Preserving Privacy Concerns of Database

Arshi Shaikh[1] Sayed Saman Zehra[2] Kimaya Manjrekar[3] Reena Saini[4] Kunal Pimple[5]
[1,2,3,4,5]Theem College of Engineering, Boisar

Abstract—In today's world with the fast growing development in internet networks, users data is being stored in database and so the users are more concerned their about data which lies in the database. As sharing of data is continuously taking place between the clients and servers. However not all the data is to be shared among all the clients. A huge volume of certain data is only reserved for authorized clients. For this to take place in real time the server is the one which needs to identify the authorized clients. In relational databases data was basically monitor by consistency control mechanism like a certain data object can only be read by the users. If still this conventional consistency mechanism would have been used the databases will be used inadequately. The matter of Privacy is still a matter of great concern to the researchers. Privacy focuses mostly on user accounts creation and managing the rights of different users to the data. In this paper we try to take a look into the aspects and analyze the available solutions to the issues regarding privacy. To deal with this issue of granting access only to the authorized clients a separate privacy module is to be made in order to authenticate the client before accessing the data from the database. This process of authentication is done by the server. Privacy module implementation can start with the process of creating and publishing appropriate privacy standards for the database along with existing privacy constraints.

Key words: Privacy constraints, Access levels, Transparency, Disclosure, Authorized users, Authentication

I. INTRODUCTION

The ability of communicating between computers through internet has spawned a new class of centred application based on data .Preserving privacy of client or user, its identity and data present in the database is very essential. With the continuous growth in data concern about preserving the privacy of the data is also increasing. But to provide and assure privacy preserved access to the data still is in progress and yet needs more modifications. Several problems such as lack of transparency, disclosure, discrimination should be addressed.

Lack of transparency is attack in which the user is unaware of its own data of where its data is, who is using it, etc. This can be a major threat to privacy of user's data. Disclosure attack takes place while the information is being gathered in the database which is capable of disclosing the user's identity to others. Many related studies have only focused on a single level of privacy which doesn't seems viable in real time situations. Hazem Elmeleegy proposed a system using a single level of privacy which could lead to leakage of necessary information. In several applications the clients can set privacy of its data as local, public or private. In this system client can request for storing of data in database or can retrieve data from the database. The server is the one who authorizes the user if the user's id is present within the database and then shared based on the privacy level the user belongs to. A separate log module keeps track of the users data stored , accessed, who all accessed the data, who logged in ,who logged out, what is been uploaded and downloaded by whom.

II. METHODOLOGY

Data is an important asset. We have made a system for an organization called SARK that collects data, often concerning individuals, and use them for various purposes, ranging from scientific research, as in the case of medical data, to demographic trend analysis and marketing purposes. Organizations may also give access to the data they own or even release such data to higher authority. Because privacy is an important concern, for that we are using two levels of privacy modules.

One is Administrator it can be a system administrator, account manager and uploader who can add employees, upload files and documents. Hence it has given a Low-level privacy.

Another is Employee, where information are shared among authorized employees the uploaded file can only be viewed by admin following there different features.t has given High-level privacy.

The login Module is a portal module that allows users to enter a User Name and Password to log in. This module can be placed on any Module Tab to allow users to login to the system. Administrator has allowed employees to create accounts. The log module in the system keeps track of the employees data, and provides mini-feeds of these activities in blocks, it stores each transaction performed on the system. Such as logging in and logging out.

III. ARCHITECTURE

In this system we implemented a flow chart for a company called SARK".As the name suggest privacy preserving for that we have given Login Id and Password. So that certain information can only be shared with authorized users. In some situations where server need to allow the assessment to only authorized users. For that purpose serer needs identify the authorized users before it permits to share the information. User can be Admin or Employee. If entered user Id and Password is valid then users can access theirdatabase. Andsharing, Downloading and uploading processes of file can be done. And side by side log Module will be maintained to track all operation like logging in and logging out.

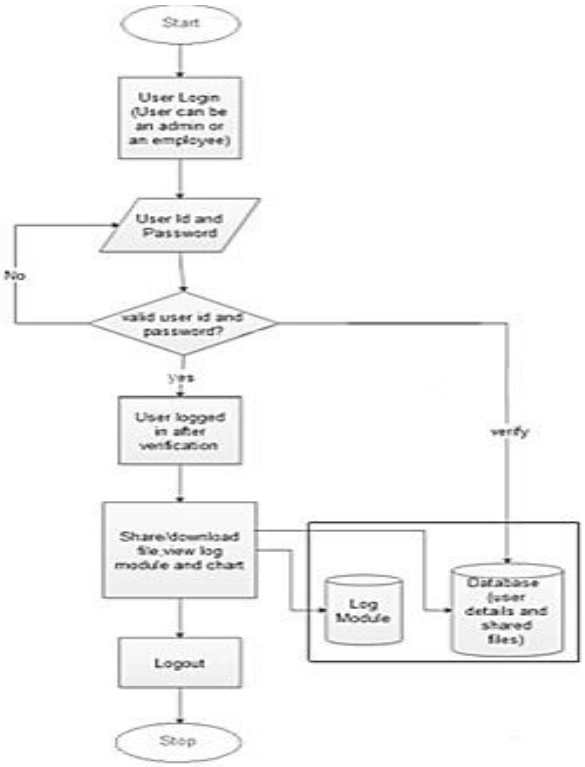

Fig. 1:

IV. SNAPSHOTS

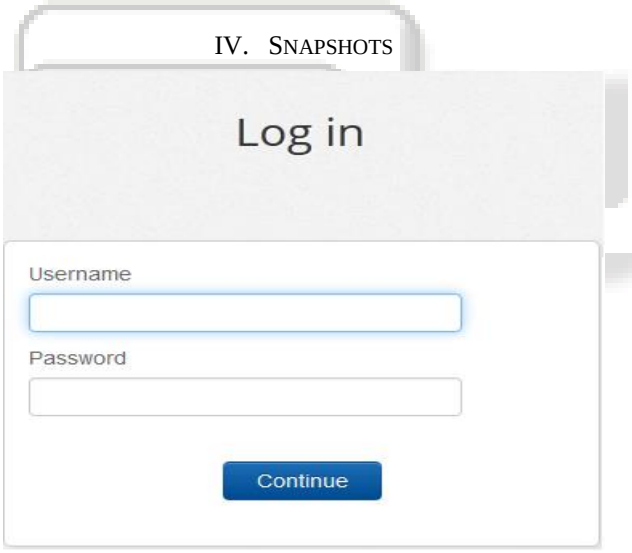

Fig. 1: Login

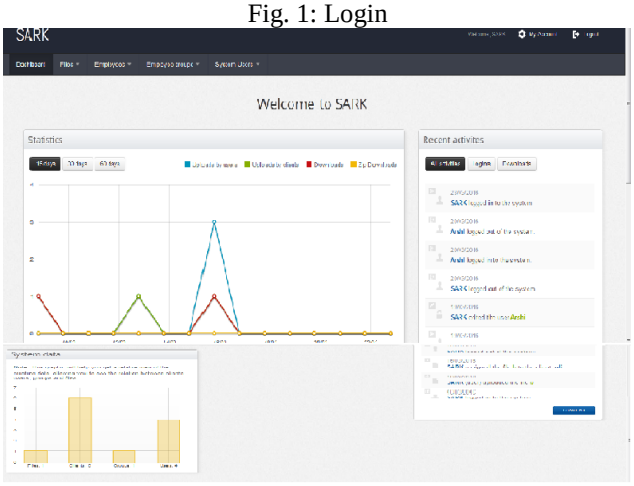

Fig. 2: Dashboard

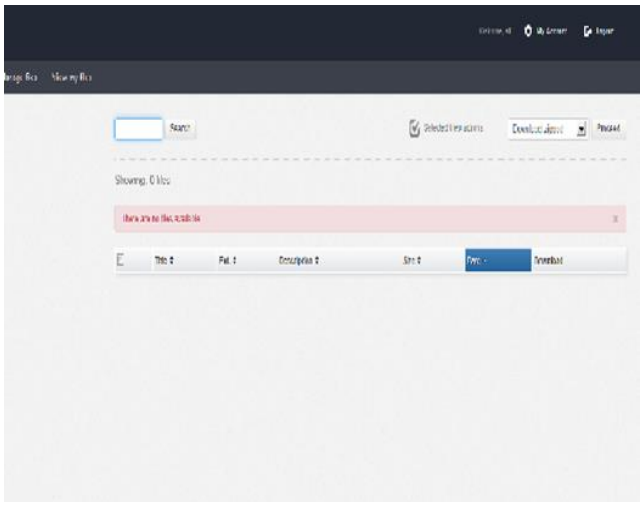

Fig. 3: Employee Login view

V. EXISTING SYSTEM

Existing studies focus on encryptions, several privacy levels, Role based access control etc.

Elisa Bertino proposed a work where it focus on only access control systems & disclosure, where the RBAC would fail to track the transparency occurring on database. There are applications where the client can set privacy to one's data to local, private or public. AbhishekShrivastav proposed a work which included privacy levels for personal data where scalable &cost-effective framework can anonymize large-scale data sets & manage data sets .Zhang proposed a where large-scale data sets could be anonymize using scalable and cost-effective framework and manage anonymous large data sets in a cost-effective and efficient fashion. Besmer proposed a system that allowed client to request the owner of the linked photo in which they are tagged in to hide it from certain people.

Tools that where designed traditionally could only analyze and manage huge amount of data.

The traditional security systems could not cover the whole of logs and events from a huge variety of systems ,though the system covered only a part of potentially relevant activity.

VI. PROPOSED SYSTEM

The proposed system is basically based on just data and data. Preserving those data from irrelevant access, i.e. preserving its privacy that may be transparency and disclosure is the real aim.

We have made this system for a company named "SARK", i.e. also the name of website. Personal details of employees within a company can be considered as its data. But here we focus more than just the employee's details/information. Owing to the working of any company there are various other important files, documents, charts, and memo and so on. So, we are making a system that preserves privacy of employee's data as well as all the other documents related to a company that is to be shared but also has to be preserved at the same time.

In the proposed systems, there are two levels or kinds users, one is an administrator (viz. system administrator, account manager or uploader) and the other is employee. There can be n number of admins and employees

based on the companies' structure. Depending on the two different levels of user the rights are given respectively.
SARK admin is a person who can add new employee as well as admin in the system, upload files or documents, make an employee activated or deactivated, allowing file download to system user or groups. SARK admin can add other admins like system admin, uploader and account manager. These admins also have the rights same as SARK admin. But, the only difference between SARK admin and other admins is that the log module can be viewed only by SARK admin. Yes, an admin can make groups of employees based on their designation or role in the company. An admin has a right to make user active and allow him to see the notification of recently updated data. Last but not the least only an admin can be able to view the bar chart, other graphs and also the log module. Log module shows all the operations performed within the system, each and every login, and logout and downloads.

Whereas, an employee have certain different rights. An employee upload files, but the uploaded file will only be visible to the admin, later on the admin decides that whether the file is to be shared with other users or not. An employee can also download the data which is allowed to be downloaded by the admin. An employee is added to group, for eg: sales, developer, trainee, etc.

We are also implementing an email integration which notifies the owner of any data through an email notification. This notification is send whenever a user downloads the data. This is all about the proposed system, i.e. Preserving Privacy Concerns of Database

VII. CONCLUSION

The proposed system efficiently & effectively provides privacy preservation to the database of the company, by providing different access levels to the employees in the company based on their designations and roles, it avoids the threat of disclosure. The files and the data stored are given privacy access levels, so that the data can be accessed by the authorized user only. The client's properties are stored to track the clients accessing the services The log module keeps the track of the activities done on the database and shows the dataflow in the system, which avoids the threat of transparency. The proposed system stills need to be hosted in private environment.

REFERENCES

[1] R. Agrawal, J. Kiernan, R. Srikant, and Y. Xu, "Hippocratic Databases," Proc. 28th Int'l Conf. Very Large Databases (VLDB), 2002.
[2] Borkar V, Carey MJ, Li C. Inside "Big Data Management": Ogres, Onions, or Parfaits. Proceedings of the 15th International Conference on Extending Database Technology (EDBT'12), 2012.
[3] R. Agrawal, A. Evfimievski, and R. Srikant, "Information Sharing across Private Databases," Proc. ACM SIGMOD '03, pp. 86-97, 2003.
[4] L. Kissner and D. Song, "Privacy-Preserving Set Operations," Advances in Cryptology—CRYPTO 2005, pp. 241-257, Springer, 2005.

