ISSN (Print) : 0974-6846
Indian Journal of Science and Technology, *Vol 9(32), DOI: 10.17485/ijst/2016/v9i32/88703, August 2016* ISSN (Online) : 0974-5645

Preserving Data Privacy with Record Retrieval using Visual Cryptography and Encryption Techniques

Hare Ram Sah[1*] and G. Gunasekaran[2]

[1]Faculty of Computer Science and Engineering, Sathyabama University, Chennai - 600119, Tamil Nadu, India; ramaayu@gmail.com
[2]Department of Computer Science and Engineering, Meenakshi College of Engineering, Chennai - 600078, Tamil Nadu, India; gunaguru@yahoo.com

Abstract

Objectives: Secure data sharing using visual cryptography with selective retrieval upon key match is introduced in this paper. As an illustration, medical and student database is considered. **Methods/Analysis:** The original database is stored as relational database model. In shared data applications encryption is used to achieve privacy of sensitive (personal) data from unauthorized users. The work includes encryption, selective retrieval, retrieving records with matching markers, etc. The proposed system search records from queries in the encrypted domain itself. **Findings:** All application related operations like checking for some threshold value, searching for similar records across different users, etc. is included. Because of proposed system any leakage of information over retrieved set of documents is avoided. Existing searching algorithm requires O (n) comparisons (searching operations) at the server to evaluate if the database contains a chosen keyword. The communication overhead minimized between the user and server. The computation is minimized between server and user. It allows the multi-user to search over the encrypted data. Searching time is minimized by relational database management. From encrypted query server cannot, distinguish between documents, determine document contents, check for search keyword and extend beyond decrypted result. **Novelty/Improvement:** The algorithm is novel in the sense that uncorrelatedness among the different user's data is preserved, along with complete sharing.

Keywords: Encryption, Data Privacy, Decryption, Record Retrieval, Visual Cryptography

1. Introduction

Data confidentiality is important in database management. Client database needs to be encrypted and stored on third party server along with multiple data. The authorized user wants to search the database with certain keywords on server among the encrypted list of documents. For example, the database of a medical record (patient) can contain cardiology report, genomic data, ophthalmology reports, billing information, insurance details etc... Existing encryption techniques do not preserve privacy at individual field level of the user. In existing encryption, the entire database file is encrypted and stored in cloud server. When queries are sent from client to server, decryption of entire database is done. The advantage of this method is that it is simple. However, it has the disadvantage that, retrieval of cardiology data of a patient by an expert also reveals the other data like his genomic data, ophthalmology reports, billing information etc. unintentionally. In this paper an improved secured database management is achieved. A secured data sharing system for medical database is proposed. In telemedicine system the use of central repository (used in conventional method for local database sharing) is avoided by proposed system. Proposed system is responsible only for answering queries from user by transfer requested dataset to the union dataset. Proposed system allows database integration (i.e. intersection)[1]. A detailed study of Mobile Health Monitoring System (MHMS) in the point of view of security of user's data which is stored in cloud service provider (i.e. third-party). Importance of privacy preserving in MHMS is studied. The proposed encryption methods are providing security to stored medical data in third party (i.e. cloud storage). These encryption methods

* *Author for correspondence*

are providing only the access control schemes over secured data rather than secure data retrieval[2]. Self-protecting Electronic Medical Records (EMRs) is designed with attribute based encryption and it is implemented on mobile device. The developed prototype model uses a novel key, attribute based encryption library and cipher text-policy. Proprietary android app is developed to retrieve the secured database through their mobile phone and securely store those records to designed EMR model is also possible[3]. In this paper, design of a confidential healthcare monitoring system to secure the user's data across the third party storage system such as outsourced cloud database is proposed. The proposed system made to used rage SQL queries over the encrypted relational database. The proposed privacy preserving mobile health monitoring system provides security to the client's medication details stored in cloud database by encryption techniques. This system not only provides confidentiality of client's medical records but also supports range queries over encrypted database[4]. This paper proposes a new CP-ABE (cipher text policy attribute based encryption) method is extended with hidden access scheme. Proposed system achieves constant cipher text size and hides the access schemes against the third party user. In this paper new technique for the design of CP-ABE schemes using AND-gate enabled with wildcard access configuration is proposed. Two vectors are generated from access scheme and client attributes and Inner Product Encryption is applied to hide the access scheme[5]. In this paper, an efficient method for similarity search over secured data (i.e. in encrypted form) is proposed. The effectiveness of the proposed system is studied to confirm the security level. The performance of the proposed method is evaluated by various data sets. Proposed system allows keyword search which is tolerant to the typographical errors both in the queries and the data sources[6]. A new scheme of searching queries over cloud to accommodate secure database management is proposed. Searching and indexing over the secured data is possible in the proposed system. The proposed method decreases the overhead of decryption to minimize the search time to an acceptable extent. Bloom Filter (BFAH) is used to provide the confidential code word. The obtained results show the fastness and effectiveness of the proposed system[7]. Proposed a novel method for friendly visual cryptography. Two meaningful shares are used to hide secret data. In every block of shares has the black-appearing ratio is same for secret pixel. Because of this property, hacking of secret image on each share is avoided, which increases the security level of proposed system. The contours of the cover image are hided on the stacked image by superimposing the shares[8]. In this paper, a system that contains Clouds and public auditing scheme which provides data integrity check by a Third Party Auditor (TPA) is proposed. The TPA is enabled to perform audits for multiple users simultaneously. Along with the alpha numeric passwords user allowed setting an image password which uses visual cryptography as its underlying mechanism. This effectively increases the security by reducing the risk password hacking. Proposed system provides an additional feature of de-duplication in order to avoid duplications of files stored at the main server. This saves the memory usage as well as the bandwidth[9]. Proposed model such that the client uses one secret and verification image is designed. Encoded shares are generated from these two images and encoded shares sends one secret share with one verification share to the clients. The received share is verified by each client and other client secret share retrieve the secret image. By using this technique hacking is avoided. The proposed method is applicable for both black and white and color images. Random number generator is used to divide an image into 'n' number of secret shares[10]. An idea about the previous researches and authentication scheme using hybrid crypto-steganography schemes. Remote authentication includes the submission of encrypted data along with visual and audio cues. A biometrics-based encryption technique is proposed for multiserver architecture using elliptical curve cryptography. The frequency part of the original image is modified to enable watermark technique with visual recognizable patterns and an original image divided into wavelet coefficients[11]. A Study on different methods providing secured database management with secured access to databases is explored. Both internal and security issues of various secure database management techniques are studied. The background of cryptography technique is studied. Internal security is achieved by different methods such as steganography, cryptography, visual cryptography, dynamic steganography, extended visual cryptography. In the proposed system two level securities is provided to content security and access security[12]. This paper proposed high level security method for encryption and decryption to achieve data security. In this proposed system two

levels of securities are used. In first level, data is encrypted and in second level hash value calculation. A weaving based technique is used in this proposed system. Elementary Number Theory Notation (ENTN) technique is used to weaving array generation. The proposed security system avoids information hacking and steeling. If the information is hacked and has committed any change, the hash value also changed[13]. Halftone images are processed by using a proposed novel technique to increases the accuracy of retrieved secret images. The drawbacks of conventional method such as pixel expansion and loss of contrast is overcome by using proposed method. In this paper, non-pixel expansion visual cryptography is explored[14]. A visual cryptographic technique for color images in which the generated shares are again encrypted. For this XOR operation is used and this will provide double security for the secret data. Thus secret shares are available in encrypted form to avoid any alternation by third party who tries to construct fake shares. The proposed scheme also uses the concept of half toning. But in proposed work when a color image is given as input, the retrieved image was color halftone image[15]. In proposed system; visual cryptography technique is used to provide database security on condition that authorization, Confidentiality, Authentication, Privacy and security are retained in VCS. In proposed model digital gray scale images is used for covering and secrete image, data confidentiality is achieved by using asymmetric cover image encryption to increase the contrast of the retrieved secret image and generate original image with good clarity. This property allows the user to select the proper features for various real time applications[16].

2. Proposed System

In proposed system, the database of the client is transformed using visual cryptograph and then encrypted and stored (for ex: in cloud server). The encryption is done based on the private key of the client. If user wants to search over encrypted data, then the query is also encrypted and searching is done on the encrypted data. In this proposed encryption method, each database is encrypted and stored into relational database. The encrypted document is sent to the client in encrypted form itself. Client decrypts data with their private key. All application related operations like checking for some threshold value, searching for similar records across different users, etc. is included.

2.1 Proposed System Architecture

The proposed system contains four major parts visual cryptography, encryption, decryption and searching and is shown in Figure 1.

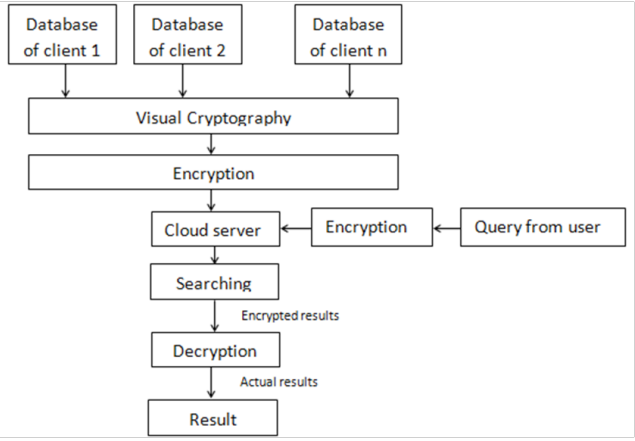


Figure 1. Block diagram of proposed system.

As shown in Figure 1 the proposed encryption allows server to search over the encrypted data. The query from the user also encrypted. The encryption is based on the attribute of database. If the data type of attribute is text, then it is encrypted into numerical value using Table 1. If the data type of attribute is numeric, then it is encrypted into text using Table 2.

Table 1. Text encryption into numerical value

Letter	Key	Letter	Key
A	1	N	14
B	2	O	15
C	3	P	16
D	4	Q	17
E	5	R	18
F	6	S	19
G	7	T	20
H	8	U	21
I	9	V	22
J	10	W	23
K	11	X	24
L	12	Y	25
M	13	Z	26

Table 2. Numerical encryption into text

Letter	Key
0	A
1	B
2	C
3	D
4	E
5	F
6	G
7	H
8	I
9	J

The flow chart of encryption (a sample medical record and student database) is shown in Figure 2.

3. Description of Different Blocks (Figure 2)

3.1 Visual cryptography

Initially, relational database is split into slices placed in matrix table, and then the slice positions are randomized. The randomization of slices is done using a zigzag rule applied initially row wise and then column wise. Table 3 and 4 shows the slicing process and randomization. The Pseudo code for visual cryptography is shown.

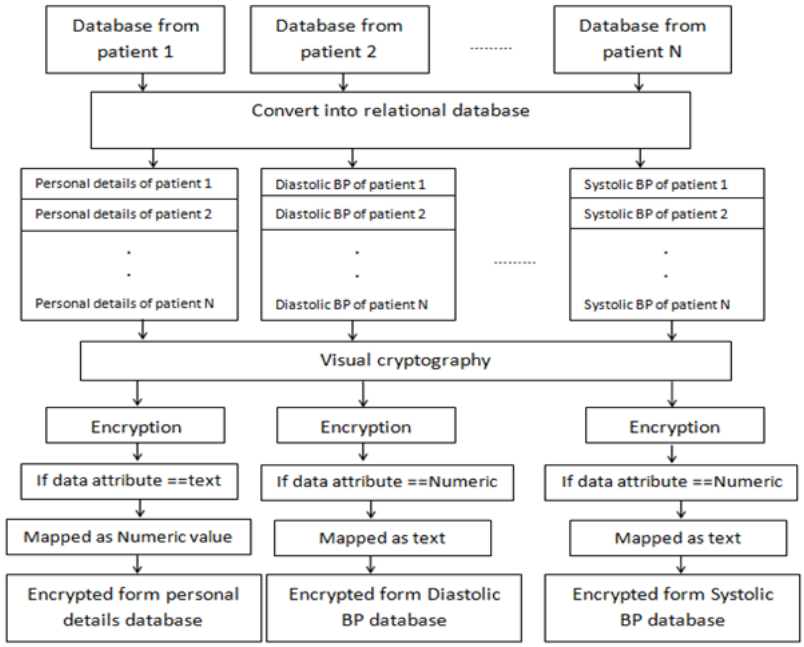


Figure 2. Flow chart of encryption.

Table 3. Relational database

Personal details	Description				Value			
Personal details$_1$	$Description_1^{(1)}\left(D_1^{(1)}\right)$	$\left(D_1^{(2)}\right)$	⋯	$\left(D_1^{(N)}\right)$	$Value_1^{(1)}\left(V_1^{(1)}\right)$	$\left(V_1^{(2)}\right)$	⋯	$\left(V_1^{(N)}\right)$
Personal details$_2$	$\left(D_2^{(1)}\right)$	$\left(D_2^{(2)}\right)$		$\left(D_2^{(N)}\right)$	$\left(V_2^{(1)}\right)$	$\left(V_2^{(2)}\right)$		$\left(V_2^{(N)}\right)$
. . .	. . .	. . .		.. . .	. . .	. . .		. . .
Personal details$_M$	$\left(D_M^{(1)}\right)$	$\left(D_M^{(2)}\right)$		$\left(D_M^{(N)}\right)$	$\left(V_M^{(1)}\right)$	$\left(V_M^{(2)}\right)$		$\left(V_M^{(N)}\right)$

Table 4. Slicing process

Personal details$_1$	$(D_1^{(1)})$	$(D_1^{(2)})$	$(D_1^{(3)})$	$(D_1^{(4)})$	$(V_1^{(1)})$	$(V_1^{(2)})$	$(V_1^{(3)})$	$(V_1^{(4)})$
Personal details$_2$	$(D_2^{(1)})$	$(D_2^{(2)})$	$(D_2^{(3)})$	$(D_2^{(4)})$	$(V_2^{(1)})$	$(V_2^{(2)})$	$(V_2^{(3)})$	$(V_2^{(4)})$
Personal details$_3$	$(D_3^{(1)})$	$(D_3^{(2)})$	$(D_3^{(3)})$	$(D_3^{(4)})$	$(V_3^{(1)})$	$(V_3^{(2)})$	$(V_3^{(3)})$	$(V_3^{(4)})$
Personal details$_4$	$(D_4^{(1)})$	$(D_4^{(2)})$	$(D_4^{(3)})$	$(D_4^{(4)})$	$(V_4^{(1)})$	$(V_4^{(2)})$	$(V_4^{(3)})$	$(V_4^{(4)})$

Table 5. Randomization process

$(V_4^{(3)})$	$(V_1^{(1)})$	$(D_4^{(3)})$	$(D_1^{(1)})$	Personal details$_4$	$(D_1^{(2)})$	$(D_4^{(4)})$	$(V_1^{(2)})$	$(V_4^{(4)})$
$(V_2^{(3)})$	$(V_2^{(1)})$	$(D_2^{(3)})$	$(D_1^{(1)})$	Personal details$_2$	$(D_2^{(2)})$	$(D_2^{(4)})$	$(V_2^{(2)})$	$(V_2^{(4)})$
$(V_1^{(3)})$	$(V_3^{(1)})$	$(D_1^{(3)})$	$(D_3^{(1)})$	Personal details$_1$	$(D_3^{(2)})$	$(D_1^{(4)})$	$(V_3^{(2)})$	$(V_1^{(4)})$
$(V_3^{(3)})$	$(V_4^{(1)})$	$(D_3^{(3)})$	$(D_4^{(1)})$	Personal details$_3$	$(D_4^{(2)})$	$(D_2^{(4)})$	$(V_4^{(2)})$	$(V_3^{(4)})$

3.2 Pseudo Code for Visual Cryptography

matrix=relational database
zigzag rule on row wise
zigzag rule on column wise

Consider size of data as four. Their relational database converted into slices is shown in Table 5.

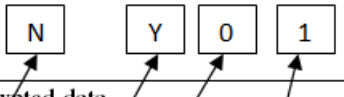
3.3 Encryption

The Pseudo code for encryption is shown below.

```
x=number of clients
----- Relational database-----
for i=0 to length(x)
    personal details [i] =”name” // personal details of client stored in string array
    Data1[i]=”value” // value of client stored in int array
    Data2[i]=”value”
    Data3[i]=”value”
    Data4[i]=”value”
    Data5[i]=”value”
------------------------------
loop: mapping encryption
for i=0 to length(data1)
data1[i] indexed to j=0
 for  length(data1[i])
    if(data1[i][j]==”0 or 1 or 2……9” ) or (data1[i][j]==”A or B or C……Z” )
    encryptdata1[i][j]=(”A or B or C……J”) or (”1 or 2 or 3……26”)
      end if
    end for
---------------------------
for every relational database
loop: mapping encryption
```

3.4 Illustration for Encryption

Case (i) Medical database
Database of patient 1



DATABASE	Encrypted data
Personal details (NITHYA)	14 9 20 8 25 1
Diastolic blood pressure (DBP):90	4 2 16:JA
Systolic blood pressure(SBP) :140	19 2 16:BEA
Body mass index(BMI):24	2 13 9:CE
2-Hour serum insulin (mu U/ml)(Insulin) :120	9 14 19 21 12 9 14:BCA
Triceps skin fold thickness(TSFT):22	20 19 6 20:CC

Database of patient 2

DATABASE	Encrypted data
Personal details (INIYA)	9 14 9 25 1
DBP :100	4 2 16:BAA
SBP :160	19 2 16 :BGA
BMI :30	2 13 9 :DA
Insulin :210	9 14 19 21 12 9 14:CBA
TSFT :42	20 19 6 20:EC

Case (ii) Student database
Database of student 1

DATABASE	Encrypted data
Personal details (DHANAM)	4 8 1 14 1 13
Physics:81	16 8 25 19 9 3 19:IB
Chemistry:75	3 8 5 13 9 19 20 18 25:HF
Tamil:88	20 1 13 9 12:II
English:78	5 14 7 12 9 19 8:HI
Maths:76	13 1 20 8 19:HG

Database of student 2

DATABASE	Encrypted data
Personal details (MONISHA)	13 15 14 9 19 8 1
Physics:30	16 8 25 19 9 3 19:DA
Chemistry:45	3 8 5 13 9 19 20 18 25:EF
Tamil:60	20 1 13 9 12:GA
English:55	5 14 7 12 9 19 8:FF
Maths:35	13 1 20 8 19:DF

3.5 Searching

When the client wants to search on server, first the query is encrypted and then sent for search. The search over encrypted database retrieves answers for the queries rather than any information about the presence (or absence) of the query keywords in each database. The answers for the query are in encrypted form. Because of this any leakage of information over retrieved set of documents is avoided. Existing searching algorithm requires $O(n)$ comparisons (searching operations) at the server to evaluate if the database contains a chosen keyword. The flow chart for searching is given in Figure 3.

3.6 Query Types

- Query for details of particular user
- Query attribute is text, then it will encrypt into numeric value. The encrypted query is sent to the server for searching
- Queries include equalities of some threshold value (=) from database.

  Query attribute is numeric, then it will encrypt into text. The encrypted query is sent to the server for searching.
- Queries include multiple record matching

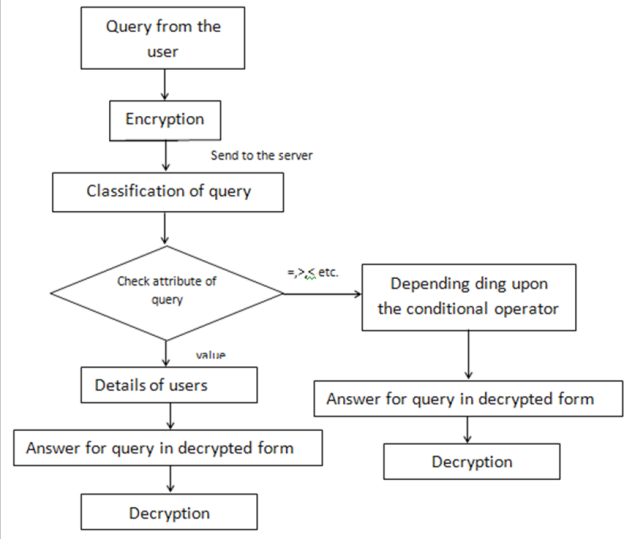


Figure 3. Flow chart for searching.

The pseudo code for searching is shown in below.

```
y=number of query from client
for length (y)
Switch (query)
case1:(query==details of patient(name))
 encryptname=encrypt(name)
 for i=0 length(encryptnamearray)
   if(encryptname==encryptnamearray[i])
return data1[i], data2[i], data3[i], data4[i] and data5[i]
   end if
 end for
case2:(query with any thresholdvalue)
 encrypt(subjectname)
 encryptsubjectname=encryptsubjectname[]
 for length(encryptsubjectname)
  if (encryptsubjectname[i]>=thresholdvalue or encrypts
ubjectname[i]=thresholdvalue or   encryptsubjectname[
i]<thresholdvalue or encryptsubjectname[i]<=thresholdv
alueor encryptsubjectname[i]<thresholdvalue)
  return decrypt(encryptname[i])
  end if
 end for
```

3.7 Decryption

The decryption algorithm takes encrypted data as input and the private key of the client and is decrypted using

Tables 6 and 7. If answer contains numerical value (alphabet), it decrypted into alphabet (numerical). The flowchart of decryption is shown in Figure 4.

Table 6. Decryption

Letter	Key	Letter	Key
1	A	14	N
2	B	15	O
3	C	16	P
4	D	17	Q
5	E	18	R
6	F	19	S
7	G	20	T
8	H	21	U
9	I	22	V
10	J	23	W
11	K	24	X
12	L	25	Y
13	M	26	Z

Table 7. Decryption

Letter	Key
A	0
B	1
C	2
D	3
E	4
F	5
G	6
H	7
I	8
J	9

The pseudo code for decryption is shown in below

---

loop: mapping decryption
for j=0 to length(encryptname[i])
if(encryptname[i][j]==”1 or 2 or C……26”) or (”A or B or C……J”)
decryptname[i][j]=(”A or B or 3……Z”) or (”0 or 1 or 2……9”
end if
end for

---

decryption on visual cryptography
reverse zigzag rule on column wise
reverse zigzag rule on row wise

---

for every relational database
return result

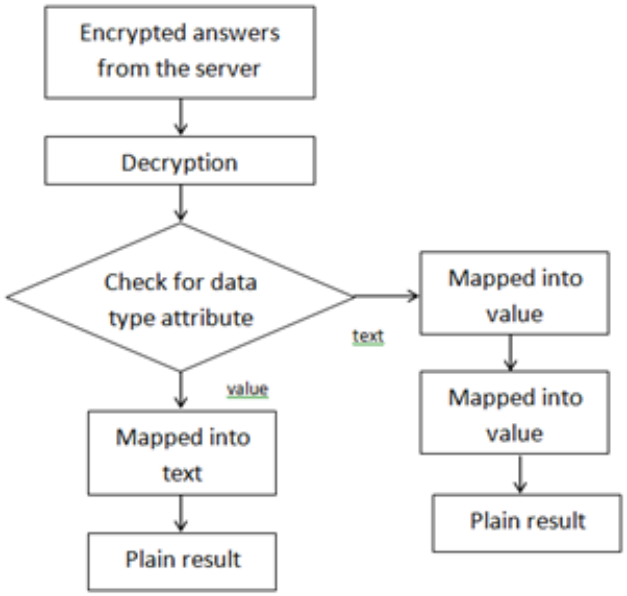


Figure 4. Flow chart for decryption.

3.8 Illustration for Decryption

Case (i) Medical database

Example 1		Example 2	
Encrypted data	**Decrypted data**	**Encrypted data**	**Decrypted data**
14 9 20 8 25 1	Personal details (denotes name)	9 14 9 25 1	Personal details (denote name)
4 2 16:JA	DBP:90	4 2 16:BAA	DBP :100
19 2 16:BEA	SBP :140	19 2 16 :BGA	SBP :160
2 13 9:CE	BMI:24	2 13 9 :DA	BMI :30
9 14 19 21 12 9 14:BCA	2-Hour serum insulin (mu U/ml) (Insulin) :120	9 14 19 21 12 9 14:CBA	2-Hour serum insulin (mu U/ml):210
20 19 6 20:CC	TSFT:22	20 19 6 20:EC	TSFT :42

Case (ii) Student database

Example 1		Example 2	
Encrypted data	**Decrypted data**	**Encrypted data**	**Decrypted data**
4 8 1 14 1 13	Personal details (denotes name)	13 15 14 9 19 8 1	Personal details (denote name)
16 8 25 19 9 3 19:IB	Physics:81	16 8 25 19 9 3 19:DA	Physics:30
3 8 5 13 9 19 20 18 25:HF	Chemistry:75	3 8 5 13 9 19 20 18 25:EF	Chemistry:45
20 1 13 9 12:II	Tamil:88	20 1 13 9 12:GA	Tamil:60
5 14 7 12 9 19 8:HI	English:78	5 14 7 12 9 19 8:FF	English:55
13 1 20 8 19:HG	Maths:76	13 1 20 8 19:DF	Maths:35

4. Advantages of Search on Encrypted Data

The communication overhead minimized between the user and server. The computation is minimized between server and user. It allows the multi-user to search over the encrypted data. Searching time is minimized by relational database management. From encrypted query server cannot, distinguish between documents, determine document contents, check for search keyword and extend beyond decrypted result.

4.1 Avoiding Dictionary Attack

A dictionary attack is a method used to crack the server security enabled with password-protection. A dictionary attack tries to crack an authentication mechanism by randomly use each word in a dictionary as a password or trying to identify the decryption key of an encrypted data or database. This attack is avoided by private key and search over the encrypted data. Since server cannot generate the encrypted query to search, the system is protected from dictionary attacks.

5. Implementation

The encryption scheme according to table 1 and table 2 is implemented in Java language and the result shown below for the sample input provided. Searching process is performed and the corresponding output is displayed below

Query

Case (i) Medical database
Input

- Details of patient2
- DBP>35
- BMI>50

Processed output

- Details of patient2

  DBP 38
  SBP 53
  BMI 29
  DPF 45
  TSFT 78

- DBP>35
  Patient 2

- BMI>50
  Patient 1

Case (ii) Student database
Input

- Details of student1
- English<=55
- Maths >=35

Processed output

- Details of student1
  Physics 81
  Chemistry 75
  Tamil 88
  English 78
  Maths 76
- English <=55
  Student 2

- Maths >= 35
  Student 1 and Student 2.

6. Conclusion

The proposed algorithm for encryption with private key achieves confidentiality of medical and student data. In this paper, secured encryption with secured search scheme on cloud server is proposed. By this proposed algorithm search time is reduced by relational database management. Dictionary attack is prevented by search algorithm. The search is processed over the encrypted data. The encryption and decryption process is done by the client private key. The secured medical database management on clod server and secured searching is implemented. By this proposed algorithm, the server only knows about the encrypted data and not the original data of the client.

7. References

1. Seng WK, Kim MH, Besar R, Salleh F. A secure model for medical data sharing. International Journal of Database Theory and Application. 2005.
2. Kurle AS, Patil KR. Survey on privacy preserving mobile health monitoring system using cloud computing. International Journal of Electrical, Electronics and Computer Systems (IJEECS). 2015; 3(4):2347–820.
3. Akinyele JA, Pagano MW, Green MD, Lehmann CU, Peterson ZNJ, Rubin AD. Securing electronic medical records using attribute-based encryption on mobile devices. SPSM '11 Proceedings of the 1st ACM Workshop on Security and Privacy in Smartphones and Mobile Devices; 2011. p. 75–86.
4. Lokhande AR, Jamgekar RS, Takalikar RA. Improving privacy in healthcare service by using cloud assisted technologies. International Journal of Computer Science and Information Technologies. 2015; 6(5):4605–10.
5. PhuongTVX, Yang G, Susilo W. Hidden ciphertext policy attribute-based encryption under standard assumptions. IEEE Transactions on Information Forensics and Security. 2016 Jan; 11(1).
6. Kuzu M, Islam MS, Kantarcioglu M. Efficient similarity search over encrypted data [Internet]. 2012. Available from: ieeexplore.ieee.org.
7. Khan MS, Wang C, Kulsoom A, Ullah Z. Searching encrypted data on cloud. International Journal of Computer Science. 2013 Nov; 10(6), No 1.
8. Hou Y-C, Quan Z-Y, Liao H-Y. New designs for friendly visual cryptography scheme. International Journal of Information and Electronics Engineering. 2015 Jan; 5(1).
9. Pawar A, Popli SK, Rawat P, Salke P. Security in banking sector using cloud computing with TPA. International Education and Research Journal. 2016 Jan; 2(1).
10. Rao RY. Secure visual cryptography. International Journal of Engineering and Computer Science. 2013 Jan; 2(1);265–303.
11. Chougule SM, Mahadik SR. Secure remote authentication using biometric data with steganography for wireless network. International Journal of Innovation in Engineering, Research and Technology. 2013 Apr; 2(4).
12. Asole SS, Mundada SM. A survey on securing databases from unauthorized users. International Journal of Scientific and Technology Research. 2013 Apr; 2(4).
13. Raja AY, Perumal SA. WSES: High secured data encryption and authentication using weaving, rotation and flipping. ICTACT Journal on Communication Technology. 2015 Dec; 6(4).
14. Menon KN, Kuriakose M. A novel visual cryptographic scheme using Floyd Steinberg halftoning and block replacement algorithms. International Journal of Advanced Research in Biology, Ecology, Science and Technology. 2015 Apr; 1(1).
15. Bhadran RA. An improved visual cryptography scheme for colour images. International Research Journal of Engineering and Technology. 2015 Aug; 2(5).
16. Yelane RD, Mhala NN, Chilke BJ. Security approach by using visual cryptographic technique. International Journal of Advanced Research in Computer Science and Software Engineering. 2015 Jan; 5(1).