Secure Mobile Health Monitoring System using Order Preserving Encryption

Abhijeet Kurle[1], Dr. Kailas Patil[2], Prof. Narendra Pathak[3]

Abstract— Most of the healthcare organizations were lagging in adoption of new technology. But, in recent few years, researchers are able to enhance healthcare services by using technologies such as mobile devices, wireless sensor networks and cloud computing. Although there is improvement in healthcare services, use of untrustworthy cloud service provider possesses a serious risk on privacy of client's medical data and intellectual property of the mobile health service provider. In addition to that, existing research efforts do not support SQL (Structured Query Language) range queries over encrypted health records stored in cloud database. To address above problems, this paper proposes a novel design of secure mobile healthcare monitoring. The proposed system makes use of Order Preserving Encryption (OPE) technique to provide confidentiality of health records as well as to support range queries over encrypted database. Morever this paper also provides security and performance analysis of Order Preserving Encryption.

Index Terms— Mobile health monitoring, SQL aware encryption, Order preserving encryption.

1 INTRODUCTION

Healthcare organizations in India has underutilized technology as compared to other organizations. According to a survey of the Wipro research team on "The mHealth Case in India" [1], most of the health organizations are still relying on paper based medical records and handwritten prescriptions for diagnostic. Information digitized by healthcare organization is typically not portable; therefore there is little possibility of sharing this information among different healthcare entities. Since information sharing is rare, there is a lack of communication and co-ordination between patients, physicians and other medical community.

However, in recent few years wide deployments of electronic devices such as sensors and smart phones has shown potential in the enhancement of healthcare services [2]. In such type of mobile health monitoring system, wireless body sensor networks are attached to the client's body to collect physiological data like Breathing Rate (BR), Blood Pressure (BP), Blood Glucose and Electrocardiogram (ECG) [3]. This data from client device is sent to a remote server where this data is analyzed, processed and return recommendation about his health and daily activity. The client can also send their queries related to healthcare data. These queries are sent to sever and based on patients past medical details server returns timely advice to the client.

In addition to mobile devices, Cloud computing technologies allow the healthcare service providers to improve their-services with the use of software as a service (SaaS) and Database as a service (DaaS) model [4]. With the use of such technology enables the health service provider to growth in adoption of personal health records (PHR), electronic medical records (EMR) and electronic health records (EHR). Cloudcomputing offers several benefits in the healthcare sector, healthcare organization provides quick access to computing and large storage facility at low cost. However, cloud computing also facilitates sharing of healthcare data across various departments and geographies.

Although use of modern technologies enhances healthcare service, it possesses risk of protecting health information from unauthorized users. Several healthcare organizations store and maintain patient's data electronically. Using cloud computting these organizations outsource patient's health related data to the cloud service provider. The cloud service providers are untrustworthy parties therefore the client's medical data stored on the cloud may be misused by such parties. They might share this data to insurance companies to make profit. Since the cloud service provider is untrustworthy party patient's data must be stored in encrypted format on cloud so that cloud service provider do not learn anything from stored data. Also, there are several laws such as Health Information Privacy and Accountability Act (HIPAA) to protect against violation of privacy of health informatics [5].

Maintaining such healthcare data in secure form is challenging task because, data stored in an untrustworthy environment such as cloud service provider. Though data is stored in encrypted format in the database, researchers [2], [6] failed to encrypt the database schema. However, the cloud service providers may learn about health record from the database schema. To provide confidentiality of electronic health records we have used order preserving encryption scheme. In our proposed system, the client is allowed to enter his medication details which are encrypted on the application server by using OPE and sent to the database server. Whenever client or physician query particular health record, this query is converted into an intermediate SQL query to run directly over outsourced encrypted cloud database.

In summary, we make following contributions

- [1]*Abhijeet Kurle is currently pursuing ME degree in Computer Engineering in Viswakarma Institute of Infromaton Technology, from Savitribai Phule University of Pune, India. PH-0917709522880. E-mail: kurleabhijeet@gmail.com*
- [2]*Dr. Kailas Patil is currently professor in Department of Computer Engineering in Viswakarma Institute of Infromaton Technology, from Savitribai Phule University of Pune, India. E-mail: kailas.patil@viit.ac.in*
- [3]*Prof. Narendra Pathak is currently Associate Professor in Department of Information Technology in Viswakarma Institute of Infromaton Technology, from Savitribai Phule University of Pune, India. E-mail: narendra.pathak@viit.ac.in*

1. We studied existing healthcare monitoring systems and identified the problem for achieving data confidentiality in electronic medical records (EMR).
2. We propose a novel and secure mobile healthcare monitoring system.
3. We propose and implement order preserving encryption (OPE) scheme that preserves the confidentiality of data in outsourced database as well as support SQL range queries over EMR stored in cloud database.

The remaining paper is organized as in section II, we explained the current healthcare scenario in India and the needof security in health informatics. In section III, we presented the existing work on mobile health monitoring and techniques for achieving confidentiality of EMR. Section IV describes our observations based on literature survey and related research study. In section V, we elaborated design and working of secure mobile health monitoring system. It also provides encryption techniques used for obtaining confidentiality of health records and processing of SQL range queries over encrypted relational database. Finally VI and VII, we give implementation details and results of our proposed scheme.

2 CURRENT HEALTHCARE SCENARIO

We did the comparative analysis of healthcare organization's status in India with organizations in some developed countries, according research articles and the World Health Organization (WHO) statistics.

2.1 International Healthcare Status

The healthcare industries in some developed countries are undergoing a change with the focus firmly on improving the quality of care delivered to people. In such organization, there is an increased focus on an integrated healthcare ecosystem with collaboration between various stakeholders. The global market, eHealth services are driven by mobile devices and desktop computers. Wide availability of landline Internet connections and 3G, 4G services from leading operators causes growth in the adoption of a mobile health segment by vendors. For most of the IT organizations, healthcare is a very strategic industry segment. IT organization has a comprehensive presence in the healthcare industry across payers, providers, healthcare distribution, healthcare services, eHealth and government funded programs.

2.2 Healthcare Status in India

India ranks low (115th) amongst world nations judged by Human Development Indicators (HDI). According to the World Health Statistics (WHS) 2013, six doctors per 10,000 people, the number of qualified doctors in the country is not sufficient for the growing requirements of Indian healthcare. Moreover, in rural area "doctors to population" ratio is lower by six times as compared to urban areas. Doctors are the most important part of the healthcare system. However, the rural area of India has 64% shortage of doctors. The population of India is the biggest hurdle in improvement of healthcare services. India is world's second most populous country after China.

The graph in figure 1 presents the statistics taken from the World Health Organization (WHO) [7]. This graph depicts the wide gap in the availability of healthcare facilities in rural and urban area of India. Willingness to pay and lack of awareness in people were the main barriers to adoption of healthcare in rural area. However, this gap in availability can bridge by using mobile technology that delivers healthcare services to the individual's home.

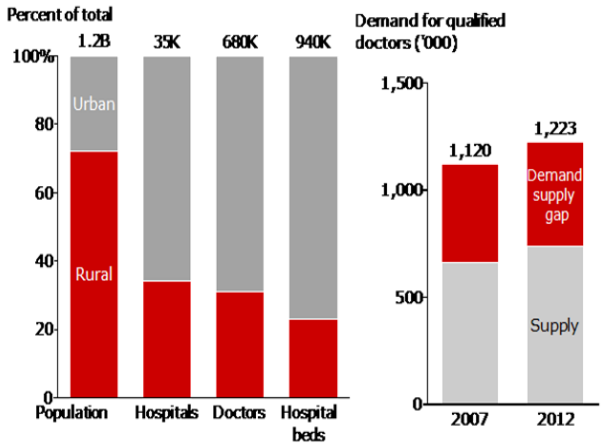

Fig. 1. Availability of healthcare facilities in rural and urban India [7]

2.3 Privacy Isuues in Healthcare Monitoring

All Data encryption is the most effective technique for preventing sensitive data from unauthorized users or curious database administrators [8]. In traditional asymmetric key cryptography or identity-based cryptographic techniques, data is encrypted and it is decrypted only by the intended legitimate user. However, such encryption techniques are not feasible where data is shared with multiple users due to multiple encryptions. Efficient encryption technique needed for more advanced data sharing where data needs to be shared among multiple parties.

Several encryption schemes can be used to preserve privacy of patient's data stored in an outsourced cloud database. Whenever we store data in a relational database at cloud (DaaS) we need some variations in these techniques, because it must be able to run SQL queries over encrypted database [9].

There are two approaches to encrypt data stored in relational database.

1. Encrypt entire database file
2. Encrypt each record stored in a table

In the first case the patient's data is stored in database files in a tabular format. Instead of encrypting each record in table the entire database file is encrypted and stored it on the cloud. Whenever patient requests data from database, entire database file is transferred from the cloud to the application server. This file is now decrypted at the application server and patient's query fired on normal database. The limitation with this solution is that even if access of single record large file is transferred from the network.

In the latter case, each record is encrypted and stored in relational database. Whenever patient queries data from the database, the query is translated in encrypted format and this encrypted query is fired on the encrypted database. These techniques also have challenges in execution of range queries on encrypted database [6].

2.4 Motivating Example

We would like to describe the need of supporting range queries over encrypted data in database as a service model of cloud computing with the help of motivating example. Patient's medical details are stored in a PatientMaster table shown in Table 1 with fields such as patient identification number (PID), Name, age, sex, etc.

Our goal is to encrypt PatientMaster table, so that a curious database administrator of DaaS will not learn anything from

TABLE 1
PATINTMASTR TABLE

PID	Name	Age	Sex
1001	Alice	56	Female
1002	Bob	45	Male
1003	Charlie	40	Male
1004	Danniel	28	Male

the database tables. In addition to that, the proposed encryption scheme must be able to search records of male patient having age between 20 and 40. Hence, we are using order preserving encryption that preserves order over encrypted database. Each column has its own key, all the values in certain column are encrypted by using key for that column.

3 RELATED WORK

There is a lot of research work has been done in the last few years on privacy preserving mobile health monitoring system. The related work is broadly organized into following categories.

3.1 Work Related to Healthcare Services

This section contains research progress and work related to the enhancement of healthcare service [2], [10], [11] The Microsoft launched the project "MediNet" [11]. It was designed for the people suffering from diabetes and cardiovascular disease in remote areas of Caribbean countries. This project is able to give personalized healthcare for the patients having diabetes. They use wearable sensors like Glucose and blood pressure sensors for measurement of glucose level and blood pressure this sensor data is sent to mobile phone through bluetooth or USB cable. The later data is transmitted to the web server via GPRS. At the web server current sensor readings are combined with previous readings and submitted to reasoning engine. By using these readings reasoning engine generates personalized access to the patient.

In [2] Cloud Assisted Mobile (CAM) health monitoring system the patient's data is stored on the cloud. This system is able to make a diagnosis of patient's query by analyzing the patient's history and his medical details. They used ID based-encryption for providing confidentiality to patient's healt records. The branching algorithm is used for diagnosis of a patient based on their medical details. The input to the branching algorithm is patient health data, such as blood pressure, daily medication details and physical activity. According to this input decision tree is formed and a decision is made as a result to the clients query.

Justin Brickell et. al in [10] presented protocol for secure evaluation of diagnostic program. In this paper the branching algorithm which can be represented as a binary decision tree is used to make health recommendation to the user. The user may input their health related data to the branching algorithm then by examining some threshold values branching algorithm will make health recommendations to users. In binary decision tree formed by branching algorithm intermediate node contains predefined threshold values, while leaf node contains the classification label to the user. By applying protocol user evaluates servers branching algorithm on users local data without revealing any data to server except the classification label.

3.2 Work Related to Access Control Policies

To avoid privacy exposure of EMR, most of the system makes use of encryption techniques. However, enforcing access control policies over encrypted data was challenging task. To address this issue, researchers came up with new encryption standards [12]–[15].

In [12] D. Boneh and M. Franklin provide the first solution to the open problem of Id based encryption proposed by Shamir in 1984. Identity-based encryption (IBE) is one of the forms of public key cryptography. It is initiated by the sender which uses a unique identifier of the recipient (such as his email address) is used to calculate a public key. Private Key Generator (PKG) uses a cryptographic algorithm to calculate the corresponding private key from the public key. Recipients can generate their own private keys directly from the server as they needed, also they don't require distribution of their public keys. The sender encrypts a message by recipient's public identity and sent to the receiver, the receiver uses a private key received from PKG to decrypt the message. However, this scheme suffers from the problem that it requires a centralized server in order to create and distribute keys. IBE's centralized system shows that some keys must be created and held in escrow and are therefore at greater risk of disclosure.

The first KP-ABE technique allows monotone access structures and was proposed by Goyal et al. [13] in 2005, in that access policies are associated with keys, while first CP-ABE technique was proposed by Bethencourt et. al. [14] in 2007 in which, access policies are associated with cipher texts. In ABE techniques mentioned above, users have to prove their identity to the trusted party. After proving identity user obtains a private key which is used for decryption of messages. However, in hierarchical ABE [15] technique user's secret key is no longer authorized by a single authority, but it is authorized separately by different independent and cooperative authorities.

3.3 Work Relaed to OPE and SQL aware Encryption

Most of the encryption techniques fail to process encrypted data at database server stored in RDBMS (Relational Database Management System). In order to process encrypted data, all records from the database were fetched to the application server. However, some researchers [16]–[20] proposed schemes that processes SQL queries directly on encrypted

RDBMS. This causes a performance overhead due to increased traffic between application server and database server.

OPE was first proposed by R. Agrawal, R. Shrikant et.al. [16]. In this research work focus was on encryption of integer dataset. The data encryption is done in such a way that, ciphertexts generated from this scheme follow certain type of distribution. For the generation of encryption function there is need of all input integer dataset and possible sample distribution. The encryption key is generated from these samples. If database does not contain minimum records required for encryption, then DBA must add some records manually. In addition to that, the authors used linear interpolation for distribution of data among several buckets. However, the speed of an encryption scheme is inversely proportional to database size. Hence, this technique is not suitable for large databases.

In 2007 Alexandra Boldyreva et. al. in [17], [18] came up with Order-preserving symmetric encryption which is based on pseudo random function (PRF) for encryption of numeric data. The authors suggest and analyze the notion of one-ways in to improve security of OPE. With this approach, encryption function based on hypergeometric distribution maps plantexts from the set [1, 2... M] to the set [1,2... N] where N > M. The ciphertexts generated from this scheme is in order and associated correspondingly with plaintext numbers.

Raluca popa et.al. [19], 2011 designed CryptDB which gives adjustable query based encryption for providing confidentiality of data stored on cloud database. They use proxy which act as intermediate between application and database. The data sent from the application is in plain text which is encrypted at proxy and encrypted data is stored in the database server stored in the cloud. Whenever an application requires data, the database proxy translates plain query into an encrypted query to run over encrypted database. The results fetched by SQL query is in encrypted format. These results are converted into plain text and given to the application server. However, CryptDB suffers from the space overhead limitation. To support equality, range and aggregate queries CryptDB encrypt each column from database to three or more columns.

3.4 Our Observations

Based on a literature survey and comparative analysis of the availability of healthcare services, we lead to the following observations:

1. Healthcare services improved by technologies such as mobile devices and cloud computing.
2. The data must be stored on a cloud in encrypted form and need a mechanism to enforce access control policies.
3. There is very little work has been done in privacy of outsourced databases (Daas), none of work is efficient.
4. The challenging problem is to perform certain operations and SQL queries over encrypted data stored on the cloud.

4 Proposed Secure Mobile Healthcare Monitoring System

Secure mobile healthcare monitoring system consists of four parties client or patient, physician or healthcare service provider company, Private Key Generator (PKG) and cloud service provider. The figure 2 depicts the information flow throughout the system between involved parties

4.1 Proposed System Architecture

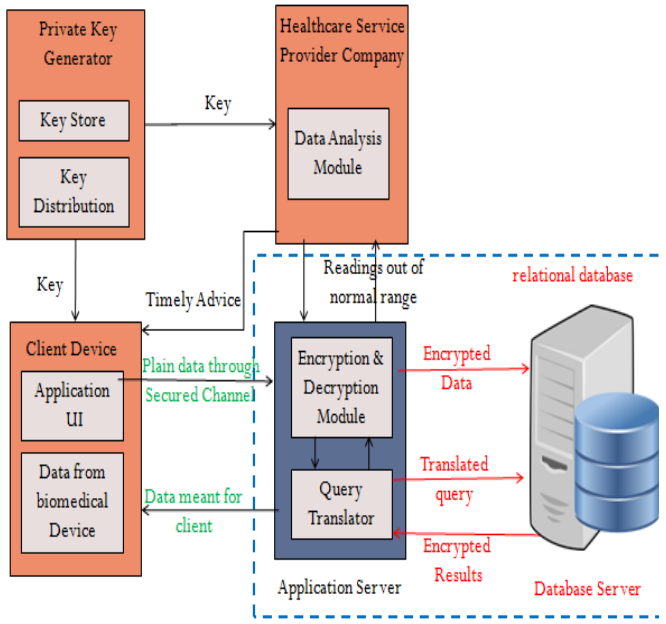

Fig. 2. System architecture for secure mobile health monitoring system

In the proposed system client first registers to the healthcare system by entering his or her personal details. These personal details from his electronic device such as smart phone, tablet, laptop or personal computer is transformed into attribute vectors. This attribute vector is given as input to the branching algorithm. The branching algorithm then runs over predefined threshold values set by healthcare service provider in cloud database. If a patient's health details are within threshold value, then branching algorithm generates timely advice to client based on their current and previous reading. If a patient's health details are not within threshold values, then these details are transferred to healthcare service provider company. Physician at company analyze the patient details by data analysis module. Physician gives advice to a patient about his daily activity and diet based on statistics generated from data analysis module. However, all the medical details of the patient as well as medical advice from a physician are encrypted on the application server by encryption module and stored in relational database hosted at cloud.

The keys are required for encryption of clients health records are generated by Private Key Generator (PKG). PKG is responsible for the creation and distribution for matrix based keys to involved parties in the encryption process. Whenever a physician requests for a particular health record from database, physician's request is translated by the query translator into intermediate SQL query which runs over encrypted database. The results of this query are in encrypted format, which are again decrypted at the application server. Finally decrypted results are provided to a physician or healthcare service provider. Query translator module at application server anonymizes column names, table names and attributes constants to hide health record details from database administrator of

cloud database. The database server is untrustworthy since it is hosted in cloud.

4.2 Branching Algorithm

The branching algorithm consists of binary classification. Based on input user value a tree will traverse and provide the decision to the user which is present at leaf nodes. Let V be the vector of clients' information in terms of attributes. Each node has a threshold value to create an information component with information index and the respective information value. The first element is a set of nodes in the branching tree in figure 3. Node above a leaf node takes decisions and label associated with the decision or feedback is present at leaf nodes.

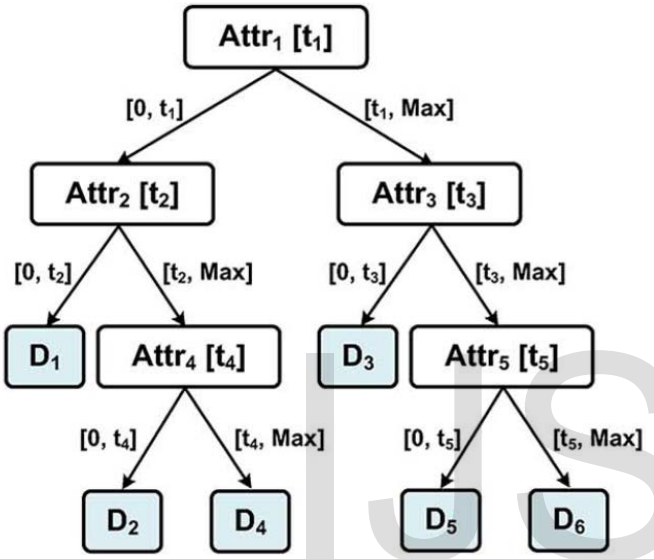

Fig. 3. Branching Algorithm

Health monitoring system works on branching algorithm. A similar algorithm is used by "MediNet" project [11] to make the diagnosis of patients having cardiovascular disease or diabetes. Branching algorithm works like a binary decision tree where decisions are taken according to user's monitoring details. The measure monitoring details of patient are represented by attribute vector V = (v_1; v_2; $v_;$ v_n). According to these monitoring details, the decision tree is formed. A leaf node of this tree represents diagnosis based on user's attribute vectors. Each non-leaf node in the tree is a decision node while leaf node is labeled node.

The patient will input his or her medical details such as blood pressure value, whether they missed a daily medication, whether they have abnormal diet and energy consumption activities. These values are inputted to the branching algorithm, the algorithm then will able to give recommendation to patients so that they will improve their health.

Example: Suppose a particular patient query to branching program with input details such as blood pressure = 160, missed medication one time, energy consumption in calories = 1000 Kcal and information about diet, such as salt intake = 1100 milligrams with threshold values such as t_1 = 150, t_2 = 0, t_3 = 800 Kcal, t_4 = 1500. The decision returned from branching algorithm is "D4; D5; D6" which is notify next kin, modify daily diet, and take regular medicine.

4.3 SQL aware Encryption Scheme

As inspired from Gentry's scheme [21], we propose a novel encryption scheme that performs SQL queries on the encrypted database. There are few SQL aware encryption schemes that use encryption technique based on the data type of attributes entered by the user and set of possible SQL queries on that attribute. If the data type of user entered attribute is text, then the type of SQL queries on this data type are equality predicate queries and LIKE operator queries [22]. If the data type of user entered attribute is numeric, then the type of SQL queries possible on that attribute are queries that involve equality predicates, queries that involve arithmetic operations and queries that involve comparison predicates and aggregate queries. We are interested especially in performing range SQL queries over encrypted database.

All the medical details of clients and healthcare service provider are stored in relational database. The database is outsourced to the cloud service provider. Since cloud service providers are untrustworthy parties the data is stored in encrypted format. The data is encrypted in such a way that, SQL range queries are directly processed on the encrypted database. This technique does not require decryption of data for SQL query processing. Following steps are require for processing range queries over encrypted electronic health records

1. The application issues a query, which is translated into a query that runs over encrypted data: it anonyms each table and column name, and, using the master key MK, encrypts each constant in the query with an encryption scheme best suited for the desired operation.
2. Translated query forwarded to the DBMS server, which executes using standard SQL over encrypted database.
3. The DBMS server returns the encrypted query result, which is decrypted by the application server and returns plain results to the application.

4.4 Order Preserving Encryption

Each medical record of the patient is encrypted with OPE scheme. This scheme does not disclose information about initial values of health records to DBA. With this scheme, each plaintext p is converted into ciphertext tuple <c_1, c_2, c_3>.

1. **Key Generation:** Private key <A, σ >is generated as
   a. Matrix A is chosen non degenerate matrix of order n*n (where det (A)!= 0) over finite field Z_m with m>2 and n >2.
   b. Matrix σ is transformation matrix with elements = {1, 2, 3 … (n*n-1)}

2. **Encryption:** The encryption process converts plaintext x into ciphertext tuple <c_1, c_2, c_3> with the help of matrix key pair <A, σ >.
   a. The first element c_1 from ciphertext calculated as

$$\sum_{i=1}^{c_1-1} d(A^i) \leq p < \sum_{i=1}^{c_1} d(A^i) \quad (1)$$

Where,

$$A = \sum_{i=0}^{n^2} a_i$$

d (A) =sum of elements a_i of matrix

Matrix permutation is done over finite field Z_m

b. To calculate c_2, we need to calculate the sum

$$S = \sum_{i=0}^{c_2} a'_i$$

Where,
a'_i= is elements from matrix A^{c1} σ

$$S \leq p - \sum_{i=1}^{c_1-1} d(A_i) \quad (2)$$

c. Finally c_3 is calculated as

$$c_3 = \sum_{i=1}^{c_1-1} d(A_i) - S \quad (3)$$

3. **Decryption:** The decryption process converts ciphertext tuple <c_1, c_2, c_3> into plaintext p by using matrix key pair <A, σ >.
   a. First we calculate c_1^{th} permutation of matrix A, i.e. A^{c1}
   b. By using σ matrix permutations, we calculate

$$S = \sum_{i=0}^{c_2} d(a'_i) \quad (4)$$

Where, a'_i is elements ot matrix σ A^{c1}

c. Adding third element to obtained sum S, we get element h which equals to following according to encryption procedure

$$h = c_3 + S = x - \sum_{i=1}^{c_1-1} d(A^i) \quad (5)$$

d. Finally by using c1, S and c3 values p can be calculated as

$$p = h + \sum_{i=1}^{c_1-1} d(A^i) \quad (6)$$

5 IMPLEMENTATION DETAILS

We implemented the secure mobile health monitoring system in C# and SQL Server. We used Microsoft visual studio 2010 tool for implementation of the mobile healthcare system on Windows 7. The data entered by a client is encrypted by using the OPE as elaborated in algorithm 1. We designed and implemented algorithm 1 in C# for encryption of health records. In this algorithm, we used BigInteger class to encrypt very large numbers. We extended the traditional OPE algorithm to support encryption of numbers as well as strings. The input for this algorithm is patient health data like name, age, medication details, and information about diet. Now the numeric data is supplied directly to the algorithm, on the other hand, string data is first encoded into numeric data. This numeric data then supplied to the algorithm as an input for encryption purpose. Now, these details are encrypted by using OPE and key for a specific column. Each column inside table has its own key for encryption. Finally, this encrypted data is stored in SQL server 2008.

Algorithm 1 : Order Preserving Encryption

Input: Plaintext = p, Key = matrix pair <A, σ >
Output: Ciphertext = $<c_1, c_2, c_3>$
Initialisation : $c_1 = 0$; $SumDetMat = 0$;
$MatrixA^{c_1} = IdentityMatrix$;

1: **Start**
2: To calculate c_1
3: **while** $SumDetMat(A^{c_1}) \leq p$ **do**
4: $MatrixA^{c_1} = MatrixA^{c_1} * MatrixA$;
5: $detMatrix(A^{c_1}) = CalculateDet(MatrixA^{c_1})$;
6: $SumDetMat(A^{c_1}) = SumDetMat(A^{c_1}) + detMatrix(A^{c_1})$;
7: **end while**
8: To calculate c_2
Transform Matrix A^{c_1} according to Matrix σ
9: Matrix $A^{c_1}\sigma$ = TransformMatrix(Matrix A^{c_1}, Matrix σ);
10: **while** $c_2 \leq (p - SumDetMat(A^{c_1-1}))$ **do**
11: **for** $i = 0$ to n **do**
12: **for** $j = 0$ to n **do**
13: $sumuptoc_2 = sumuptoc_2 + MatrixA^{c_1}\sigma[i, j]$;
14: $c_2 + +$;
15: **end for**
16: **end for**
17: **end while**
18: To calculate $c_3, c_3 = p - SumDetMat(A^{c_1-1}) - sumuptoc_2$;
19: return $<c_1, c_2, c_3>$
20: **End**

In order to encrypt string, we first encoded string into digital code. After this conversion, the string is encrypted by using key matrices called A and σ. The entire encryption is done at the application server; finally the encrypted details of patients are stored on the cloud database. In order to hide schema details, we anonymized table names; i.e. patient table is stored in the cloud database with some different name like tableX. We also anonymized column names of the table.

The figure 4 and figure 5 depicts EMR of patients inside table before and after applying our proposed OPE technique respectively. The table in figure four contains information about patient health details, such as name, age, gender and so on. These details reveal all the information to DBA of cloud databases. However, the second table in figure five contains information about patient health details in encrypted format. In addition to that, we also anonymized database schema to prevent exposure of schema details. Each and every object from the database is anonymized so that curious database administrators will not learn anything from our database. On the other hand patient or physician shouldn't care about weather data in encrypted or not.

	Id	Name	City	Height	Weight
1	7	rahul	kop	5.80	65.00
2	8	DKP	Pune	6.00	65.00
3	9	mayuri	Abad	5.10	42.00
4	10	Nivant	delhi	8.00	55.00
5	11	Nivant	pune	7.00	60.00
6	12	dkp	Jalgaon	8.00	55.00

	Col1	Col2	Col4	Col5	Col6
1	7	~8uWC1♥UFYtHwo"@JCMk$l/s-♣u7vXw	~jXL53331nf3Omg_@lJZnnMlyU=J+j	0105	0505
2	8	~rT"♦Kf$`m*,no"@JCMk$l/s-♣u7vXw	~8VAH3D-60f3Omg_@lJZnnMlyU=J+j	0106	0514
3	9	~lT+OD6♀♣g%♥3fF@JCMk$l/s-♣u7vXw	~98R=J{-{[.3Omg_@lJZnnMlyU=J+j	0104	0415
4	10	~r TE♣=:MY@Hwo"@JCMk$l/s-♣u7vXw	~NQABP,~Enf3Omg_@lJZnnMlyU=J+j	0105	0417
5	11	~R.TB_b❀MY@Hwo"@JCMk$l/s-♣u7vXw	~QXL=LB♠Enf3Omg_@lJZnnMlyU=J+j	0104	0504
6	12	~9lWCE4❀MY@Hwo"@JCMk$l/s-♣u7vXw	~oJN♣D,♣♥H23Omg_@lJZnnMlyU=J+j	0106	0506

Fig.5. The encrypted table stored in database if it would be outsourced to untrustworthy databasedatabase

6 RESULT ANALYSIS

We implemented and tested the results "Secure Mobile Health Monitoring System using Order Preserving Encryption" on PC with Intel(R) core i3 processor, four GB RAM and Windows 7 operating system. These results were analyzed with respect to efficiency of healthcare system, security and performance factors of order preserving encryption.

6.1 Efficiency of Secure Healthcare System

To asses our secure healthcare system we conducted few experiments and compared system generated results with the results in CAM [2], MediNet [11] and [19] projects.

In our system, we assumed the maximum 100 nodes in generation branching program. It represents more complex decision support system as compared to decision support system in MediNet project with 31 nodes. The attribute vector for branching program contains ten attributes which is greater than four attributes in MediNet project. The attribute vector or tuple generated by client is encrypted using order preserving encryption (OPE) scheme. Each node in branching program is encrypted by using OPE. The time required for encryption of each node in branching program roughly takes 600 to 1000 milliseconds based on character length of node and size of key used for encryption. Each node is encrypted only once hence encryption time is much lesser than CAM project which is near about 10 seconds. In our healthcare system, we does not involved Trusted Authority (TA) as involved in CAM, therefore the work of client authentication and token generation is done by healthcare company itself, this reduces overhead of key re-generation.

Finally all the medical records of client or patient are encrypted using order preserving encryption and stored in relational database. Whenever, particular client queries about his health details or physician wants to access data for his client, these queries are directly processed at database server. We analyzed this query processing time over encrypted database with respect to CryptDB [19]. The table 2 obtains time required

TABLE 1
TIME REQUIRED FOR PROCESSING RANGE QUERIES OVER EMR

Number of records	SQL server	CryptDB	Our system
100	85 ms	414 ms	164 ms
500	120 ms	785 ms	764 ms
1000	140 ms	1682 ms	1583 ms
5000	320 ms	5560 ms	6046 ms
10000	493 ms	7203 ms	8348 ms

for accessing encrypted electronic health records of patient from database. From these statistics it is clear that our system processes range queries efficiently than the CryptDB for less than 1000 electronic health records.

All these queries involve only read operation from the relational database. The CryptDB or other existing OPE schemes such as [17] [16] has overhead of database insertion while inserting new health record. These schemes required to modify key to re-encrypt database while insertion of new record to the database. Also CryptDB system encrypts each attribute of EMR by different techniques such as deterministic encryption, order preserving encryption, homomorphic encryption and the ciphertexts generated from these schemes are stored if separate columns. This increases space overhead of healthcare system. However, in our scheme we encrypt each attribute of EMR only once by OPE and stored in particular column of relational database. Our system requires lesser space for storage of EMR than the CryptDB.

6.2 Performance of OPE

We have used different key size for the encryption of health records. The key size varies from 32 bit to 512 bit; this key is transformed into square matrix ranging from order two to our eight. We examined that performance of the algorithm is inversely proportional to key size. This is because the time of encryption increases when using matrices of bigger size. Figure 6 depicts the time in milliseconds to encrypt certain plaintext with different key size. The increase in key size degrades the performance of an algorithm.

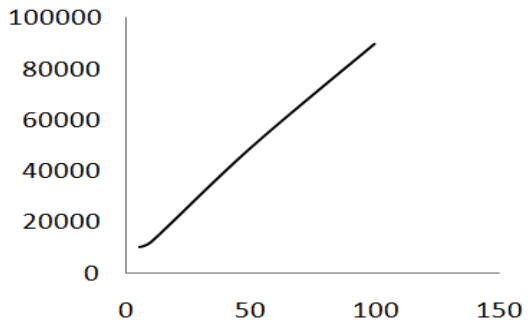

Fig.6. Encryption time in ms with respect to key size of matrix of order n*n

H[illegible] an
ac[illegible] n-
creasing the size modulo factor of an algorithm we can increase the number of elements in the matrices, hence it will lead faster encryption of large numeric data or string. The graph in figure 7 depicts encryption time in millisecond to

encrypt certain plaintext.

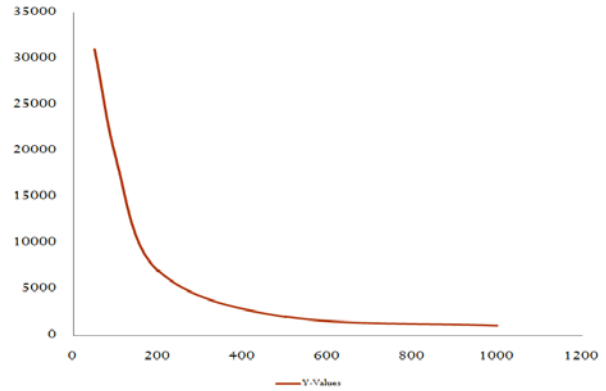

Fig.7. Encryption time in ms with respect to modulo factor of an algorithm

6.3 Security of OPE

Further, we analyze the security of the proposed system with respect to key size and attacks such as a brute force attack and ciphertext-only attack. Our algorithm is strong enough against ciphertext-only attacks. If the attacker does not have any key parameters other than ciphertext parameters $<c_1, c_2, c_3>$, then there is very little chances of a possibility of the ciphertext only attack with our system. Suppose the key of a matrix is of order n*n and permutation operation is performed under modulus m. Now, the sum of matrix elements ranges from minimum (n+1) to maximum n^2 (m-1), and presented with m_K variants.

The proposed OPE scheme is secure against brute force attack. Since the key size in OPE varies from 32-bit to more than 512-bit, the combinations required to break this algorithm is large enough ranging from 2^{32} to 2^{512}. Therefore, it is impossible to break this algorithm in polynomial time and learn about the health records stored in an outsourced database. Cloud also fails to obtain any information about the clients attribute vector as well as branching program from the query submitted to the curious database administrator. In addition to that secrecy of ciphertext in proposed OPE technique guarantees that cloud neither learn about leaf decision nodes or the intermediate threshold nodes from branching tree. On the other hand, a client is completely unaware about the encryption/decryption process. They gain information of decision regarding their query from doctor or health care service provider.

We analyze the cryptographic strength of the algorithm with the help of results shown in the graphs of figure 8 and figure 9. In these figures, we have shown the amount of change in the ciphertext with respect to change in plaintexts. These results are obtained by using 128-bit key, which is key of matrix 4*4. With constant key size the ciphertext elements $<c_1, c_2, c_3>$changes with respect to change in plaintext.

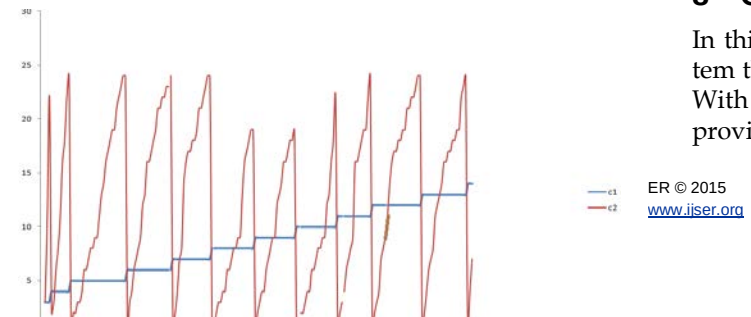

TABLE 2
TIME REQUIRED FOR PROCESSING RANGE QUERIES OVER EMR

Number of records	SQL server	CryptDB	Our system
100	85 ms	414 ms	164 ms
500	120 ms	785 ms	764 ms
1000	140 ms	1682 ms	1583 ms
5000	320 ms	5560 ms	6046 ms
10000	493 ms	7203 ms	8348 ms

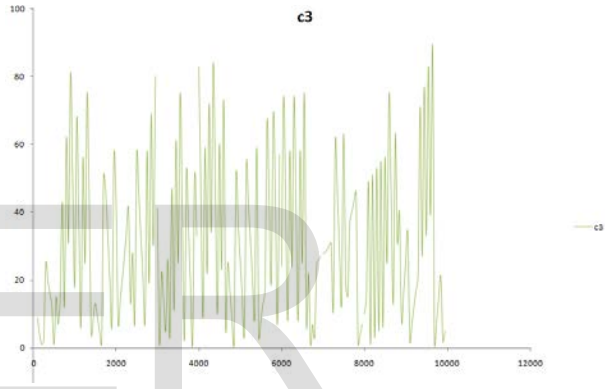

Fig.9. Change in ciphertext elements c3, with respect to change in plaintext

7 Discussion and Future Work

The results of OPE scheme are poor under certain circumstances. We cannot apply null string or string containing all spaces as a key to our algorithm. This causes generation of zero matrix, and as a result, this matrix fails to do permutation operations specified in an algorithm. However, we are working on advancement in key generation algorithm. The key size in OPE can be chosen according to a range of expected values inside a specific column, for better performance of an algorithm. There are certain possible ways to enhance the performance of OPE with the help of standard algorithms that generate matrix permutation in parallel using graphics processor unit (GPU). In addition to that, we are currently working on the mathematical study to improve cryptographic strength of proposed algorithm. We also are trying to attack our proposed system for security enhancement of electronic medical records.

8 Conclusion

In this paper, we proposed secure healthcare monitoring system that makes use of mobile and cloud assisted technologies. With the use of order preserving encryption, we are able to provide confidentiality to client's health records even if data-

base administrator is untrustworthy. The proposed scheme does not leak any information about health records, except the order of plaintexts. OPE scheme can also be used in the scenario where confidentiality of database is must and still there is a requirement to support SQL queries over encrypted database.

REFERENCES

[1] S. Lunde, "The mhealth case in india," Industry white paper of Wipro Council for Industry Research (WCIR), Available at https://www.wipro.com/documents/the-mHealth-case-inIndia.pdf.

[2] H. Lin, J. Shao, C. Zhang, and Y. Fang, "CAM: cloud-assisted privacy preserving mobile health monitoring," *IEEE Transactions on Information Forensics and Security*, vol. 8, no. 6, pp. 985–997, 2013.

[3] M. Barni, P. Failla, R. Lazzeretti, A.-R. Sadeghi, "Privacy-preserving ECG classification with branching programs and neural networks," *IEEE Transactions on Information Forensics and Security*, vol. 6, no. 2, pp. 452–468, 2011.

[4] M. Jang, M. Yoon, and J.-W. Chang, "A privacy-aware query authentication index for database outsourcing," in *Big Data and Smart Computing (BIGCOMP), 2014 International Conference on*, pp. 72–76, Jan 2014.

[5] J. W. Brady, "Securing health care: Assessing factors that affect HIPAA security compliance in academic medical centers," in *HICSS*, pp. 110, IEEE Computer Society, 2011.

[6] H. Hacig¨um¨us¸, B. Iyer, C. Li, and S. Mehrotra, "Executing sql over encrypted data in the database-service-provider model," in *Proceedings of the 2002 ACM SIGMOD International Conference on Management of Data*, pp. 216–227, ACM, 2002.

[7] "World health organization" healthcare statistics for India. Available at http://www.who.int/countries/ind/en.

[8] A. Cavoukian, A. Fisher, S. Killen, and D. Hoffman, "Remote home health care technologies: how to ensure privacy? Build it in: Privacy by design," *Identity in the Information Society*, vol. 3, no. 2, pp. 363–378, 2010.

[9] H. Hacig¨um¨us, S. Mehrotra, and B. R. Iyer, "Providing database as a service," in *Proceedings of the 18th International Conference on Data Engineering, San Jose*, CA, USA, pp. 29–38, 2002.

[10] J. Brickell, D. E. Porter, V. Shmatikov, and E. Witchel, "Privacypreserving remote diagnostics," in *Proceedings of the 14th ACM Conference on Computer and Communications Security*, CCS '07, pp. 498–507, ACM, 2007.

[11] P. Mohan and S. Sultan, "Medinet: A mobile healthcare management system for the Caribbean region," in *Mobile and Ubiquitous Systems: Networking Services, MobiQuitous, 2009. MobiQuitous '09. 6th Annual International*, pp. 1–2, July 2009.

[12] D. Boneh and M. K. Franklin, "Identity-based encryption from the weil pairing," *in Proceedings of the 21st Annual International Cryptology Conference on Advances in Cryptology*, CRYPTO '01, (London, UK, UK), pp. 213–229, Springer-Verlag, 2001.

[13] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-based encryption for fine-grained access control of encrypted data," in *Proceedings of the 13th ACM Conference on Computer and Communications Security*, pp. 89–98, ACM, 2006.

[14] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attribute-based encryption," in Security and Privacy, 2007. SP '07. *IEEE Symposium on*, pp. 321–334, May 2007.

[15] G. Wang, Q. Liu, J. Wu, and M. Guo, "Hierarchical attribute-based encryption and scalable user revocation for sharing data in cloud servers," *Comput. Secur.*, vol. 30, pp. 320–331, jul 2011.

[16] R. Agrawal, J. Kiernan, R. Srikant, and Y. Xu, "Order preserving encryption for numeric data," in *Proceedings of the 2004 ACM SIGMOD International Conference on Management of Data*, SIGMOD '04, pp. 563–574, ACM, 2004.

[17] A. Boldyreva, N. Chenette, Y. Lee, and A. O'Neill, "Order-preserving symmetric encryption," in *Proceedings of the 28th Annual International Conference on Advances in Cryptology: The Theory and Applications of Cryptographic Techniques*, pp. 224–241, Springer-Verlag, 2009.

[18] A. Boldyreva, N. Chenette, and A. O'Neill, "Order-preserving encryption revisited: Improved security analysis and alternative solutions," *in Proceedings of the 31st Annual Conference on Advances in Cryptology*, pp. 578–595, Springer-Verlag, 2011.

[19] R. A. Popa, C. M. S. Redfield, N. Zeldovich, and H. Balakrishnan, "Cryptdb: Processing queries on an encrypted database," *Commun. ACM*, vol. 55, pp. 103–111, Sept. 2012.

[20] S. Krendelev, M. Yakovlev, and M. Usoltseva, "Order-preserving encryption schemes based on arithmetic coding and matrices," *in Computer Science and Information Systems (FedCSIS), 2014 Federated Conference on*, pp. 891–899, Sept 2014.

[21] C. Gentry, "Fully homomorphic encryption using ideal lattices," in *Proceedings of the Forty-first Annual ACM Symposium on Theory of Computing, STOC '09*, pp. 169–178, ACM, 2009.

[22] D. X. Song, D. Wagner, and A. Perrig, "Practical techniques for searches on encrypted data," in *IEEE Symposium on Security and Privacy*, 2000. Proceedings. 2000, pp. 44–55, 2000.

[23] A. S. Kurle, K. R Patil, "Survey on Privacy Preserving Mobile Health Monitoring System using Cloud Computing," in *International Journal of Electrical, Electronics and Computer Systems (IJEECS)*, Volume 3, Issue 4, pp. 31-36, 2015.

[24] A. R. Mathew, A. Al Hajj, K. Al Ruqeishi, "Cyber crimes: Threats and protection, in "*International Conference on Networking and Information Technology (ICNIT)*, pp 16-18, 2010.

[25] S. B. Sadkhan, "Cryptography: current status and future trends, in " *International Conference on Information and Communication Technologies: from Theory to Applications*, pp 417-418, 2004.