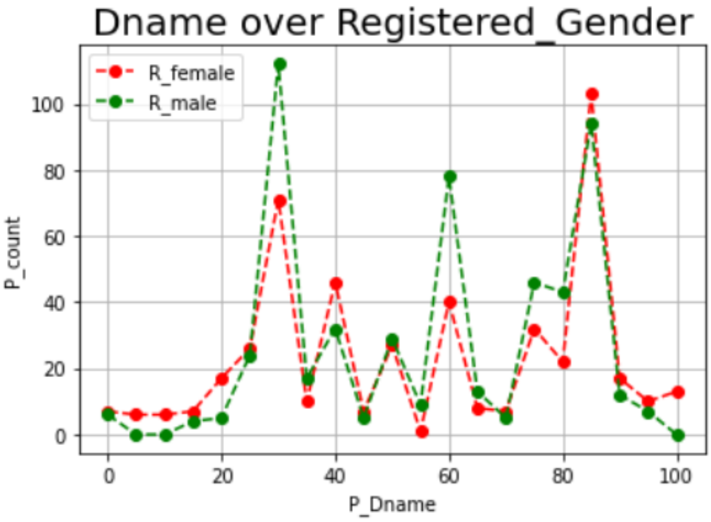

Figure 6.3: Result of Scenario 2

Scenario 2: When the nurse is unregistered they are only able to see the anonymised data of the $P_{disease}$ and P_{gender}, while they are able to see the P_{id} and P_{floor}. So here when the query is inputed for the unreg user or reg user it checks the P_{floor} entered along with the P_{Dname} selected and shows the result based on them. For example: if the P_{floor} = {any} and P_{Dname} = {any} the results shown to both will be the same, but one is in KADP format while the other is in Complete format respectively. Here we have plotted a comparison graph between the registered users gender count to the registered doctor users.

The results and comparison charts show that combining the rule based hippocratic database to KADP method resulted in a privacy preservation gain of over 46 percent then the original model where only hippocratic data along with anonymity was applied.

Chapter 7

Summary and Conclusions

7.1 Conclusion

Our goal in this paper is to improve the security and privacy of healthcare data that is vulnerable to attacks like the similarity and homogeneity attack. We have presented the HiPPRule, which achieves the following three goals easily and efficiently. *Goal 1* to increase the potentiality of privacy preservation method and reducing the attacks probability has been obtained by the differential privacy method, *Goal 2* achieving HDBs to ensure privacy even when the resources are shared is obtained with the help of Rule based Hippocratic method, *Goal 3* to authenticate the E_H users with the help of smart contract.

Future work we plan to expand our experimental work and explore more of smart contract modules such as transmitting the E_p data over to the authenticated E_H entities. This will create a more secure and ease free environment for the E_p on which they can place their trust on

Bibliography

[1] S. Coughlin, D. Roberts, K. O'Neill, and P. Brooks, "Looking to tomorrow's healthcare today: a participatory health perspective," *Internal medicine journal*, vol. 48, pp. 92–96, 01 2018.

[2] M. Patel, V. Prasad, P. Bhattacharya, M. Bhavsar, and M. Zuhair, "Privacy preservation for big data healthcare management," 05 2022.

[3] M. Kundalwal, K. Chatterjee, and A. Singh, "An improved privacy preservation technique in health-cloud," *ICT Express*, vol. 5, 10 2018.

[4] S. Hartmann, H. Ma, and P. Vechsamutvaree, *Providing Ontology-Based Privacy-Aware Data Access Through Web Services and Service Composition*, vol. 10130, pp. 109–131. 12 2016.

[5] G. Wang, R. Lu, C. Huang, and Y. L. Guan, "An efficient and privacy-preserving preclinical guide scheme for mobile ehealthcare," *J. Inf. Secur. Appl.*, vol. 46, pp. 271–280, 2019.

[6] R. Nortey, Y. Li, P. Ricardo, and M. Adjeisah, "Privacy module for distributed electronic health records(ehrs) using the blockchain," pp. 369–374, 03 2019.

[7] R. Bhatia and M. Gujral, *Privacy Aware Access Control: A Literature Survey and Novel Framework*, pp. 2028–2043. 01 2018.

[8] S. Imtiaz, S.-F. Horchidan, Z. Abbas, M. Arsalan, H. Chaudhry, and V. Vlassov, "Privacy preserving time-series forecasting of user health data streams," pp. 3428–3437, 12 2020.

[9] G. Puri, "A novel method for privacy preservation of health data stream," *International Journal of Advanced Trends in Computer Science and Engineering*, vol. 9, pp. 4959–4963, 08 2020.

[10] J. Li, J. Cheng, N. Xiong, L. Zhan, and Y. Zhang, "A distributed privacy preservation approach for big data in public health emergencies using smart contract and sgx," *Computers, Materials Continua*, vol. 65, pp. 723–741, 01 2020.

[11] V. Suneetha, S. Suresh, and V. Jhananie, "A novel framework using apache spark for privacy preservation of healthcare big data," pp. 743–749, 03 2020.

[12] R. Aljably, *Privacy Preserving Data Sharing in Online Social Networks*, pp. 142–152. 06 2021.

[13] D. Wu, X. Wu, J. Gao, G. Ji, T. Wu, X. Zhang, and W. Dou, *A Survey of Game Theoretical Privacy Preservation for Data Sharing and Publishing*, pp. 205–216. 10 2020.

[14] J. Liu, K. Fan, H. Li, and Y. Yang, "A blockchain-based privacy preservation scheme in multimedia network," *Multimedia Tools and Applications*, vol. 80, pp. 1–15, 08 2021.

[15] D. Irene, S. Vijayan, D. Kavitha, R. Shankar, and J. Justin, "An intellectual methodology for secure health record mining and risk forecasting using clustering and graph-based classification," *Journal of Circuits, Systems and Computers*, vol. 30, p. 2150135, 11 2020.

[16] J. Xu and F. Wang, "Federated learning for healthcare informatics," *CoRR*, vol. abs/1911.06270, 2019.

[17] M. Kundalwal, K. Chatterjee, and A. Singh, "An improved privacy preservation technique in health-cloud," *ICT Express*, vol. 5, 10 2018.

[18] T. Li, W. Ren, Y. Xiang, X. Zheng, T. Zhu, K.-K. R. Choo, and G. Srivastava, "Faps: A fair, autonomous and privacy-preserving scheme for big data exchange based on oblivious transfer, ether cheque and smart contracts," *Information Sciences*, vol. 544, pp. 469–484, 01 2021.

Major project_18_05_2022

ORIGINALITY REPORT

8%	2%	8%	%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	Mayank Kumar Kundalwal, Kakali Chatterjee, Ashish Singh. "An improved privacy preservation technique in health-cloud", ICT Express, 2018 Publication	2%
2	Jasmin Azemović. "Privacy aware eLearning environments based on hippocratic database principles", Proceedings of the Fifth Balkan Conference in Informatics on - BCI '12, 2012 Publication	1%
3	Pronaya Bhattacharya, Farnazbanu Patel, Vishaka Ralegankar, Bhaumik Thakkar, Sudeep Tanwar, Mohammad Abouhawwash. "Chapter 30 Trusted 6G-Envisioned Dynamic Spectrum Allocation: A Reference Model, Layered Architecture, and Use-Case", Springer Science and Business Media LLC, 2022 Publication	1%
4	www.researchgate.net Internet Source	<1%