Vol 3 Issue 11 May 2014 ISSN No :2231-5063

International Multidisciplinary Research Journal

Golden Research Thoughts

Chief Editor
Dr.Tukaram Narayan Shinde

Publisher
Mrs.Laxmi Ashok Yakkaldevi

Associate Editor
Dr.Rajani Dalvi

Honorary
Mr.Ashok Yakkaldevi

Welcome to GRT

RNI MAHMUL/2011/38595 **ISSN No.2231-5063**

Golden Research Thoughts Journal is a multidisciplinary research journal, published monthly in English, Hindi & Marathi Language. All research papers submitted to the journal will be double - blind peer reviewed referred by members of the editorial board.Readers will include investigator in universities, research institutes government and industry with research interest in the general subjects.

International Advisory Board

Flávio de São Pedro Filho
Federal University of Rondonia, Brazil

Kamani Perera
Regional Center For Strategic Studies, Sri Lanka

Janaki Sinnasamy
Librarian, University of Malaya

Romona Mihaila
Spiru Haret University, Romania

Delia Serbescu
Spiru Haret University, Bucharest, Romania

Anurag Misra
DBS College, Kanpur

Titus PopPhD, Partium Christian University, Oradea,Romania

Mohammad Hailat
Dept. of Mathematical Sciences, University of South Carolina Aiken

Abdullah Sabbagh
Engineering Studies, Sydney

Catalina Neculai
University of Coventry, UK

Ecaterina Patrascu
Spiru Haret University, Bucharest

Loredana Bosca
Spiru Haret University, Romania

Fabricio Moraes de Almeida
Federal University of Rondonia, Brazil

George - Calin SERITAN
Faculty of Philosophy and Socio-Political Sciences Al. I. Cuza University, Iasi

Hasan Baktir
English Language and Literature Department, Kayseri

Ghayoor Abbas Chotana
Dept of Chemistry, Lahore University of Management Sciences[PK]

Anna Maria Constantinovici
AL. I. Cuza University, Romania

Horia Patrascu
Spiru Haret University, Bucharest,Romania

Ilie Pintea,
Spiru Haret University, Romania

Xiaohua Yang
PhD, USA

.....More

Editorial Board

Pratap Vyamktrao Naikwade
ASP College Devrukh,Ratnagiri,MS India

R. R. Patil
Head Geology Department Solapur University,Solapur

Rama Bhosale
Prin. and Jt. Director Higher Education, Panvel

Salve R. N.
Department of Sociology, Shivaji University,Kolhapur

Govind P. Shinde
Bharati Vidyapeeth School of Distance Education Center, Navi Mumbai

Chakane Sanjay Dnyaneshwar
Arts, Science & Commerce College, Indapur, Pune

Awadhesh Kumar Shirotriya
Secretary,Play India Play,Meerut(U.P.)

Iresh Swami
Ex - VC. Solapur University, Solapur

N.S. Dhaygude
Ex. Prin. Dayanand College, Solapur

Narendra Kadu
Jt. Director Higher Education, Pune

K. M. Bhandarkar
Praful Patel College of Education, Gondia

Sonal Singh
Vikram University, Ujjain

G. P. Patankar
S. D. M. Degree College, Honavar, Karnataka

Maj. S. Bakhtiar Choudhary
Director,Hyderabad AP India.

S.Parvathi Devi
Ph.D.-University of Allahabad

Sonal Singh,
Vikram University, Ujjain

Rajendra Shendge
Director, B.C.U.D. Solapur University, Solapur

R. R. Yalikar
Director Managment Institute, Solapur

Umesh Rajderkar
Head Humanities & Social Science YCMOU,Nashik

S. R. Pandya
Head Education Dept. Mumbai University, Mumbai

Alka Darshan Shrivastava
Shaskiya Snatkottar Mahavidyalaya, Dhar

Rahul Shriram Sudke
Devi Ahilya Vishwavidyalaya, Indore

S.KANNAN
Annamalai University,TN

Satish Kumar Kalhotra
Maulana Azad National Urdu University

Address:-Ashok Yakkaldevi 258/34, Raviwar Peth, Solapur - 413 005 Maharashtra, India
Cell : 9595 359 435, Ph No: 02172372010 Email: ayisrj@yahoo.in Website: www.aygrt.isrj.net

Golden Research Thoughts
ISSN 2231-5063
Impact Factor : 2.2052(UIF)
Volume-3 | Issue-11 | May-2014
Available online at www.aygrt.isrj.net

DATABASE SECURITY USING HOMOMORPHIC ENCRYPTION

Sagar Choudhary , Sandeep Giri and Chunchun Singh

Abstract:-Cloud computing technique emerges an captivating solution to store and process confidential data. However, several security risks are encountered with such a system as the securely encrypted data should be decrypted before processing them.With the emergence of cloud computing organizations can store data in the cloud provider's data centre, but the security of the data in the cloud is a major concern. Data can be stored in the cloud in an encrypted format, but the problem is that while data can be sent to and from a cloud provider's data centre in encrypted form, the servers that power a cloud can't do any work on it that way. With homomorphic encryption, a company could encrypt its entire database and upload it to a cloud and it is possible to analyse data without decrypting it. In this paper we present a relational database system based on homomorphic encryption schemes to preserve the integrity and confidentiality of the data. Our system executes SQL queries over encrypted data. We tested our system with a recently developed homomorphic scheme that enables the execution of arithmetic operations on ciphertexts. With homomorphic encryption, a company could encrypt its entire database and upload it to a cloud and it is possible to analyse data without decrypting it.

Keywords: Database Security , Homomorphic Encryption , organizations.

INTRODUCTION :-

Cloud computing uses the concept of multi-tenancy where there is one application and many users can customize and use this application along with the custom build applications. Upgrades and maintenance is taken care by the cloud service provider. While yesterday's business applications required thousands, if not millions, of dollars and sometimes years of professional services help to set up and customize, the technologies offered by the Internet today make it much easier to create, configure, and use business applications of all kinds. Indeed, the power of the Internet has given us the ability to solve new kinds of business problems that, because of complexity or cost, had previously remained out of reach. Cloud Computing is an Internet-based technology. The increasing network bandwidth and reliable yet flexible network connections in the recent past makes it possible for users to use the power of cloud computing in order to subscribe to services and to utilize the cloud environment to store data.In theory, the data can be encrypted by the client, and then sent to the cloud's provider for storage or processing. Only the client holds the decryption keys necessary to read the data. Despite the fact that this type of processing may increase the amount of computing time, the benefits associated with it are worth the processing overhead. Indeed, this model of computing can preserve the confidentiality and integrity of the data while delegating the storage and processing to an un-trusted third party. In this paper, we present a novel technique to execute SQL statements over encrypted data. We develop a secure database system that processes these queries. The parameters of SQL queries are encrypted by the client and sent to the server for processing. The latter performs the requested operation over an encrypted database and returns an encrypted result to the client. The advantage of this system is that the database server knows neither the content nor the position of the records affected by the query.

The remainder of this paper is organized as follows. In Section II, we review the literature for the work related to private information retrieval (PIR) approaches. Section III provides a formal description of our secured SQL statements approach. Section IV presents a homomorphic cryptosystem that we use to build a prototype system. Section V presents an implementation of a secure relational database system. In Section VI we provide performance analysis of the proposed secure database system. Finally, Section VII concludes our work and provides future research directions.

PRIVATE INFORMATION RETRIEVAL

Alice wants to query a database but she does not want the database to learn what she is querying. She can ask for the entire database. Can she get her query answered with less communication? One model of this problem is Private Information Retrieval , henceforth PIR. We obtained some knowledge that the PIR model including partial answers to the following questions. (1) What if there are k non-communicating copies of the database but they are computationally unbounded? (2) What if there is only one copy of the database and it is computationally bounded?

Among the most important criteria in PIR protocol are the communication cost and the amount of data sent back to the querier. The trivial solution of the PIR protocol is to send back the entire database to the client. However, this solution is expensive, even for a simple request that results in retrieving two matching records. Other approaches proposed to retrieve only the requested data, by using replicated databases that are stored at multiple servers. In this case, the request is forwarded to all servers. With this approach, although we deal with multiple replicated databases, the privacy is better protected. . The authors pointed out that the adoption of such technology is still below ambition. Some users are still concerned about the security of these clouds. Even those who started using the technology, they only utilize it with their less sensitive data. The limited usage of cloud computing is mainly due to the lack of control over the communicated data. The authors highlight that people require explicit guarantees that their data will be protected under well-defined policies and mechanisms. However, no technical security solutions were proposed to back-up their information centric model where data can self defend itself in a hostile or an un-trusted environment.

The private information retrieval (PIR) approach, introduced by Chor et al. in [9], achieves the retrieval of an ith bit in a block without revealing information about the bit retrieved or about the request for the bit itself. This approach has been widely used as a basis for several tools, and has supported various distributed applications. However, the approach requires more improvements and the work with it is still in progress, both at the security of the communication channel level and the hidden client identity level.

Raykova et al. [10] extended the PIR approach by proposing a secure anonymous search system. The system employs keyword search such that only authorized clients have access to their blocks. This system is capable of mapping the database content to the appropriate client, thus guaranteeing the privacy of the data and the query. The ultimate target of Raykova's system is to ignore the identity of the client while protecting the database from malicious queriers.

Shang et al. [11] tackled the problem of protecting the database itself. The problem is studied through monitoring the amount of data disclosed by a PIR protocol during a single run. The information attained from the monitoring process is used to understand how a malicious querier can conduct attacks to retrieve excessive amount of data from the server.

PIR has also been used to develop authentication systems. Nakamura et al. [12] constructed a system with three components, a querier that initiates requests, an authentication-server that processes these requests, and a database that returns the appropriate data in response to the request. This system ensures the security of data and the anonymous communication between the querier and the database. Yinan and Cao [13] used the PIR approach to propose a system that controls the access to the database. According to this system, the privacy of data is enforced by enabling each authorizer to give or deny access to his/her own data with a hierarchical authorization access right scheme.

Among the most important criteria in PIR protocol are the communication cost and the amount of data sent back to the querier. The trivial solution of the PIR protocol is to send back the entire database to the client. However, this solution is expensive, even for a simple request that results in retrieving two matching records. Other approaches proposed to retrieve only the requested data, by using replicated databases that are stored at multiple servers. In this case, the request is forwarded to all servers. With this approach, although we deal with multiple replicated databases, the privacy is better protected. However, this approach is still complicated and may result in extended processing and communication times. Gentry et al. [14] proposed a scheme to retrieve a bit or a block from a database with a constant communication rate. Melchor et al. [15] proposed a scheme that reaches the available data with a reasonable communication cost while achieving lower computational cost compared to other PIR protocols.

SECURED SQL OPERATION

In this section we review some basic security concepts which are important for un-derstanding this chapter. We also de ne some technical terms which will be used throughout this chapter. Whenever we use a technical term for the rst time we will italicize it, to draw attention to its de nition which is given at that point.

Secrecy, Integrity and Availability

The objective of data security can be divided into three separate, but interrelated, areas as follows.

Secrecy is concerned with improper disclosure of information. The terms con - dentiality or non-disclosure are synonyms for secrecy. Integrity is concerned with improper modi cation of information or processes. Availability is concerned with improper denial of access to information. The term denial of service is also used as a synonym for availability.

These three objectives arise in practically every information system. For example, in a payroll system secrecy is

concerned with preventing an employee from nding out the boss's salary; integrity is concerned with preventing an employee from changing his or her salary; and availability is concerned with ensuring that the paychecks are printed on time as required by law. Similarly, in a military command and control system secrecy is concerned with preventing the enemy from determining the target coordinates of a missile; integrity is concerned with preventing the enemy from alter-ing the target coordinates; and availability is concerned with ensuring that the missile does get launched when the order is given.

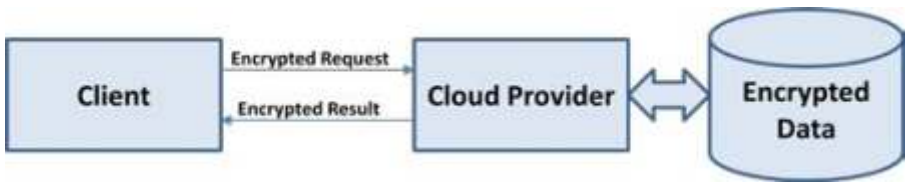
Data Dependent Access Control

Database access controls are often data dependent. For example, some users may be limited to seeing salaries which are less than $30,000. Similarly, a manager may be restricted to seeing salaries for employees in his department. We now discuss two basic techniques, viz., view-based access controls and query modi cation, for implementing data-dependent access controls in relational databases.

View Based Access Control

A base relation is a real" relation in the database, that is it is actually stored in the Database. A view is a virtual" relation which is derived from base relations and other views. The database stores the view de nitions and materializes the view as needed. To illustrate the concept of a view, and its security application, consider the EMPLOYEE relation of Table 1. (The value NULL indicates that Harding has no manager.) The following SQL statement de nes a view called TOY-DEPT.

we develop a secure database system that processes SQL queries over encrypted data. As shown in Figure 1, parameters of the queries are encrypted by the client and sent to the server for processing. The latter performs the requested operation and returns encrypted results to the client.



We describe below the circuit of a simple SQL SELECT query:
SELECT * from T where c=v

where the value v is in encrypted form. The trivial solution to securely perform this statement is to send back to the client the entire database, but this solution suffers from complexity and scalability issues. Instead, we propose a methodology to implement the SELECT circuit at the server side, while preserving the confidentiality and the privacy of the request.

HOMOMORPHIC ENCRYPTION SCHEME

In this Section, we describe some classical homomorphic encryption systems which have created substantial interest among the researchers in the domain of cryptography. We start with the first probabilistic systems proposed by Goldwasser and Micali in 1982 (Goldwasser & Micali, 1982; Goldwasser & Micali, 1984) and then discuss the famous Paillier's encryption scheme (Paillier, 1999) and its improvements. Paillier's scheme and its variants are well-known for their efficiency and the high level of security that they provide for homomorphic encryption. We do not discuss their mathematical considerations in detail, but summarize their important parameters and properties.

Goldwasser-Micali scheme: This scheme (Goldwasser & Micali, 1982; Goldwasser & Micali, 1984) is historically very important since many of subsequent proposals on homomorphic encryption were largely motivated by its approach. Like in RSA, in this scheme, we use computations modulo n = p.q, a product of two large primes. The encryption process is simple which uses a product and a square, whereas decryption is heavier and involves exponentiation. The complexity of the decryption process is: b _9 H ?_'_, where H ?_ denotes the number of bits in p. Unfortunately, this scheme has a limitation since its input consist of a single bit. First, this implies that encrypting k bits leads to a cost of b _9 H ?_ '_. This is not very efficient even if it may be considered as practical. The second concern is related to the issue of expansion – a single bit of plaintext is encrypted in an integer modulo n, that is, H E _ bits. This leads to a huge blow up of ciphertext causing a serious problem with this scheme.

Goldwasser-Micali (GM) scheme can be viewed from another perspective. When looked from this angle, the basic principle of this scheme is to partition a well-chosen subset of integers modulo n into two secret parts: F^ and F&. The encryption process selects a random element Fc to encrypt plaintext b, and the decryption process lets the user know in which part the randomly selected element lies. The essence of the scheme lies in the mechanism to determine the subset, and to partition it into F^ and F&. The scheme uses group theory to achieve this goal. The subset is the group G of invertible integers

modulo n with a Jacobi symbol with respect to n, equal to 1. The partition is generated by another group d e f, consisting of the elements that are invertible modulo n with a Jacobi symbol, with respect to a fixed factor n, equal to 1. With these settings of parameters, it is possible to split G into two parts – H and G\H. The generalization schemes of GM deal with these two groups. These schemes attempt to find two groups G and H such that G can be split into more than k = 2 parts.

decryption phase is more complex. If the input and output sizes are H __ and H E_ bits respectively, the expansion is equal to H E_7H __. The value of expansion obtained in this

approach is less than that achieved in GM. This makes the scheme more attractive. Moreover, the encryption is not too expensive as well. The overhead in the decryption process is estimated to be b i_9 H ___ for pre-computation which remains constant for each dynamic decryption step. This implies that the value of k has to be taken very small, which in turn limits the gain obtained on the value of expansion.

NAME	DEPT	SALARY	MANAGER
Smith	Toy	10,000	Jones
Jones	Toy	15,000	Baker
Baker	Admin	40,000	Harding
Adams	Candy	20,000	Harding
Harding	Admin	50,000	NULL

NAME	SALARY	MANAGER
Smith	10,000	Jones
Jones	15,000	Baker

REFER TO REFERENCE NO. [8]

Table 2: View TOY-DEPT

```
CREATE  VIEW TOY-DEPT
        SELEC   NAME, SALARY,
AS      T       MANAGER
        FROM    EMPLOYEE
        WHERE   DEPT = `Toy'
```

REFER TO REFERENCE NO. [8]

This de nes the virtual relation shown in Table 2. A user who has read access to TOY-DEPT is thereby limited to retrieving information about employees in the Toy Department. To illustrate the dynamic aspect of views suppose that a new employee Brown is inserted in base relation EMPLOYEE, as shown in Table 3. The view TOY-DEPT will be automatically modi ed to include Brown, as shown in Table 4.

Views can also be used to provide access to statistical information. For example, the following view gives the average salary for each department.

```
CREAT
E       VIEW AVSAL(DEPT, AVG)
                DEPT,
AS      SELECT  AVG(SALARY)
        FROM    EMPLOYEE
        GROUP
        BY      DEPT
```

REFER TO REFERENCE NO. [8]

For retrieval purposes users need not distinguish between views and base relations. A view is simply another relation in the database, which happens to be automatically modi ed by the DBMS whenever its another relation in the database,

base relations are modi ed. Views, therefore, provide a very powerful mechanism for specifying data-dependent

authorization for data retrieval. There are, however, significant problems if views are modified by users directly (rather than by side effect of modifying base relations). This is due to our theoretical inability, in general, to translate updates on views into updates of base. We see the further details in the table which is shown homomorphic encryption scheme

NAME	DEPT	SALARY	MANAGER
Smith	Toy	10,000	Jones
Jones	Toy	15,000	Baker
Baker	Admin	40,000	Harding
Adams	Candy	20,000	Harding
Harding	Admin	50,000	NULL
Brown	Toy	22,000	Harding

Table 3: Modi ed Base Relation EMPLOYEE

REFER TO REFERENCE NO. [8]

NAME	SALARY	MANAGER
Smith	10,000	Jones
Jones	15,000	Baker
Brown	22,000	Harding

Table no. 4 : Automatically Modi ed View TOY-DEPT

REFER TO REFERECE NO. [8]

Relations.This limits the usefulness of views for data dependent authorization of update operations.

IMPLEMENTATION

In our implementation, we aim at proving that it is possible to perform SQL queries over an encrypted database. For example, the user can specify a search criterion through a database. Then, the client software encrypts the parameters of the query, corresponding to the search criterion, and sends it to the appropriate server. The server retrieves the requested record (blind processing) from the database and returns it to the client. The client software decrypts the record and displays it to the user.

We built a simple medical application containing 10 patients' records. In Figure 3, we show the result of the SELECT query. This is how the result appears in a screenshot of the client side of our built application.



The application supports the following SQL operations:

SELECT with wildcard characters (*, ?) and relational operators (< >).
UPDATE with wildcard characters (*, ?) and relational operators (< >).
DELETE with wildcard characters (*, ?) and relational operators (< >).
Statistical operations like COUNT and AVG.

It is worth mentioning that the implementation of the medical application was built using a simplified and non-secure version of the somewhat homomorphic scheme. This is due to performance issues as it is impractical to perform our tests using the fully homomorphic cryptosystem. We chose the security parameters in such a way to support all the SQL operations with no need to employ the bootstrapping technique. We discuss the performance of our system in the next section.

CONCLUSION AND FUTURE DIRECTION

The concept of processing encrypted data is promising to revolutionize traditional computing. Indeed, this concept has many direct applications in cloud computing environments, banking, electronic voting and many other applications.

In this paper we developed the first secure database system based on a fully homomorphic encryption scheme. We presented the circuits to implement SQL statements over encrypted data. We built a prototype of a database system where data is stored and processed in encrypted form. The database server can execute most of the SQL statements in a blind fashion, that is, it returns the results without any knowledge of the content or the position of the records extracted/affected. We conducted performance analysis to measure the time needed to execute a simple query on the database. We found that the current technology is not sufficiently mature yet as it is time-consuming. Indeed, the encryption schemes proposed by Gentry et al. in [5][6][7] are very impractical. According to our measurements, the time needed to perform simple calculations is substantial. We believe that there still is a great opportunity for researchers to develop more efficient homomorphic encryption schemes.

As future work, we are planning to work on the optimization of the efficiency of the system. Processing can be parallelized in order to take advantage of multiple processors executing the encrypted requests. We will also investigate how to reduce the number of recryptions needed. Indeed, since the noise UPDATE, etc.). If we can encrypt the SQL circuits, the system will preserve the confidentiality of the data and operations performed on these data. We believe that this new system can be the foundation of a highly secure cloud computing environment.

REFERENCES

1.Implementing Gentry's Fully-Homomorphic Encryption Scheme Preliminary Report
2.Homomorphic encryption Technique-(ElGamal, Goldwasser & Micali, Blum & Goldwasser and Lance Fortnow Report.
3.Data Networking and Security by Forozoun
4.Database Security by Alfred Basta
5.Implementing database security and Auditing by Ron Ben Natan
6.Homomorphic encryption theory and application by Jaydip sen
7.A fully homomorphic encryption Scheme by Craig Gentry Stanford university Cse department
8.Data and Database Security and controls BY RAVI S. SANDHU AND SUSHIL JAJODIA
9.Implementing Gentry's Fully-Homomorphic Encryption Scheme By Craig gentry AND Shai Halevi A survey on private information retrieval by William gasarch
10.C. Gentry. A fully homomorphic encryption scheme. PhD thesis, Stanford University, 2009.
http://crypto.stanford.edu/craig.
11.C. Gentry. Fully homomorphic encryption using ideal lattices. In STOC '09, pages 169{178. ACM, 2009.
12.C. Gentry. Toward basing fully homomorphic encryption on worst-case hardness. In Advances in Cryptology - CRYPTO'10, volume 6223 of Lecture Notes in Computer Science, pages {. Springer, 2010.
13.C. Gentry and S. Halevi. Public Challenges for Fully-Homomorphic Encryption. TBA, 2010.
14.The GNU Multiple Precision Arithmetic Library. http://gmplib.org/, Version 5.0.1, 2010.
15.O. Goldreich, S. Goldwasser, and S. Halevi. Public-key cryptosystems from lattice reduction problems. In Advances in Cryptology - CRYPTO'97, volume 1294 of Lecture Notes in Computer Science, pages 112{131. Springer, 1997.
16.V. Lyubashevsky, C. Peikert, and O. Regev. On ideal lattices and learning with errors over rings. In Advances in Cryptology - EUROCRYPT'10, volume 6110 of Lecture Notes in Com-puter Science, pages 1{23. Springer, 2010.
17.D. Micciancio. Improving lattice based cryptosystems using the hermite normal form. In CaLC'01, volume 2146 of Lecture Notes in Computer Science, pages 126{145. Springer, 2001.
18.M. S. Paterson and L. J. Stockmeyer. On the number of nonscalar multiplications necessary to evaluate polynomials. SIAM Journal on Computing, 2(1):60{66, 1973.
19.C. Peikert and A. Rosen. Lattices that admit logarithmic worst-case to average-case connec-tion factors. In Proceedings of the 39th Annual ACM Symposium on Theory of Computing { STOC'07, pages 478{487. ACM, 2007.

Publish Research Article
International Level Multidisciplinary Research Journal
For All Subjects

Dear Sir/Mam,

We invite unpublished Research Paper,Summary of Research Project,Theses,Books and Book Review for publication,you will be pleased to know that our journals are

Associated and Indexed,India

- International Scientific Journal Consortium
- OPEN J-GATE

Associated and Indexed,USA

- EBSCO
- Index Copernicus
- Publication Index
- Academic Journal Database
- Contemporary Research Index
- Academic Paper Databse
- Digital Journals Database
- Current Index to Scholarly Journals
- Elite Scientific Journal Archive
- Directory Of Academic Resources
- Scholar Journal Index
- Recent Science Index
- Scientific Resources Database
- Directory Of Research Journal Indexing

Golden Research Thoughts
258/34 Raviwar Peth Solapur-413005,Maharashtra
Contact-9595359435
E-Mail-ayisrj@yahoo.in/ayisrj2011@gmail.com
Website : www.aygrt.isrj.net