International Journal of Current Engineering and Technology
E-ISSN 2277 – 4106, P-ISSN 2347 – 5161
Available at http://inpressco.com/category/ijcet

Research Article

Handling of Personal Health Record Access Control Mechanism through Blockchain and AI

Kajal Umesh Kamthe Dr.Gitanjali Shinde

Computer Engineering S.K.N. College of Engineering, Pune, India

Received 10 Nov 2020, Accepted 10 Dec 2020, Available online 01 Feb 2021, **Special Issue-8 (Feb 2021)**

Abstract

Health is one of the key components of a fulfilling life. But certain diseases can cause an individual a significant amount of discomfort that can only be alleviated by proper diagnosis and medication by a doctor. In most developing nations, when a patient visits the doctor diagnoses the symptoms and provides medication if the symptoms fall under a particular ailment. Sometimes the symptoms are broad and a conclusive diagnosis cannot be reached, such a scenario the doctor opts for a trial and error method to weed out the actual ailment. This is a highly painful inconvenience for the patient. In most developed countries, there is a system to record and store Personal Health Records of the patients. These PHRs can be utilized in such cases where a conclusive diagnosis cannot be reached. Hence, when such a scenario is experienced by the doctor, he/she will consult the previous PHRs for similar cases. There are also independent Data Vendors that aggregate medical data from different medical institutes and hospitals. But there is a lack of trust between the entities that hamper the data sharing paradigm. Therefore, this paper outlines an effective Access Control mechanism which utilizes the blockchain platform to secure the data and alleviate the trust issues. The methodology also implements Linear Regression along with Hidden Markov Model and Fuzzy classification to enable an effective, secure and reliable Access control Mechanism on a distributed system for data sharing.

Keywords: *Blockchain, Data Vending, Natural Language Processing, Hidden Markov Model, Linear Regression.*

Introduction

Data is one of the most essential requirements for achieving various different approaches such as Medical procedures, artificial intelligence etc. The collection of large amounts of data for such applications is essential for the normal working of these applications. The data for such applications are generally aggregated through various different sources and collected together by data aggregators. These entities are responsible for providing the various different approaches that require the data with the right amount of data at the right time as requested. These data vendors provide adequate data at regular intervals which keeps various applications satiated. This is the same process that is followed by major hospitals and medical institutions outside India. In India, when a patient with a particular disease approaches the doctor or the hospital, his/her symptoms are analyzed and then compared to the different diseases and their symptoms. Once the disease is identified the doctor then performs the treatment accordingly. But in a scenario where the symptoms do not match any other disease or multiple diseases, it becomes really difficult to treat the patient and the doctors then employ a trial and error technique to eliminate several diseases and extract the actual ailment of the patient. This type of procedure is a highly dangerous one which can be quite painful for the patient. The trial and error method is inhumane as it puts the patient under undue stress as the patient is in pain until the correct disease is identified and the treatment for it is provided. The whole procedure of trial and error must be performed as all the diseases cannot be eliminated without proper proof. This is what happens every time someone goes to the doctor with symptoms that have not been encountered by the doctor before in India. This is the normal procedure that is being followed everywhere in this country and this needs to change. Outside India, all the different hospitals and other medical institutions maintain an Electronic Health Record or EHR of every patient that visits their facilities and the various symptoms along with the treatments offered to the patient. These records are kept as a way of documenting the various treatments and other important procedures performed on the patient. In a scenario where a patient arrives with an ailment and a set of symptoms, the doctor analyzes the patient and if the symptoms match a disease then the doctors prescribe some medicines and treat it accordingly.

If the symptoms have not been encountered before, the doctor checks if there has been a patient with such symptoms before in the vast library of Electronic Health Records. If a similar patient with similar symptoms is identified the doctor can study the previous patient to get an insight into the patient's ailment and can hence provide efficient treatment based on the past data. This act of storing the medical data for future purposes benefits the doctors as well as the patients. This eliminates the stress on the patient as well as reduces the suffering of the patient significantly.

In a scenario where there isn't any past record of such symptoms and ailment, and the doctors cannot readily resort to the trial and error technique. Therefore, the doctors then utilize the Data Vendors or Data Aggregators by sending them a request for the data on a particular ailment. The Data Vendors are in contact with the different hospitals and medical institutions and sends this particular request to all of them requesting data if there is any regarding the patient's ailment. The hospitals check their database of Electronic Health Records for the occurrence of such symptoms. If any of the records are correlated, the hospitals send that particular data to the data vendor.

Once the Data is received by the Data Vendor which then packages it and sends it to the requestor and charges a fee for its services. This allows the doctor to analyze and study other patients records that are similar to its patient and its symptoms. This reduces the chances of the patient going through the trial and error method which reduces the pain and the suffering of the patient and promotes swift recovery. This structure is applied in the majority of developed countries which increases the convenience of the doctor as well as the patient.

Most of the times, the patients are concerned about the privacy of their data and how it is being utilized. This is due to the fact that most of the Electronic Health Records contain personal information that is highly sensitive and cannot be shared with anyone. The medical organizations are also usually sceptical about the Data Vendors and there is a loss of trust between these two entities that lead to reduced instances where the data is being shared to the Data Aggregators. This is a problematic occurrence as this system of Electronic Health Record sharing is reliant on the open sharing of data that enables such a great amount of convenience amongst the medical organization and their patients.

Therefore, there is a need for the development of an effective Access control Mechanism that increases the security of the whole system and restores the trust between the organizations and the Data Vendors. The Access Control mechanism does not allow an unauthorized person to gain access to the sensitive information present in the EHR. This allows for a much more transparent exchange of information, here the EHR/PHR are depersonalized to remove the sensitive information pertaining to the patient. The Depersonalization encourages the patients to share their information without worry as their EHR after depersonalization cannot be traced back, which eliminates any trust issues with the Data Vendor completely.

The Hidden Markov Model is an innovative technique that is based on the concepts of Markov models. The Markov Models are models that are based on the mathematical branch of statistics. Markov models are greatly used in biological models that have been utilized for computation. The Markov models have been named after a Russian mathematician that had a great influence on the statistics. They are widely used in speech recognition and for the computation of biological sequences. The Hidden Markov Model has hidden parameters that cannot be observed. The main assumption for the application of this model is that the process in question is a Markov process. The Hidden Markov Model is tasked with the modelling of the stochastic process. The Hidden Markov Model is considered a part of the Bayesian Network that utilizes inference algorithms to achieve probabilistic modelling of the hidden states.

Fuzzy Classification is a novel application of the Fuzzy logic for achieving the goal of classification. Classification is defined as a technique that is tasked with the assignment of various different labels to objects. The fuzzy classification utilizes the fuzzy logic for the classification. This is through the use of degrees of the relationship of the particular object to a particular label. As most classification technique works on the hard labelling based on the fact that the label classes are mutually exclusive. This assumption is discarded in Fuzzy classification which employs soft labelling. The Fuzzy classifiers are also highly transparent allowing their application in sensitive environments such as medical institutions without any problems as they are comprehensible and traceable. The fuzzy classification employs fuzzy rules which result in a strong classification which achieves maximum efficiency.

In this paper, section 2 is dedicated for literature review of past work and Finally Section 3 concludes this paper.

Literature Review

This section of the literature survey eventually reveals some facts based on thoughtful analysis of many authors work as follows.

M. Khan states that there has been a significant increase in the number of data breaches and attacks that are orchestrated to steal data by individuals with malicious intent. The authors have stated that Electronic Health Records are highly private and cannot be subject to unauthorized access unless it is by the medical professional [1]. The authors have implemented a system that utilizes the RBAC model that is used to provide flexible access control to electronic health records to balance the security as well as help the medical community and other data seekers at the same time. The experimental results indicate that the proposed methodology provides superior access control for the EHR. The major limitation of the proposed methodology is that the authors have not implemented a post-fact verification of the emergency access control mechanism.

N. Lu explains that there is a widespread use of the Big Data paradigm in the medical industry due to a large amount of data generated by large hospitals and other corporations. Due to a large amount of data, most of which are personal health records of the patient, need to be safeguarded for data leakage [2]. Therefore, the authors have implemented a system for providing an access control mechanism for accessing the medical data, through the use of Information Entropy to limit the access of the user to the search field specified. This leads to efficient and secure access to sensitive personal health record data. The major limitation of this paper is that the proposed technique increases the computational complexity in comparison to conventional techniques.

Y. Yang elaborates on the large-scale development and release of various low powered IoT devices for the purpose of monitoring a patient's vital stats and collect the data for use by the doctor or to indicate an emergency situation. Most of these devices do not have the computing power to safeguard the data that is being generated which puts the extremely sensitive data at risk of a data leak [3]. Therefore, the authors have proposed a technique called LiBAC or Lightweight Break Glass Access Control system that provides encryption of the medical files and emergency access to the data along with attribute-based access. Extensive experimentations have revealed that the technique is highly efficient. The major drawback of this methodology is that due to the lightweight nature it has a low level of encryption offered for the data.

F. Ullah introduces WBAN or Wireless Body Area Network, which is a wireless network designed for the purpose of supervising the condition and the vital signs of a patient. Due to the critical nature of the network, there should be zero packet loss and delay along with a diverse Quality of Service to the patients [4]. To achieve this the authors have proposed a system that utilizes the MAC Superframe that switches between various channels depending on the severity of the patient's condition and if it is severe, the transmission is made immediately without any transmission loss or delay. The major limitation of this project is that the authors have not implemented in this application in a real-world scenario.

S. Belguith states that there is a very strong need for a system that provides an emergency access feature to be added to the various different applications without relying on a server authentication as during a disaster or a calamity there would be a lapse in the connectivity. Therefore, the authors have presented an innovative break glass access control technique using a QR code [5]. The authors have utilized the attribute-based encryption and along with Shamir's Secret Sharing Scheme to provide secure break glass access in the time of an emergency. The experimentation on the proposed technique has demonstrated its efficiency. The major drawback of this proposed technique is the increased space complexity that is observed.

H. Aung explains that there has been a widespread increase in the number of Wireless Sensor Networks as there is a lot of research that is being conducted on this topic along with the large-scale improvements in the production of these wireless sensor devices. These wireless devices are predominantly used for the purpose of implementation in a medical institution to monitor the vital signs of the patients in real-time [6]. But such a system would collect and maintain a personal record of the patient's data, which is at risk of a data leak and encryption of the data would lead to poor handling in the scenario of an emergency. Therefore, the authors have proposed BTG-AC or Break the glass Access control for providing an access control mechanism to access the patient data in the time of an emergency. The main limitation of this paper is that BTG-AC needs the doctor to predefine the BTG policy for every user.

A. Lertpiya elaborates that most of the techniques that provide Natural Language Processing or NLP utilize the various different texts for this purpose wherein all the texts are perfect with correct spelling and grammar, which is very different from real life. Therefore, the authors have proposed a technique for performing Natural Language Processing on user-generated Web content, not much research has been done on this topic in the past years specifically on the actual web data [7]. The proposed Thai NLP tasks achieve an accuracy of 93% demonstrated by the extensive experiments. The major drawback of this proposed technique is the increased computational complexity of the methodology in comparison to conventional techniques.

N. Srinivasan explains that there has been an increase in the number of individuals that have developed an interest in farming and agriculture nowadays. Most of these individuals are from an IT background and other fields, they do not have the expertise that a farmer would accumulate over the years of farming. Therefore, there is a need for guidance from experienced farmers that could help these individuals out [8]. Therefore, the authors have proposed a would allow for communication between the farmers and also facilitate the farmers to collect their knowledge in a database using Subject matter of expertise and the Resource Description Framework or RDF platform is used to answer to user queries.

Y. Liu introduces the paradigm of Blockchain which has been increasing in popularity over the past few years. Due to large-scale use, there is a need for an efficient evaluation of a blockchain that is missing in recent researches [9]. Therefore, the authors have proposed a technique for the evaluation of the blockchain using the continuous-time Markov chain model. The authors have tested the various attributes that affect the reliability and effectivity of the Blockchain. The authors have tested the proposed methodology extensive which has produced satisfactory results. The major drawback of this scheme is that the authors have not considered the consensus algorithm in their application.

K. Kato states that the use of a centralized authority or a central server for any purpose is a very dangerous maneuver and could lead to a massive data leak if the node for the server gets compromised. Therefore, the authors propose the use of a decentralized framework that can be highly secure and robust [10]. The authors then present a Rideshare service that utilizes the blockchain framework for securing the system as well as provide an efficient decentralized system where the drivers can be the miners too. The proposed technique has experimented extensively and the results indicate satisfactory performance. The major limitation of this paper is the increased space complexity observed.

K. Zheng explains on the blockchain paradigm and its increasing popularity nowadays. The blockchain has increasingly used various different applications such as energy, medical applications etc. This is due to the resilience of the Blockchain platform in achieving a tamper-proof application. The authors also comment that there is a lack of research on the various applications in analyzing the performance of a blockchain, therefore, the authors present a technique based on the Practical Byzantine Fault Tolerance (PBFT) and the Continuous-time Markov chain or CTMC to evaluate the performance of a healthcare blockchain network [11]. The experimental results indicate that there is room for optimization in the network. the major drawback of this system is that it has only been simulated.

J. An elaborates on the concept of crowdsourcing, which is based on the concept of “unity is strength” wherein a large group of people complete a complicated task. Crowdsourcing has a large number of advantages such as fast speed, low cost and high convenience. But the crowdsourcing paradigm is not immune to the actions of some individuals with nefarious intents that commit fraud and lower the quality of service for the other workers and requestors [12]. Therefore, to increase accountability and safeguard the platform the Blockchain is introduced. Blockchain successfully implements robust security over the platform and the experimental results demonstrate this effect. The main drawback of this technique is the increased computational complexity of the system.

I. Hashish explains that with the increasing popularity of the Blockchain platform, there has been an increase in the interest in the decentralized architecture which is being applied in various different fields [13]. The cryptocurrencies are getting a highly popular alternative to fiat money and are gaining enormous traction as people from all over the world are investing in the digital currency. Therefore, the authors devise an innovative technique for the prediction of bitcoin prices and also an LSTM or Long Short-Term Memory for the optimization of the blockchain network. The proposed methodology has been experimented extensively and has produced results better than conventional techniques. The main drawback of this technique is that the authors have not utilized the internal details of the bitcoin transactions for prediction purposes.

P. Piriou introduces the stochastic blockchain models which are a simulation tool that is used for the analysis of blockchain applications. The proposed methodology utilizes the PyCATSHOO paradigm which analyses the blockchain application according to its application fields. The simulation also analyses the consistency and performance of the blockchain application through the use of the Markov process [14]. The simulation results indicate that the proposed methodology is consistent and provides efficient results. The major drawback of this scheme is that the tool is not complete as it is just a foundation for the tool.

A. Rajput states that the paradigm of personal health records are the private information of the various different patients, but it is also a piece of valuable information for the different doctors and the individuals suffering from the same ailment. The researchers state that there is a need for maintaining the privacy of personal health records while helping other patients by providing them with effective treatment [15]. Therefore, the author proposes an Emergency Access Control Mechanism or EACMS that safeguards the patient’s data by implementing an efficient and secure access control mechanism through the blockchain platform. The major limitation of the paper is the increased space complexity observed in comparison with the conventional techniques.

Proposed Methodology

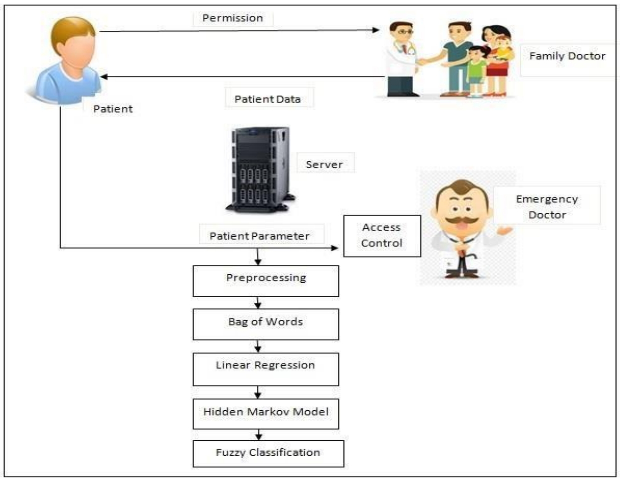


Figure 1: Proposed model System Overview

The proposed methodology for emergency access control system for personal health record based on block chain is depicted in the above system overview diagram of figure 1. The steps that are involved in the process of providing the emergency access control are described in the below mentioned steps.

Step 1: *Data Seeking and Data preprocessing* - This is the basic step of the proposed model, where an emergency doctor who is treating the patient who is visited in bad condition. This Emergency Doctor is seeking the patient info with the earlier diagnosed family physician or the personal health care centers by firing a query about the patient's symptoms and some personal information if they are known to the emergency doctor.

This query on reaching the server, which stored the data of the personal health care system triggers to work to provide the best access controlled data to the emergency doctor. For this purpose the proposed model has to reprocess the query. This preprocessing technique mainly involves the four steps as described below.

Special Symbol Removal- This step involves the shredding of the special symbols from the string of the fired query. All the special symbols are involved in this process like ?,;,., etc.

Tokenization- Tokenization is the process of splitting a string on space to store them in well indexed string. This list eventually helps to maintain the strict processing of the string data in an array, which eases the technique of string handling.

Stopword Removal – Stopwords are conjunctive words of the English language that are often not playing much more important role. On their removal also the semantics of the phrases are almost remain intact. By keeping this idea in mind this step, shred off all the Stopwords presented in the English language. On the removal of this the query string becomes more light weight and retains the core meaning as it was present earlier.

For example, if a phrase was there like: we are going to college. After Stopword removal it becomes going college. Here if we observe the meaning remains unchanged post Stopword removal process.

Stemming- This is the process of bringing the word to its base form to get rid of the redundant data. To achieve this proposed model uses the string replacement technique to replace the irrelevant postfixes with the desired string. For example going will become go after substring "ing" is replaced with an empty character. By observing the difference between the Going and go the core meaning of the word remains intact.

Step 2 : Bag of words and Linear Regression – This is the preliminary step for the prediction of the data for the fired query. Here a bag of words for the diseases are maintained in the database for the possible query words of symptoms. On matching of these symptom words a count has been maintained for the matching of the query words with the bag of words that is stored in an array called x[ ]. And on the other hand a count is maintained for the matching of query words and the stored database is stored in an array called y [ ]. These two arrays are subjected to estimate the Regression analysis in between the bag of words and PHR data for the fired query.

This can be represented by an equation 1.

$Y=mx+b$ ________________(1)

Where:

- ➢ y = how far up
- ➢ x = how far along
- ➢ m = Slope or Gradient (how steep the line is)
- ➢ b = the Y Intercept (where the line crosses the Y axis)

This equation yields the value of the slope and intercept so that a prediction can be made for the specific disease based the highest value of y. This calculation of the regression analysis is calculated using the algorithm 1.

Algorithm 1: Linear Regression Estimation

```
//input: x[ ] ,y [ ]
// Output: Regression List $R_L$
Step 0: Start
Step 1: Initialize sumxy=0, sumx=0,sumy=0,sumx2=0
Step 2: RN = CFL[0]
Step 3: FOR i=1 to size of x
Step 4:  sumxy=sumxy+(x[i]*y[i])
Step 5: sumx=sumx+x[i]
Step 6: sumy=sumy+y[i]
Step 7: sumx2=sumx2+( x[i]*x[i])
Step 8: END FOR
Step 9: $M_N$ = ( size of x[ ] * sumxy) – ( sumx * sumy)
Step 10: $M_D$= ( size of x[ ]* sumx2) – (sumx * sumx)
Step 11: M=$M_N$ / $M_D$
Step 12: B= ( sumy – ( M * sumx))/ size of x[ ]
Step 13: Y=M * x[i] +B Step 14: ADD Y into $R_L$
Step 15: return $R_L$
Step 13: Stop
```

Step 3: Hidden Markov Model – This is the core prediction step which mainly predicts the data which is needed to be provided access control, This is containing three major parts like

(a) Forward Probability : Here all the majorly matched keywords from the bag of words are considered and that row is selected for the access control mechanism.
(b) Backward probability : Here the access controlled data is selected based on the linear regression list and other effective parameters.
(c) Baum-Welch Model: This model eventually includes the both the data from the forward and backward probability to form a possible matrix. This matrix is subjected to transition based on the ratios of the possible data access attributes. Then a ratio is evaluated in between 0 and 1 for each of the rows. The value 1 majorly indicates to provide high access control for the attributes and on the other hand, value 0 indicates low access control for the attributes. This decision will be taken by the Fuzzy Classification process.
Step 4: Fuzzy Classification – This step of fuzzy classification accepts the score list provided by the Hidden Markov model, where the score is varied from 0 to 1. These Scores are divided into 5 fuzzy crisp sets like VERY LOW, LOW, MEDIUM, HIGH and VERY HIGH. Then any of the scores which are fall in these ranges are subject to set the access control rules according to the fuzzy crisp ranges in the inference engine. Once these rules are provided, this data is being forwarded to the Data seeker using the secure channel of the blockchain.

Step 5: Data Routing using the Blockchain- Here in this step the access controlled data is being subjected to evaluate the Hash key using the MD5 algorithm and this hash key is named as the block head key. This hash key is forwarded to both the Data vendor and the data seeker for authentication and integrity evaluation process to maintain the trust less data access control mechanism in the distributed environment.

The whole proposed system is expressed mathematically with the below model.

Mathematical Model

1.S= { } be as system Data Access Control mechanism using blockchain in Distributed system
2.Identify Input as D_R={ D_{R1}, D_{R2}, D_{R3}…. D_{Rn}}
Where D_R= Data Request
S= { D_{Rn}}
3.Identify A_C and D_I as Output i.e. Access Control and Data
Integrity
S= { D_{Rn}, A_C, D_I }
4. Identify Process P S= { DRn,P, AC , DI }
5.P= {L_R ,H_{MM},F_C, B}
Where
L_R =Linear Regression
H_{MM}=Hidden Markov Model
F_C =Fuzzy Classification
B=Blockchain

So the Complete system for heart failure prediction can be given as

6.S = { D_{Rn}, L_R ,H_{MM},F_C, B, A_C, D_I }

IV. RESULTS AND DISCUSSIONS

The proposed methodology in this paper for an efficient Access control mechanism has been developed in Java programming language on the NetBeans IDE. For the development process 3 Laptops are required with a standard configuration of Intel i5 processor with 4GB of physical memory and 500 GB of Storage. The database responsibilities were fulfilled by the MySQL database server along with a Dlink WIFI router.

For determining the performance metrics of the proposed methodology, extensive experimentation was executed and analyzed through the use of Precision and Recall. The evaluation was performed to ascertain that the access control mechanism on the distributed blockchain framework is being implemented according to the expectations.

Performance Evaluation based on Precision and Recall

Precision and Recall are one of the most accurate and insightful parameters that are utilized to extract the performance of the system. Precision evaluates the relevant accuracy of the process by extracting the precise values of the level of accuracy of the system.

Precision in this approach is being defined as the ratio of the number of accurate predictions performed and the combined sum of all the queries that have been matched. Therefore, the parameters in precision allow for an in-depth evaluation of the effectiveness of the methodology completely.

The Recall parameters are different from the precision parameters and instead extract the absolute accuracy of the methodology. This is possible through the evaluation of the ratio of the number of accurate predictions for the given query matched versus the total number of inaccurate predictions for the given query matched. This indicates that the recall extracts the absolute accuracy of the system. Precision and recall are mathematically elaborated in the equations detailed below.

Precision can be concisely explained as below

✓ A = The number of accurate predictions for the given query matched using regression analysis

✓ B= The number of inaccurate predictions for the given query matched using regression analysis

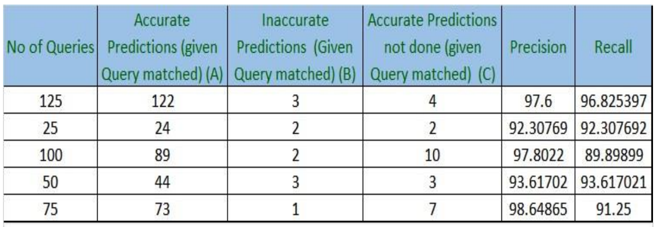
✓ C = The number of accurate predictions that are not done for the given query using regression analysis

So, precision can be defined as

Precision = (A / (A+ B)) *100
Recall = (A / (A+ C)) *100

The above equations are utilized for conducting extensive experimentation on the proposed system through the analysis of the regression results. The analysis results are detailed in table 1, given below.

Table 1: Precision and Recall Measurement Table for the Regression analysis



No of Queries	Accurate Predictions (given Query matched) (A)	Inaccurate Predictions (Given Query matched) (B)	Accurate Predictions not done (given Query matched) (C)	Precision	Recall
125	122	3	4	97.6	96.825397
25	24	2	2	92.30769	92.307692
100	89	2	10	97.8022	89.89899
50	44	3	3	93.61702	93.617021
75	73	1	7	98.64865	91.25

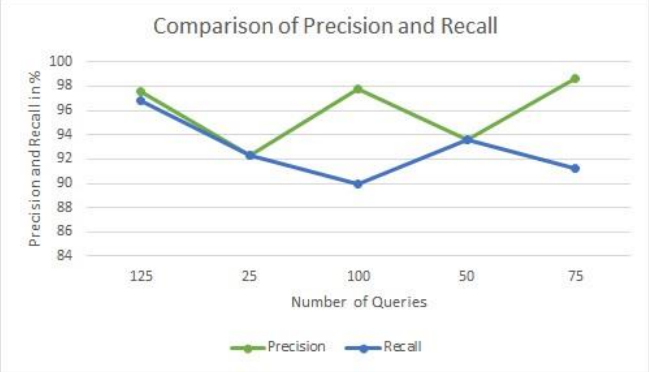


Figure 2: Comparison of Precision and Recall for the Regression analysis

The above graph indicates that the regression analysis of the proposed methodology achieves expected levels of precision and recall. The high values of precision and recall indicate an exceptionally fair execution of the regression analysis module in the proposed methodology.

This experimentational results indicate that the performance of the module designed for the purpose of regression analysis is extremely accurate and is being implemented correctly. The regression analysis is one of the most important aspects of the proposed methodology and its successful and accurate performance is a significant contribution for boosting the further process of Access control mechanism.

Conclusion and Future Scope

The sharing of PHR data is one of the most useful applications that reduce patient suffering and pain. The PHR paradigm allows effective treatment of all the patients in the fastest and most efficient way. For this purpose, several Data Vendors or aggregators collect and dispense PHRs on request. But most of the time the data vendors are not trustworthy which deters most of the data providers due to the fact that the PHRs contain a lot of personally identifiable sensitive information. Therefore, to ameliorate this effect and safeguard the sensitive data, a secure and efficient access control mechanism is proposed based on the decentralized framework called Blockchain. The presented technique also utilizes Linear Regression, Hidden Markov Model and fuzzy classification to achieve its goals of a secure access control system efficiently.

This publication deals with the performance of the regression analysis module through the use of extensive experimentation. The results of the experiment indicate that the proposed regression analysis framework has a comparable performance that is significantly better. Precision and Recall parameters were utilized to ascertain the performance metrics of the regression analysis procedure. The experimental results have been fruitful in determining the superiority of the proposed regression analysis.

For the purpose of future work, the presented technique can be implemented in a real-time scenario. The technique could also be extended to various different fields such as law and agriculture.

References

[1]. M. Khan et al, “A Secure and Flexible e-Health Access Control System with Provisions for Emergency Access Overrides and Delegation of Access Privileges”, 18th International Conference on Advanced Communication Technology (ICACT), 2016.

[2]. N. Lu et al, “An Adaptive Access Control Model Based on Trust and Risk for Medical Big Data”, IEEE 3rd International Conference on Communication and Information Systems, 2018.

[3]. Y. Yang et al, “Lightweight Break-glass Access Control System for Healthcare Internet-of-Things”, IEEE Transactions on Industrial Informatics, 2017.

[4]. F. Ullah et al, “Emergency Data Handling Medium Access Control Protocol for Wireless Body Area Network”, 6th ICT International Student Project Conference (ICT-ISPC), 2017.

[5]. S. Belguith et al, “Emergency Access Control Management Via Attribute Based Encrypted QR Codes”, Fourth Workshop on Security and Privacy in the Cloud (SPC), 2018.

[6]. H. Aung et al, “BTG-AC: Break-The-Glass Access Control Model for Medical Data in Wireless Sensor Networks”, IEEE Journal of Biomedical and Health Informatics, 2016.

[7]. A. Lertpiya et al, “A Preliminary Study on Fundamental Thai NLP Tasks for User-generated Web Content”, International Joint Symposium on Artificial Intelligence and Natural Language Processing (iSAI-NLP), 2018.

[8]. N. Srinivasan and A. Selvaraj, “Mobile Based Data Retrieval using RDF and NLP in an Efficient Approach”, Third International Conference on Science Technology Engineering & Management (ICONSTEM), 2017.

[9]. Y. Liu et al, “Evaluating the Reliability of BlockchainBased Internet of Things Applications”, 1st IEEE International Conference on Hot Information-Centric Networking (HotICN 2018), 2018.

[10]. K. Kato et al, “Blockchain Application for Rideshare Service”, 8th International Conference on Logistics, Informatics and Service Sciences (LISS), 2018.

[11]. K. Zheng et al, “Model Checking PBFT Consensus Mechanism in Healthcare Blockchain Network”, 9th International Conference on Information Technology in Medicine and Education, 2018.

[12]. J. An et al, “Crowdsensing Quality Control and Grading Evaluation based on a Tw o-consensus Blockchain”, IEEE Internet of Things Journal, 2018.

[13]. I. Hashish et al, “A Hybrid Model for Bitcoin Prices Prediction using Hidden Markov Models and Optimized LSTM Networks”, 24th IEEE International Conference on Emerging Technologies and Factory Automation (ETFA), 2019.

[14]. P. Piriou and J. Dumas, “Simulation of stochastic blockchain models”, 14th European Dependable Computing Conference, 2018.

[15]. A. Rajput et al, “EACMS: Emergency Access Control Management System for Personal Health Record Based on Blockchain”, IEEE Access, 2019.