Scrutinize The Utility Of Preserved Data

Mounika. Kodela[1], Pranathi.Sivva[2], Muthamil Sudar K[3], Nagaraj.P[4]
Student [1,2] , Assistant Professor[3,4]
Kalasalingam Academy of Research and Education, Anand Nagar, Krishnankoil-626126, Tanilnadu, India

Abstract

A large amount of data which has been handled over a sector in note to that the data which has been collected from the source will be stored in a database. The admin has the authority of approving the manager so that after the approval of admin the manager can access the application. Once the manager gets declined by the admin the can't able to login in that process the manager won' t be able to access the application. The details which have been stored can be retrieved later in case of using those details or viewing that information. The admin and the manager is one who can able to view the actions performed by the employees. By handling these data by the admin, he can view the data. In case of loss of data or theft of data in a form of attack the manager and the admin can view the details of the employee who has been attacked in the form of tables. The action can be performed here. The details can be attacked by four methods such as a data linkage attack, attribute attack, table linkage attack and probabilistic attack. By these attacks, we can attack the details of an individual by getting their id which has been published. By this action the manager and the admin can view the details of the employee who has been attacked.

Keywords *Privacy preserving, Scrutinize, Security.*

1. INTRODUCTION

A protection framework detects and mitigates vulnerabilities in the network, either by eliminating or limiting access to a very small community. There's endless tension between inventing new security mechanisms to secure data and inventing hacking methods along with finding and exploiting pre-existing vulnerabilities. The protection of data and resources is therefore becoming more frequent.

This application is focused on a company that maintains full employee and manager information that was handled by an admin in a company the need for this application is to improve the employee's details as to whether it is a protected data. As a significant amount of data was treated over a sector in a note that the data obtained from the source would be stored in a database. The administrator has the power to approve the manager, so that the manager can access the application after the admin approval. If the manager is rejected by the administrator, the manager will not be able to log in to that operation. In case of using those details or displaying the information, the details that have been stored can be retrieved later. The planner and the boss are one who can see the actions the workers do. By using the admin to handle those details. The Administrator will access the data. In the case of data loss or data theft in a form of assault, the manager and the admin will access the information of the employee who was attacked in tables form. Should conduct the action here. Four methods like a data connection attack, attribute attack, table linkage attack and probabilistic attack can attack the information. Via those attacks we may target an individual's data.

2. RELATED WORK

The following series of confidentiality operations was clustered in order to prevent the privacy leakage of the published data: generalization and exclusion, anatomization and permutation, and perturbation. Data-publishing privacy algorithms vary in their choice of anonymity operations.

The most popular anonymity operations used to enforce k-anonymity for privacy protection are generalization and suppression. Anatomization and permutation Anatomization and permutation are intended to de-link the relationship between attributes without alteration. The approaches to anatomization discern the association between QIs and SAs and produce several different tables with a non-overlapping attribute.

.

2.1 System Requirements

Hardware Requirements

- RAM 4GB
- Dual-Core 2.8 GHz Processor and Above
- HDD 80 GB Hard Disk Space and Above

Software Requirements

- WINDOWS Operating System (7 /XP and above)
- Visual Studio .Net 2015
- Visual Studio .Net Framework 4.5
- SQL Server 2014

2.2 Existing System

Using bigger classes will help to protect privacy more, but it would also take longer to compile details from the released tables. If the intruder will not interact with the category to which the victim belongs, the database space would be very wide, making it far less probable that the victim may provide any details.

In this portion, we systematically calculate the privacy protections after an attacker has effectively performed data driven attacks. Preserving data protection is an important challenge in order to enable for the dissemination of these data for different purposes of study and review. As mentioned earlier, privacy is defined as the entropy of confidential information given an opponent has access to other public information connected with it.

Disadvantages

- The details can be modified on the grounds of the presumption, so that the protected details can become impacted.
- The critical data that lose due to any attacks when executing an application is not quantitative in nature.
- Resource-restrictive such that data may be protected with logical evidence that the interest must be preserved
- Evidence leakage from the database can occur during this session.

2.3 Proposed System

In several data studies the data statistics need to be collected. We classify the usefulness according to how well one can predict the number of queries, i.e. you need to find Number of records which satisfy the condition of the question. To check the anonymous data utility of our system, we first explain how to address a query about counting to prove that our analysis of the privacy utility of published data. In this case, the intruder tries to assume a portion of Sensitive data information on the target victim's right. The requirement for privacy is specified to resist an attack by the attribute linkage. We're assuming in this case an attacker might recognize any aspect of the person. The intruder attempts to assume true, confidential details regarding the intended person. To avoid the attached table relation the confidentiality condition is set. We assume an intruder can learn about the confidential data of a part of the target group. The attacker is trying to determine that the target appears in the tables that have been written. The necessity to Privacy to endure a probabilistic assault is defined. In this case, we suspect an attacker might be informed of the victim's sensitive details, or the victim's likelihood. The attacker attempts to conclude some valuable information by measuring the discrepancy in likelihood of knowing the critical data importance before and after the study.

3. PRIVACY ATTACKS AND PRIVACY MODEL

We first introduce four privacy attacks in this section, and then present our model of privacy. Much of the reported data is stored in tabular format like Table 1. In Table 1 each person has three types of attributes (EI, QIs, and SA). A person can be uniquely identified by the EI Name. Qis include gender, jobs, age and Zip code. The SA Salary should be covered the protection of data privacy is an important task to enable the publishing of such data for various purposes of research and analysis.

In this paper, we concentrate on protecting individual privacy in a table T and our main goal is to prevent two types of attacks. An attacker in the first category focuses on connecting documents, attributes, or tables in order to locate an exact target victim. The attacking approaches are named as record linkage, attribute linkage and table linkage respectively. In the second group, an attacker cannot actually connect documents, attributes or tables to a target victim, however the attacker's probabilistic confidence in the target victim's sensitive information can be modified based on context knowledge and published data. Typically, this is referred to as the probabilistic attack. To describe the attacks, different attacks demonstrate where EI has been removed for each record.

3.1 Record linkage attack. An attacker may recognize a tuple or a small number of tuples based on the target victim's QIs from the reported anonymous T details.

3.2 Attack correlation factor. The intruder cannot precisely recognize the victim's tuple, but may be able to infer the sensitive information of the victim from Tang depending on the category to which the victim belongs.

3.3 Table linkage attack Both the linking of documents and the linking of characteristics was based on the presumption that the perpetrator realized the victim's data was present in T. The object of the table connection is to decide if the record of the victim is present in T.

3.4 Probabilistic attack. The three attacks above rely on documents, attributes and tables that specifically relate to a specific individual. The probabilistic assault implies an intruder will derive certain knowledge from the disparity between the previous views and the current ones. The disparity between the prior and the posterior beliefs must be minimal to avoid this assault.

4.SOFTWARE REQUIREMENT SPECIFICATION

This paper has the function of providing a comprehensive overview of the Web application framework. This will describe the function and features of the system, the system interfaces, what the system will do, the constraints it will work under and how the system will respond to external stimuli. This paper is intended for stakeholders as well as device creators, and will be submitted for approval by the Area Historical Society. The aim of this Specification for Software Requirement (SRS) is to help the project. Some specifications are provided which are used in the Transaction Mercator Framework. Both parts design, coding and testing with helping of SRS. This document aims to explain the requirements imposed on the Transaction Mercator System and acts as a contract between the customer and the developers on what to expect from the stock exchange and how the system components interact with external systems. Developing the program that meets the SRS and addressing all program specifications is the responsibility of the developer. Demonstration of the program and deployment of the program at the client's location is satisfactory after the acceptance test. Provide the correct software manual outlining the device implementations to work on it, as well as the framework manuals undertaking the software training that could be necessary to utilize the application. The program is maintained for a duration of one year after deployment.

4.1 Functional Requirements

The following is a list of browsing-enabled device functionalities.

- An operation with a UI enabling you to change browser settings.
- Provide a second Event allowing users to access the share with the administrator's permission.
- Manage lifecycle operation properly.

- A precondition for compiling and running code for some points in this section of the grade is code that compiles and runs.Your application will allow a user to browse the shares with unique metadata, buy and sell the shares. The task allows you to create a browsing UI, and a built-in UI for both.

4.2. Non-FUNCTIONAL REQUIREMENTS

Every member will have to have a separate program. The program would ask to open the application by the username and password. Unregistered consumer is not permitted to access the network. The program will have access to Role-based Machine functions. Approval process

- You have to describe it. The framework will provide modules for flexible design, so that they can be reused during deployment.
- These are basically the following:
- Safe access to classified data (the identity of the employee). Availability 24 X 7
- Better component design to improve peak-time performance
- Flexible service-based architecture is highly desirable for future expansion

4.3. Performance Requirements

Performance is calculated according to the output the application produces. The definition of specifications plays an significant part in the design of a program. Only when the correct specifications are correctly described can a device be developed which suits into the required context. It is mostly up to existing device users to provide the required specifications, because they are the ones who would really be using the program. It is because during the early phases it is necessary to learn the specifications, so that the device can be designed according to these specifications. When developed, it is very difficult to modify the system and, on the other hand, it is of no use to design a system that does not meet the user's requirements.

5. SYSTEM DEVELOPEMENT ENVIRONMENT

5.1 Introduction To. Net

The .NET Framework Architecture

.NET Platform (pronounced dot net) is a Microsoft-developed software system that runs predominantly on Windows. It includes a wide software library known as the System Software Library (FCL) which provides interoperability of languages (each language may use code written in other languages) through multiple languages. The programs written for the. NET System run in a software environment (as opposed to the hardware environment), known as the Common Language Runtime (CLR), memory management, and exception handling. Together FCL and CLR form the .NET Structure. FCL provides user interface, data access, accessibility to the database, cryptography, creation of web applications, computational algorithms, and network communications. Programmer allows software by integrating its own source code with the. NET System and other libraries. Most new applications developed for the Windows platform are intended to use the. NET Framework. Microsoft is now increasingly developing an interactive production platform for Visual Studio. NET applications.

The operating system is the first level of representation; the .NET layer is situated between the system and the applications. The second level is the Common Language Runtime (CLR) which provides the most work for the part of the. NET System. Later in this chapter we'll discuss the CLR. The next level is the Base Class Library (BCL), which includes all .NET objects that can be used in your code and by Visual Basic when building applications. The BCL also offers the framework of a range of. NET technologies that you use in building applications, such as WPF, Windows Forms, ASP.NET, WCF, etc. Applications that depend on preceding layers reflect the last level.

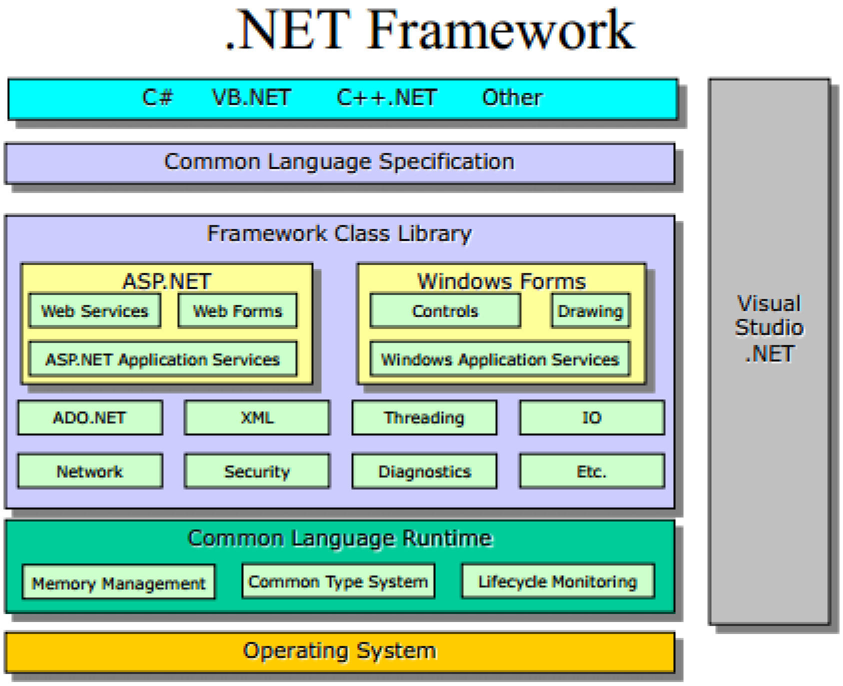


Fig.1 .Net Architecture

Common Language Runtime engine

Common Language Runtime (CLR) serves as the .NET Framework execution engine. All. NET systems are executed under the control of the CLR, maintaining certain properties and actions in the fields of memory management, protection and managing exceptions.

Language independence

.NET defines a Specific Form Scheme, or CTS. The CTS specification specifies all potential CLR-supported data types and programming structures, and how they can or may not communicate with each other in compliance with the Popular Language Interface (CLI) specification. The. NET Platform Requires class and object instances to be exchanged between libraries and applications written using any conformation. NET language, regardless of this functionality.

Framework Class Library

Framework Configuration Library (FCL) is a software library which is accessible in all languages utilizing the. NET Platform. FCL offers classes encapsulating a variety of specific features, including file reading and writing, graphical rendering, database contact, manipulation of XML records, and so on. It consists of modules, modular form interfaces that integrate CLR.

Simplified deployment

The. NET Platform provides interface features and resources to help control computer product deployment and insure it will not conflict with previously installed applications, and complies with security specifications.

Security

The architecture fixes some of the bugs which have been abused by malicious hackers, such as buffer overflow. Therefore, .NET provides a growing protection architecture for all programs.

Portability

Although Microsoft has never deployed the complete application on any device but Microsoft Windows, the architecture has been built Implementations for other operating systems can be platform-agnostic and cross-platform (see Silver light and § Alternate implementations). Microsoft sent to ECMA and ISO the CLI requirements (including core class modules, CTS, and Generic Intermediate Language), C #, and C++/CLI, rendering them accessible as official standards. This allows third parties on other platforms to create compatible implementation of the Framework and its languages.

Common Language Specification

CLS is a set of rules defining the features that the. NET system supports various languages should be accepted by all languages is an agreement between language designers and class library designers on the features and implementation conventions that can be relied on. Example: public names should not depend on uniqueness case because certain languages are not immune to the case. It does not mean that all languages are not case sensitive outside the CLR. At the heart of the Framework is a common type system called the. NET Common Type System (CTS) Everything is an object-yet powerful packaging and unboxing All types fall into two groups-Value types and Reference types. Stored in stack. Three types of values: Primitive, structures and enumerations.

5.2 Sql Server 2014

SQL is a Relational Database Management System (RDBMS) operating as a server that offers multi-user access to multiple databases. It is a common database option for web applications, and it is an open source software. The setup process for a SQL database varies from host to host, but we can end up with a database name, a user name, and a password. We'll need to build a table before using our database. A table is a section for storing similar information in the database. We'll set up the different fields that will be included in a list. Creating a table is simple; just type the name, choose the number of fields and click the "go" button.

We will then be taken to a setup screen where you must create the fields in the database.

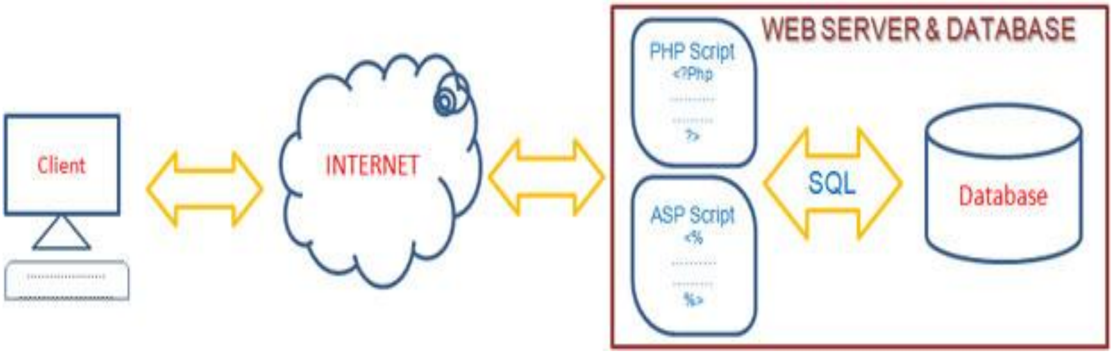


Fig.2 Web Server & Database

SQL is used for data base correspondence. It is the basic language for relational data base management frameworks according to ANSI (American National Standards Institute).

SQL statements are used to execute functions such as modifying database data, or extracting database data. Such widely utilized SQL link database management systems are: Oracle, Sybase, Microsoft SQL Server, Connect, Ingres, etc

While most database systems use SQL, most of them do have their own proprietary extensions which are typically used only on their framework. Nevertheless, basic SQL commands such as "Pick," "Add," "Edit," "Remove," "Build," and "Fall" can be used to do nearly all that a database need.

Microsoft SQL Server is a framework built by Microsoft for the maintenance of relational databases. As a database, that is a computer device whose primary purpose is to store and retrieve data as needed by certain software programs, including those on the same machine or those operating over a network (including the Internet) on another machine.

6. SYSTEM DESIGN

Software design sits in the software engineering cycle technological kernel and is implemented irrespective of the technology paradigm and application area. For any engineered product or device, the first phase in the production cycle is architecture. The designer's aim is to build a model or image of an entity which is later to be built. Starting with the device necessity being defined and evaluated, the design of the program is the first of three engineering activities-design, coding and testing required for software development and evaluation. A single word "Price" may state the value. Design is the position where the software development promotes efficiency. Design gives us software representations that can be appraised for consistency. Design is the only way we can effectively turn a vision of a customer into a finished product or system of software. Software design forms the basis for all software engineering steps that follows. We risk designing an unpredictable device without a solid specification – one that will be difficult to evaluate, one whose consistency can't be measured until the final point. A single word "Price" may state the value. Development is the position where quality is promoted when creating applications.

Design gives us software representations that can be appraised for consistency. Design is the only way we can effectively turn a vision of a customer into a finished product or system of software. Software design serves as the foundation for all phases in software engineering that follow.

Progressive improvement of the data structure, system structure, and operational information is checked and reported during design. You may view system design from either the technological or project management perspective. Design consists of four tasks from a technological point of view architecture of data systems, design of the applications and design of procedures.

7. SENSITIVE LABEL PRIVACY PRESERVATION WITH ANATOMIZATION (SLPPA)

7.1 Overview

1 our SLPPA scheme includes two procedures, table division and group division. By dividing the original table into several tables, the complexity of reconstructing the original table from the published tables may be increased. By splitting the original table into several classes, we can ensure that each group in the published tables is able to follow our model of privacy (α, β, π), and thereby resist the four types of attacks:

EI is first removed from the original Table 1 to generate Table 2.

- The SA is first put in a different table during the table separation, and the QIs are then partitioned into many other tables. To calculate the QI weight and mean-square contingency coefficient, we follow the principle of entropy to evaluate the degree of interaction between QIs. Table 2 is split into a few tables of certain operations as seen in Table 4.
- We first divide the original data into separate buckets each comprising records of the same SA interest during the community division and rate the buckets in a decreasing order depending on the bucket scale. When we separate people into various classes in the buckets, we call the four conditions of privacy.
- After separating entities into various classes, their category identifiers (GIDs) would be applied to the tables comprising specific attributes. These tables should eventually be released as seen in Table 3.

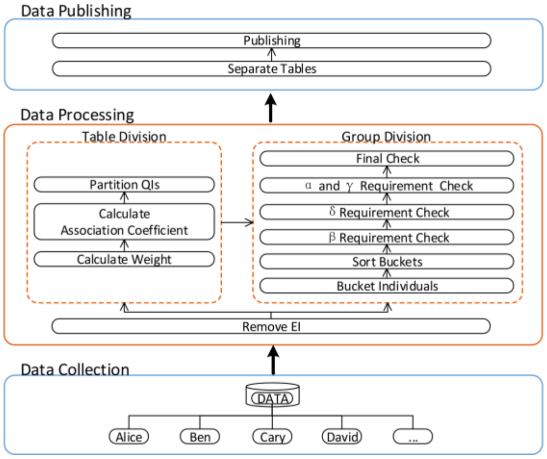


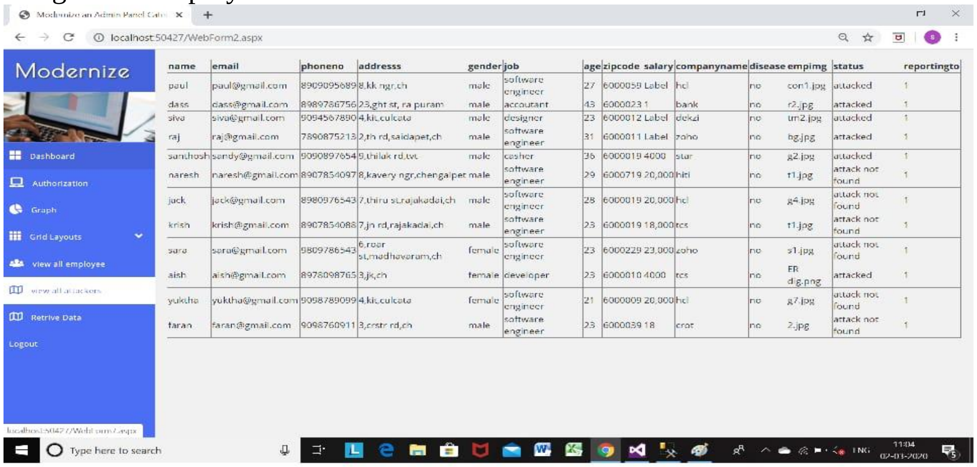
Fig.3 SLPPA Architecture

7.2 Algorithm SLPPA

Anatomization de-associates the association between attributes to protect the privacy of the SA by splitting them into separate tables without any alteration. In our design, we first divide the attributes into several tables, depending on the QI weight and the QI relationship, and then complete the group division. Table division seeks to optimize the association of attributes in the same table and to minimize the association of attributes in the various tables. We divide attributes into three tables, for QIs two and for SA one. As table division involves three steps, calculating the weight of the QI, calculating the coefficients of association between the QIs and partitioning QIs. The original data was divided into different tables after division of the table. Subsequently, group division is introduced to split the original data into various categories in order to satisfy each group's expectation of privacy (α, β, π, ÿ). Each single person belongs only to one party. This illustrates how one can follow community division.

8. OUTPUT

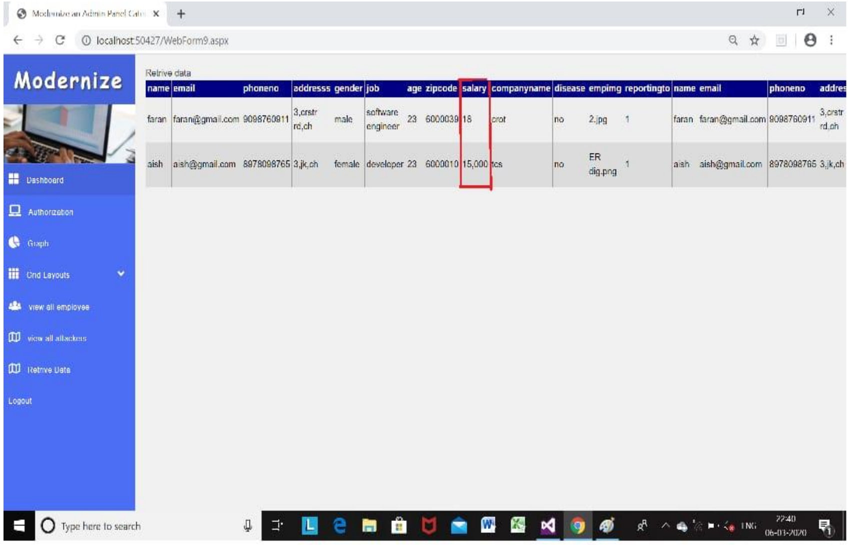
This is the form in which we can give the employees who have been attacked. Both manager and admin can give the employees who have been attacked.



name	email	phoneno	addresss	gender	job	age	zipcode	salary	companyname	disease	empimg	status	reportingto
paul	paul@gmail.com	8909095689	8,kk ngr,ch	male	software engineer	27	6000059	Label	hcl	no	con1.jpg	attacked	1
dass	dass@gmail.com	8989786756	23,ght st, ra puram	male	accoutant	43	6000023	1	bank	no	r2.jpg	attacked	1
siva	siva@gmail.com	9094567890	4,kit,culcata	male	designer	23	6000012	Label	dekzi	no	un2.jpg	attacked	1
raj	raj@gmail.com	7890875213	2,th rd,saidapet,ch	male	software engineer	31	6000011	Label	zoho	no	bg.jpg	attacked	1
santhosh	sandy@gmail.com	9090897654	9,thilak rd,tvt	male	casher	36	6000019	4000	star	no	g2.jpg	attacked	1
naresh	naresh@gmail.com	8907854097	8,kavery ngr,chengalpet	male	software engineer	29	6000719	20,000	hiti	no	t1.jpg	attack not found	1
jack	jack@gmail.com	8980976543	7,thiru st,rajakadai,ch	male	software engineer	28	6000019	20,000	hcl	no	g4.jpg	attack not found	1
krish	krish@gmail.com	8907854088	7,jn rd,rajakadai,ch	male	software engineer	23	6000019	18,000	tcs	no	t1.jpg	attack not found	1
sara	sara@gmail.com	9809786543	6,roar st,madhavaram,ch	female	software engineer	23	6000229	23,000	zoho	no	s1.jpg	attack not found	1
aish	aish@gmail.com	8978098765	3,jk,ch	female	developer	23	6000010	4000	tcs	no	ER dig.png	attacked	1
yuktha	yuktha@gmail.com	9098789099	4,kit,culcata	female	software engineer	21	6000009	20,000	hcl	no	g7.jpg	attack not found	1
faran	faran@gmail.com	9098760911	3,crstr rd,ch	male	software engineer	23	6000039	18	crot	no	2.jpg	attack not found	1

Fig.4 View Attacker Profile

This is the form where we have been retrive the data of the employees who have been attacked.The admin alone can retrived the data of a particular employee.



Retrive data

name	email	phoneno	addresss	gender	job	age	zipcode	salary	companyname	disease	empimg	reportingto	name	email	phoneno	addres
faran	faran@gmail.com	9098760911	3,crstr rd,ch	male	software engineer	23	6000039	18	crot	no	2.jpg	1	faran	faran@gmail.com	9098760911	3,crstr rd,ch
aish	aish@gmail.com	8978098765	3,jk,ch	female	developer	23	6000010	15,000	tcs	no	ER dig.png	1	aish	aish@gmail.com	8978098765	3,jk,ch

Fig.5 Retriving The Data

9. CONCLUSION

We develop and introduce an anonymity technique called SLPPA to protect the sensitive attribute when social data is being written. In order to avoid attacks resulting from record linkage, table linkage and linkage of attributes as well as probabilistic attacks, we suggest a model of privacy (α, β, ÿ, π). We design two algorithms respectively to reduce the time consumption and increase the efficiency of our SLPPA we design two algorithms respectively for efficient table division and the group division. Our performance studies focused on two detailed sets of real-world data show that SLPPA can also provide good data usability, in addition to better data privacy protection. Our data security review shows that SLPPA can also withstand the attack on context information. We will consider in future research how to protect the privacy of published data with multiple sensitive attributes and expand our algorithms to protect the privacy of graph data in social networks.

REFERENCES

[1] Y. Wang, L. Xie, B. Zheng, and K. C. Lee, “ High utility k-anonymization for social network publishing,” Knowledge and Information Systems, vol. 41, no. 3, pp. 697– 725, 2014.

[2] Y. Xu, T. Ma, M. Tang, and W. Tian, “ A survey of privacy pre- serving data publishing using generalization and suppression,” Applied Mathematics and Information Sciences, vol. 8, no. 3, p. 1103, 2014.

[3] N. Victor, D. Lopez, and J. H. Abawajy, “ Privacy models for big data: a survey,” International Journal of Big Data Intelligence, vol. 3, no. 1, pp. 61– 75, 2016.

[4] B. Fung, K. Wang, R. Chen, and P. S. Yu, “ Privacy preserving data publishing: A survey of recent developments,” ACM Computing Surveys (CSUR), vol. 42, no. 4, p. 14, 2010.

[5] L. Sweeney, “ k-anonymity: A model for protecting privacy,” International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems, vol. 10, no. 05, pp. 557– 570, 2002.

[6] M. Rajaei, M. S. Haghjoo, and E. K. Miyaneh, “ Ambiguity in social network data for presence, sensitive-attribute, degree and relation- ship privacy protection,” PloS one, vol. 10, no. 6, p. e0130693, 2015.

[7] X. Xiao and Y. Tao, “ Anatomy: Simple and effective privacy preservation,” in Proceedings of the 32nd international conference on Very large data bases. VLDB Endowment, 2006, pp. 139– 150.

[8] T. Li, N. Li, J. Zhang, and I. Molloy, " Slicing: A new approach for privacy preserving data publishing," IEEE transactions on knowledge and data engineering, vol. 24, no. 3, pp. 561– 574, 2012.

[9] K. Tadisetti, P. Madhuri, and J. B. Shastri, " Implementation of slicing technique for privacy preserving data publishing," Journal of Neurophysiology, vol. 114, no. 3, pp. 1538– 44, 2015.

[10] M. Wang, Z. Jiang, Y. Zhang, and H. Yang, " T-closeness slicing: A new privacy-preserving approach for transactional data pub- lishing," Informs Journal on Computing, vol. 30, no. 3, pp. 438– 453, 2018.

[11] V. S. Susan and T. Christopher, " Anatomization with slicing: a new privacy preservation approach for multiple sensitive attributes," SpringerPlus, vol. 5, no. 1, pp. 1– 21, 2016.Z. H. Zou, Y. Yi, and J. N. Sun, " Entropy method for determination of weight of evaluating indicators in fuzzy synthetic evaluation for water quality assessment," Journal of Environmental Sciences, vol. 18, no. 5, pp. 1020– 1023, 2006.

[12] A. Gkoulalas-Divanis, G. Loukides, and J. Sun, " Publishing data from electronic health records while preserving privacy: A survey of algorithms," Journal of Biomedical Informatics, vol. 50, no. 8, pp. 4– 19, 2014.

[13] P. Samarati, " Protecting respondents' identities in microdata re- lease," IEEE transactions on Knowledge and Data Engineering, vol. 13, no. 6, pp. 1010– 1027, 2001.

[14] L. Sweeney, " Achieving k-anonymity privacy protection using generalization and suppression," International Journal of Uncertain- ty, Fuzziness and Knowledge-Based Systems, vol. 10, no. 05, pp. 571– 588, 2002.

[15] S. Kiyomoto and T. Tanaka, " A user-oriented anonymization mechanism for public data," in International Conference on Inter- national Workshop on Data Privacy Management. ACM, 2010, pp. 22– 35.

[16] V. S. Iyengar, " Transforming data to satisfy privacy constraints,"
Kdd, pp. 279– 288, 2002.

[17] X. Zhang, C. Liu, S. Nepal, and J. Chen, " An efficient quasi- identifier index-based approach for privacy preservation over incremental data sets on cloud," Journal of Computer and System Sciences, vol. 79, no. 5, pp. 542– 555, 2013.

[18] K. LeFevre, D. J. DeWitt, and R. Ramakrishnan, " Incognito: Efficient full-domain k-anonymity," in Proceedings of the 2005 ACM SIGMOD international conference on Management of data. ACM, 2005, pp. 49– 60.

[19] R. Chen, B. C. M. Fung, N. Mohammed, B. C. Desai, and K. Wang, " Privacy-preserving trajectory data publishing by local suppression," Information Sciences an International Journal, vol. 231, no. 1, pp. 83– 97, 2013.

[20] M. Serpell, J. Smith, A. Clark, and A. Staggemeier, " A preprocessing optimization applied to the cell suppression problem in statistical disclosure control," Information Sciences, vol. 238, no. 7, pp. 22– 32, 2013.

[21] B. C. M. Fung, K. Wang, and P. S. Yu, " Anonymizing classification data for privacy preservation," IEEE Transactions on Knowledge & Data Engineering, vol. 19, no. 5, pp. 711– 725, 2015.

[22] B. C. Fung, K. Wang and P. S. Yu, " Top-down specialization for information and privacy preservation," in 21st International Conference on Data Engineering (ICDE' 05). IEEE, 2005, pp. 205– 216.

[23] X. Sun, L. Sun, and H. Wang, " Extended k -anonymity models against sensitive attribute disclosure," Computer Communications, vol. 34, no. 4, pp. 526– 535, 2011.

[24] M. Ye, X. Wu, X. Hu, and D. Hu, " Anonymizing classification data using rough set theory," Knowledge-Based Systems, vol. 43, no. 2, pp. 82– 94, 2013.