ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 7, July 2013

Privacy Preserving Updates to Anonymous and Confidential Database (Secure Computing)

B.Srinivasulu[1], B.V.Usha[2], R.V.Gandhi[3],K.Ramakrishna[4]

Abstract: The main theme of Secure Computing is to provide Data Security which can be well explained by a simple example. Suppose "X" owns a k-anonymous database and needs to determine whether "X" database, when inserted with a tuple owned by "Y", is still k-anonymous. Clearly, allowing "X" to directly read the contents of the tuple breaks the privacy of "Y". (e.g., a patient's medical record); In this place, "Y" not get the privacy of own information because the information of "Y" can be accessed by "X" without the prior knowledge of "Y". On the other hand, the confidentiality of the database managed by "X" is violated once "Y" has access to the contents of database. Thus, the problem is to check whether the database inserted with the tuple is still k-anonymous, without letting "X" and "Y" knows the contents of the tuple and database respectively. Here, we implement Homomorphism Cryptographic Algorithm to serve the purpose.

Keywords: Generalization and suppression techniques, Anonymous and Confidential Databases, secured computing, Homorphism cryptographic algorithm.

I.INTRODUCTION

For securing the Database and also to maintain its confidentiality.Implementing"Homorphismcryptographic algorithm is the key way preferred to serve the purpose.

Existing system with limitations:

The existing system supposes Alice owns a k-anonymous database and needs to determine whether her database, when inserted with a tuple owned by Bob, is still k-anonymous. Also, suppose that access to the database is strictly controlled, because data are used for certain experiments that need
to be maintained confidential.Clearly, allowing Alice to dire ctlyread thecontents of thetuple breaks the privacy of Bob; o n theother hand, the confidentiality of the database managed by Alice is violated once Bob has access to the contents of the database. Thus the problem is to check whether the database inserted with the tuple is still k-anonymous, without letting "X" and "Y" know the contents of the tuple and database respectively.

Limitations:

1. The Database with the Tuple data doesn't be maintained confidentially.
2. The Existing System allows another person to easily access Database.

Proposed system with features:

In the current paper, we present two efficient protocols,oneofwhichalso supports the private update of a ge neralizationbased anonymous database. We also provide security proofs and experimental results for both protocols. So far no experimental results had been reported concerning such type of protocols; our results show that both protocols perform very efficiently.

Features:

The anonymity of DB is not affected by inserting the records.

We provide security proofs and experimental results for both protocols.

II.SYSTEM OVERVIEW

Module1: EMPLOYEE

On the user side, the user initially has to register to the organization by entering his/her details. Later after he is up with his Registration, if interested he/she can change the details entered, by clicking on the "edit profile" option. However Admin later enters the confidential information(salary) which only both user and admin knows. Applying the algorithm now, the confidential information cannot be seen by the other employees. Rather they see the boundaries of the salary if they view it in "Generalization" view and in star(*) form in "Surpression" view.

Module2: ADMIN

In our project we have admin module .what admin does is? He inserts or updates the important/confidential information of every registered user. This inserting is done in such a way that the salary(confidential information) is stored in the encrypted format in the Database.

This sort of security to the database is done to avoid hacking the employee details from the database. Now, only the admin can see the original information by selecting "Original" option. This mechanism is done by applying "Homomorphism Cryptographic" algorithm. Now only the admin and respective user knows the original salary. Other than these rights to the admin, he has the power to delete any user too.

ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 7, July 2013

Functional Requirements:

In software engineering, a **functional requirement** defines a function of a software system or its component. A function is described as a set of inputs, the behavior, and outputs (see also software).Functional requirements may be calculations, technical details, data manipulation and processing and other specific functionality that define what a system is supposed to accomplish. Behavioral requirements describing all the cases where the system uses the functional requirements are captured in use cases. Functional requirements are supported by non-functional requirements (also known as quality requirements), which impose constraints on the design or implementation (such as performance requirements, security, or reliability). How a system implements functional requirements is detailed in the system design.As defined in requirements engineering, functional requirements specify particular results of a system. This should be contrasted with non-functional requirements which specify overall characteristics such as cost and reliability. Functional requirements drive the application architecture of a system, while non-functional requirements drive the technical architecture of a system.

- In this, the employee registers and enters his/her details and thus a employee data is created at Admin side for inserting confidential data.
- Every insertion of data will store the encrypted form of the salary entered by the Admin given for every employee.
- Only the Admin can view the original data however the employee knows his/her respective salary and thus others are not allowed to view the data entered by the Admin.

Non-Functional Requirements:

In systems engineering and requirements engineering, a **non-functional requirement** is a requirement that specifies criteria that can be used to judge the operation of a system, rather than specific behaviors. This should be contrasted with functional requirements that define specific behavior or functions. In general, functional requirements define what a system is supposed to do whereas non-functional requirements define how a system is supposed to be. Non-functional requirements are often called **qualities** of a system. Other terms for non-functional requirements are "constraints", "quality attributes", "quality goals" and "quality of service requirements". Qualities, that is, non-functional requirements, can be divided into two main categories:

- Execution qualities, such as security and usability, which are observable at run time.
- Evolution qualities, such as testability, maintainability, extensibility and scalability, which are embodied in the static structure of the software system.

III.THE WORKING PRINCIPLE

After analyzing the requirements of the task to be performed, the next step is to analyze the problem and understand its context. The first activity in the phase is studying the existing system and other is to understand the requirements and domain of the new system. Both the activities are equally important, but the first activity serves as a basis of giving the functional specifications and then successful design of the proposed system. Understanding the properties and requirements of a new system is more difficult and requires creative thinking and understanding of existing running system is also difficult, improper understanding of present system can lead diversion from solution.

ANALYSIS MODEL

Mainly there are four phases in the "**Spiral Model**":

Planning

Evolutions

Risk Analysis

Engineering

Software Development India

Planning: In this phase, the aims, option and constraints of the project are determined and are documented. The aims and other specifications are fixed so as to determine the strategies/approaches to go after during the project life cycle.

Risk Analysis: It is the most significant phase of "Spiral Model". In this phase the entire possible option that are available and helpful in developing a cost efficient project are analyzed and strategies are determined to employ the available resources. This phase has been added particularly so as to recognize and resolve all the possible risks in the project **Orphan Foundation Development.** If any indication shows some uncertainty in needs, prototyping may be utilized to continue with the obtainable data and discover out possible **software development** solution so as to deal with the potential modification in the needs.

Engineering: In this phase, the specific **software development** of the project is worked out. The output of developed of modules by modules is passed through all the phases iteratively so as to obtain development in the same.

Customer Evaluation: In this phase, before releasing the developed product, the product is passed on to the customer so as to obtain customer's views and suggestions and if some is left or the desire result is not achieved then all the needs will be identified and resolve all the possible problems/errors in the Farmers Buddy. One can compare it from the TESTING phase.

The spiral model, illustrated in below figure, combines the iterative nature of prototyping with the controlled and systematic aspects of the waterfall model, therein providing the potential for rapid development of incremental versions of the software. In this model the software is developed in a series of incremental releases with the early stages being either paper models or prototypes. Later iterations become increasingly more complete versions of the product.

Depending on the model it may have 3-6 task regions our case will consider a '6-task region' model.

These regions are:

ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 7, July 2013

- The **User communication** task – to establish effective communication between developer and User.
- The **planning** task – to define resources, time lines and other project related information..
- The **risk analysis** task – to assess both technical and management risks.
- The **engineering** task – to build one or more representations of the application.
- The **construction and release** task – to construct, test, install and provide user support (e.g., documentation and training).

The **User evaluation** task – to obtain customer feedback based on the evaluation of the software representation created during the engineering stage and implemented during the install stage.

The evolutionary process begins at the centre position and moves in a clockwise direction. Each traversal of the spiral typically results in a deliverable. For example, the first and second spiral traversals may result in the production of a product specification and a prototype, respectively. Subsequent traversals may then produce more sophisticated versions of the software.

An important distinction between the spiral model and other software models is the explicit consideration of risk. There are no fixed phases such as specification or design phases in the model and it encompasses other process models. For example, prototyping may be used in one spiral to resolve requirement uncertainties and hence reduce risks. This may then be followed by a conventional waterfall development.

Note that each passage through the planning stage results in an adjustment to the project plan.

Each of the regions is populated by a set of work tasks called a task set that are adapted to characteristics of the project to be undertaken. For small projects the number of tasks and their formality is low. Conversely, for large projects the reverse is true.

Advantages of the Spiral Model :

The spiral model is a realistic approach to the development of large-scale software products because the software evolves as the process progresses. In addition, the developer and the client better understand and react to risks at each evolutionary level. The model uses prototyping as a risk reduction mechanism and allows for the development of prototypes at any stage of the evolutionary development. It maintains a systematic stepwise approach, like the classic life cycle model, but incorporates it into an iterative framework that more reflect the real world. If employed correctly, this model should reduce risks before they become problematic, as consideration of technical risks are considered at all stages.

Disadvantages of the Spiral Model

Demands considerable risk-assessment expertise

It has not been employed as much proven models (e.g. the WF model) and hence may prove difficult to 'sell' to the client that this model is controllable and efficient.

IV.IMPLEMENTATION OF SYSTEM

The core API gives you the following features:

The Essentials: Objects, Strings, threads, numbers, input and output, data structures, system properties, date and time, and so on.

Applets: The set of conventions used by Java applets.

Networking: URL's TCP and UDP sockets and IP addresses.

Internationalization: Help for writing programs that can be localized for users.

Worldwide programs can automatically adapt to specific locates and be displayed in the appropriate language.

Networking

This article is about a client/server multi-threaded socket class. The thread is optional since the developer is still responsible to decide if needs it. There are other Socket classes here and other places over the Internet but none of them can provide feedback (event detection) to your application like this one does. It provides you with the following events detection: connection established, connection dropped, connection failed and data reception (including 0 byte packet).

1) IP datagram's

The IP layer provides a connectionless and unreliable delivery system. It considers each datagram independently of the others. Any association between datagram must be supplied by the higher layers. The IP layer supplies a checksum that includes its own header. The header includes the source and destination addresses. The IP layer handles routing through an Internet. It is also responsible for breaking up large datagram into smaller ones for transmission and reassembling them at the other end.

UDP is also connectionless and unreliable. What it adds to IP is a checksum for the contents of the datagram and port numbers.

TCP supplies logic to give a reliable connection-oriented protocol above IP. It provides a virtual circuit that two processes can use to communicate.

Internet addresses

In order to use a service, you must be able to find it. The Internet uses an address scheme for machines so that they can be located. The address is a 32 bit integer which gives te IP address. This encodes a network ID and more addressing. The network ID falls into various classes according to the size of the network address.

2) Network address

Class A uses 8 bits for the network address with 24 bits left over for other addressing. Class B uses 16 bit network addressing. Class C uses 24 bit network addressing and class D uses all 32.

3) Subnet address

Internally, the UNIX network is divided into sub networks. Building 11 is currently on one sub network and uses 10-bit addressing, allowing 1024 different hosts.

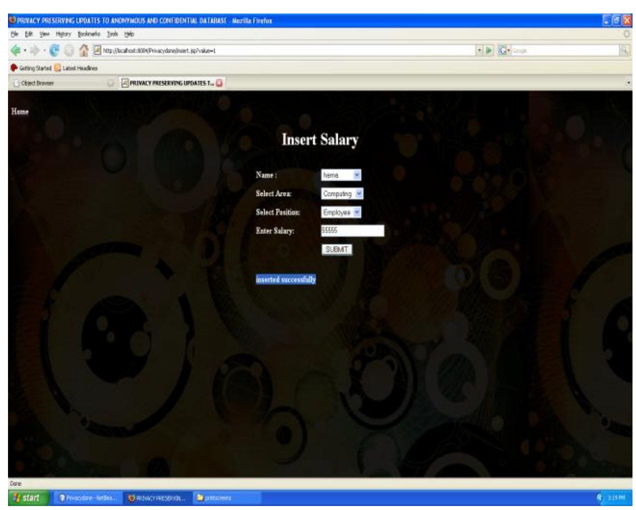
ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 7, July 2013

Login.html:

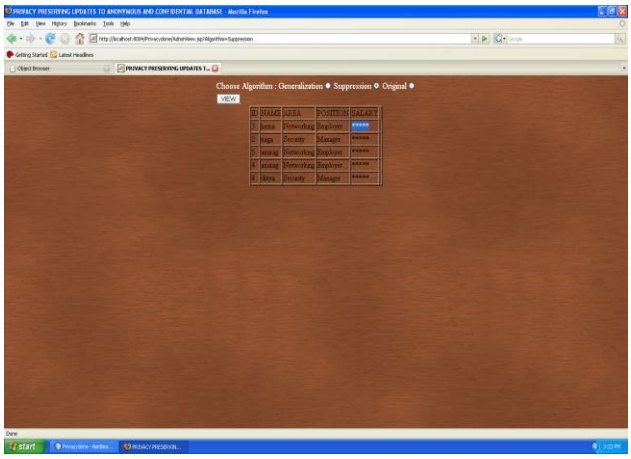
```
<%--
    Document   : login
    Created on : Feb 15, 2012, 1:55:56 PM
    Author     : Administrator
--%>
<%@page contentType="text/html" pageEncoding="UTF-8"%>
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN"
   "http://www.w3.org/TR/html4/loose.dtd">
<html>
    <head>
        <script language="javascript">
            function log()
            {
                var name=document.f.user.value;
                var pass=document.f.pwd.value;
          if(name=="")
                    {
                        alert("Please enter username");
                        document.f.user.focus;
                        return false;
                    }
                    else if(name.length<3)
                        {
                         alert("Please enter more than 6 characters");
                        document.f.user.focus;
                        return false;
                        }
                        else if(pass=="")
                            {
                                alert("Please enter Password");
                                document.f.pwd.focus;
                                return false;
                            }
                          else if(user=="")
                              {
                                alert("Please select any one radio button");
                                return false;
                              }
                            else
                              {
                                return true;                    }
            }
            </script>
    </head>
     <body background=" 6.jpg">
        <form name="f" onsubmit="return log()" action="log.jsp" method="post">

                                                                             <img alt="" src="153.GIF">

        <center><h1>LOGIN</h1></center>
        <center>
          <table>
              <try>
                  <the>
                      Username:</the>
                  <the><input type="text" name="user"></the>
              </try>
              <try>
                  <the>Password:</the>
                  <the><input type="password" name="pad"><br><br></the>

              </tr>
              <tr><th><input type="submit" value="submit"></th>

                   <th><a href="Forgotpass.jsp"> Forgot Password</a></th>
             </tr>
              </table>
        </center>
        </form>
    </body>
</html>
```

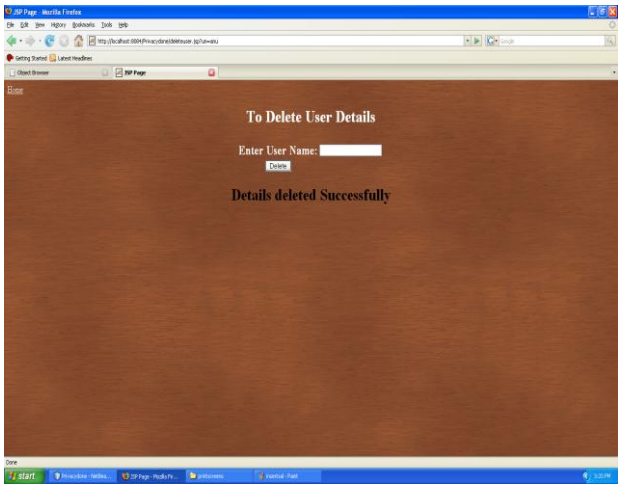
V.EXPERIMENTAL RESULTS



ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 7, July 2013





VI.CONCLUSION

In our project, we have concentrated on maintaining data security on few fields of the registered employees in an organization. This is achieved by applying the Generalization And Suppression techniques. Here, we have implemented the techniques such that even though the Database is hacked the important or the confidential details of the user on which the above techniques were applied cannot be viewed but can be viewed by only admin through web pages behind which the JSP code was applied i.e now the data is secured. Our project "Privacy Preserving Updates to Anonymous and Confidential Databases" can be further developed by implementing the "Generalization" and "Surpression" techniques on the other fields whichever the Admin feels important or the employee wants to keep those field data confidential. Also, other than the data fields, protection and security can be applied to the images stored in the database and also for the images that the user feel not to be revealed to other co-users while they visit respective user/employees profile.If at all any type of algorithms are developed in the future which are more strong in protecting and securing the data, then those algorithms can be used in our project to have a more secured computing.

REFERENCES

1)Alberto Trombetta, Wei Jiang, Elisa Bertino, Lorenzo Bossi. Privacy-Preserving Updates to Anonymous and Confidential Databases. IEEE Trans. Dependable Sec. Comput., 2011: 578~587

2)N. R. Adam and J. C. Wortmann. Security-control methods for statistical databases: A comparative study. ACM Computing Surveys, 21(4):515–556, December 1989.

3)D. Agrawal and C. C. Aggarwal. On the design and quantification of privacy preserving data mining algorithms. In Proceedings of the 20th Symposium on Principles of Database Systems, Santa Barbara, California, USA, May 2001.

4)N. Ahituv, Y. Lapid, and S. Neumann. Processing encrypted data. Communications of the ACM, 30(9):777–780, September 1987.

5)S. Ajmani, R. Morris, and B. Liskov. A trusted third-party computation service.Technical Report MIT-LCS-TR-847, MIT, May 2001.

6)N. Alon, L. Babai, and A. Itai. A fast and simple randomized parallel algorithm for the maximal independent set problem. Journal of Algorithms, 7:567–583, 1986.

7)C. Cachin, S. Micali, and M. Stadler. Computationally private information re-trieval with polylogarithmic communication. Advances in Cryptology – EUROCRYPT '99, 1592:402–414, 1999.

8)B. Chor and N. Gilboa. Computationally private information retrieval. In Proc.of 29th ACM Symposium on Theory of Computing, pages 304–313, 1997.

9)U. Dayal and H.-Y. Hwang. View definition and generalization for database integration in a multidatabase system. IEEE Transactions on Software Eng.,10(6):628–645, 1984.

BIOGRAPHY

Mr. B.Srinivasulu, Post Graduated In (CSE-M.Tech) From JNTUH, 2010, And Graduated In Computer Science & Engineering (CSE-B.TECH) From JNTU Hyderabad, 2008. He Is Working Presently As Asst.Professor In Department Of Computer Science & Engineering In HOLY MARY INSTITUTE OF TECHNOLOGY & SCIENCE (HITS), R.R.Dist, A.P, INDIA.He Is Has 2+ Years Experience,His Research Interests Include Data Warehousing & Data Mining And Cloud Computing And Mobile Communication.

Mrs.B.V.Usha, Post Graduated In (CSE-M.Tech) From SRMU, And Graduated In Computer Science & Engineering (B.TECH-CSE) From JNTU,She Is Working Presently As Asst.Professor In Department Of Computer Science & Engineering In CMEC-Hyderabad,A.P.She Is Has 3+ Years Experience,His Research Interests Include Data Warehousing & Data Mining And Database Systems.

ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 7, July 2013

Mr.R.V.Gandhi,Post Graduated In (CSE-M.Tech) From JNTUH, And Graduated In Computer Science & Engineering (CSE-B.TECH) From JNTU Hyderabad,He Is Working Presently As Asst.Professor In Department Of Computer Science & Engineering In HOLY MARY INSTITUTE OF TECHNOLOGY & SCIENCE (HITS), R.R.Dist, A.P, INDIA.He Is Has 4+ Years Experience,His Research Interests Include Data Warehousing & Data Mining And Software Testing.

Mr. K. Ramakrishna, Post Graduated in (CSE-M.Tech) From JNTUH, 2010, and graduated in Information Technology& Engineering (B.TECH-IT) From K.U. He is working presently as Asst.Professor in Department of Computer Science & Engineering in HOLY MARY INSTITUTE OF TECHNOLOGY & SCIENCE (HITS), INDIA.He Is Has 4+ Years Experience, His Research Interests Include Data Warehousing & Data Mining and Cloud Computing and mobile communication.