Implementation of Single Sign-On Technique in Heterogeneous Distributed Environment
Kirti Bhandari*, Parminder Kaur
CSE & Guru Nanak Dev University
India

Abstract— In a Distributed database system, the database is stored physically across computers or sites in different locations that are connected together by some form of data communication network. Distributed database security is to deal with protecting data from people or software having malicious intentions, from unauthorized access, modification and misuse of information or destruction. Most distributed systems are assembled from different components. Each of the component acts as an isolated security domain independently. In the multi sign-on environment, the end-user who wants to use services housed in different servers has to sign-on multiple times. User has to remember large numbers of passwords. With multiple sign on, user may have some bad habits that reduce the system security, such as, using the same password for all the systems. Therefore, multiple sign-on is very troublesome, so the single sign-on solution has been introduced to solve this problem. Single sign-on (SSO) is the mechanism whereby a single action of user authentication and authorization can permit a user to access all computers and systems where that user has access permission, without the need to enter. This paper implements the Single Sign-On Scenario in Distributed Heterogeneous Environment.

Keywords— Distributed database system, Database security, Single sign-on, Web Services, Facebook Connect services

I. INTRODUCTION

In a Distributed database system, the database is stored/spread physically across computers or sites in different locations that are connected together [3] by some form of data communication network. The main objective of Distributed database is Location transparency and Local Autonomy. Homogeneous and Heterogeneous are two main environments of distributed Database. In the former, the data stored across multiple sites is managed by same DBMS software whereas in latter, the data stored across multiple sites is managed by different DBMS software. When database is stored on multiple locations, security of Distributed Database is very important. The main security issues of Distributed Database describes by the following table:

Table1 A Matrix of Security Risks and Solutions [10]

<table>
<thead>
<tr>
<th>Problem</th>
<th>Solution</th>
<th>Security Technology</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unauthorized users</td>
<td>Know your users</td>
<td>Authentication</td>
</tr>
<tr>
<td>Unauthorized access to data</td>
<td>Limit access to data</td>
<td>Access control</td>
</tr>
<tr>
<td></td>
<td>Dynamic query modification</td>
<td>Fine-grained access control</td>
</tr>
<tr>
<td></td>
<td>Limit access to data rows and columns</td>
<td>Label-based access control</td>
</tr>
<tr>
<td></td>
<td>Encrypt data</td>
<td>Data encryption</td>
</tr>
<tr>
<td></td>
<td>Limit privileges</td>
<td>Privilege management</td>
</tr>
<tr>
<td>Eavesdropping on communications</td>
<td>Protect the network</td>
<td>Network encryption</td>
</tr>
<tr>
<td>Corruption of data</td>
<td>Protect the network</td>
<td>Data integrity</td>
</tr>
<tr>
<td>Denial of service</td>
<td>Control access to resources</td>
<td>Availability</td>
</tr>
<tr>
<td>Complexity to user</td>
<td>Limit number of passwords</td>
<td>Single sign on</td>
</tr>
<tr>
<td>Complexity to administrator</td>
<td>Centralize management</td>
<td>Enterprise user security</td>
</tr>
<tr>
<td>Lack of accountability</td>
<td>Monitor users’ actions</td>
<td>Auditing</td>
</tr>
</tbody>
</table>
By increasing the users of the distributed systems that should often access to remote resource, different authentication techniques are needed when users want to enter the systems. Therefore, SSO technology has been introduced as a special form of authentication mechanisms. This technology is meant to facilitate the job for users in a way that with one time authentication they could be able to access to several software resources on different servers.

II. RELATED WORK

In 1995, Parker [8] defined the various Technologies and The Products of Single Sign-on Systems. Scripting and Access Tickets are the two main approaches of single sign-on. In 2000, Lee and Chang proposed [4] a user identification and key distribution scheme to maintain user anonymity in distributed computer networks. Later, Wu and Hsu pointed out that Lee-Chang scheme is insecure against both impersonation attack and identity disclosure attack. Meanwhile, Yang et al. identified a weakness in Wu-Hsu scheme and proposed an improvement.

In 2004, Gang et al [2] proposed two designs of Single Sign-On and discuss its advantages and disadvantage of these two versions. In 2007, Suriadi et al [11] find out that there is a lack of built-in privacy mechanisms within the current identity management systems. They give a proposal for the extension of existing Federated Single Sign-On (FSSO) systems to adopt the beneficial properties of the User-Centric Identity Management (UCIM) model to provide an identity management system that allows the users to control and enforce their privacy requirements while still retaining the convenient features of FSSO.

In 2007, Maryam [6] et al demonstrates a centralized password-based authentication system using SSO for Web-based application in distributed environments. Centralised, Distributed and Federated Approaches are introduced and Cookie capabilities are used for implementation of this system that is called centralized cookie-based SSO or CCSSO. In 2008, David [1] proposed a framework for single sign-on by using an EMV card for two-factor authentication. Single sign-on by using an EMV card does not need the card making physical contact with the network connected device and without exposing the keys and PIN that are used to protect financial transactions. The proposed method could improve the protection for the card, the cardholder and the service provider(s).

In 2009, Magyari et al [5] proposed a single sign-on mechanism which is based on certificates generated on request for client applications. In 2009, Rajesh and Alwyn [9] discussed that several Single Sign-On frameworks were proposed and implemented so far but they are not balance in Security, Efficiency and Usability. Their proposed framework using Identity Based Encryption System (IBES) instead of Public key infrastructure (PKI).

In 2010, Moo Nam Ko et al [7] discussed Facebook Connect services which allow users to login to other websites using their Facebook identity and information and which will then potentially feed back to a users Facebook network information about their actions on the site. Facebook Platform allows users to import their identity, profile, privacy policy, social graph and content from Facebook to third-party sites.

III. PROPOSED SCHEME

In this scheme, user does not need to remember multiple passwords. In Single Sign-on, only one password is needed to log-on to different sites. In this scheme, data is distributed among Blog Answer and Single Sign-on Services. User first need to enter their personal information on Single Sign-on server. User's information is stored in SQL database. With this Username and Password, he/she log in to Social Networking Site and Blog Answer.

When the user sign in Blog Answer with Single Sign-on Services Username and password, user first redirects to single sign-on services server and finds user's information in their database. If user's data exist in the database then it will generate a authenticated key. With this key, user can log on to the Blog Answer.

The main steps when user log on to social Networking Site with single sign-on are:
1. User enter their single sign-on Email and Password and then click on sign-in. This information first strikes on single sign-on server and get all the necessary attributes but some attributes (Father Name, Landline Number, Photo) are not present on this site.
2. Single sign-on server requests the necessary attributes to the Blog Answer. Blog Answer find the attributes in their database.
3. Blog Answer sends the required information (Gender, Father Name, Photo) about user to Single sign-on server.
4. Single sign-on Services generate an authenticated key to Social Network Site and providing all the information about the user from a Blog Answer. User can log on by getting authenticated key and provided information can easily seen through User's profile on Social Networking Site. Data is only accessed through Web Services.
IV. IMPLEMENTATION

User made an account on Single Sign-On services by giving all the information like username, password, Email id, DOB, Address, Mobile No. but username, password, Email id are unique fields. This information is stored in SQL database. All the required fields are shown by * mark. After filling this sign up form, they have to click on sign up button.
After making an account Single Sign-on Services, user fill up the sign up form on Blog answer. All the data stored in Oracle database. User fill the form with same Email Username and password as single sign-on service.

User sign up successfully after filling above form by hitting Sign up button.

When user fills the Sign up form on Blog Answer, they have two options for log in. They can log in both cases because they have filled signup form also. By login using single sign-on, they can log in through same username and password which they have fill on single sign-on services.
A profile is created on Blog Answer which contains all the user information like Father Name, Address, Gender, DOB, Landline No, Photo. Landline No and Photo is blank because user does not provide information about these fields during Sign up form.

![User Profile on Blog Answer](image)

Fig. 4.6 User's Profile is shown on Blog

Now, user can easily add a question, view a question, change password and edit profile in Blog Answer. They can easily add a question by typing the question and select the category from which it belong. Then click on Add Question button. They can easily view the added question by pressing View Question link. User can successfully log out from Blog Answer account by clicking on log out button.

When the user wants to visit social networking site, they have two options for log in. Either they can log in through using Single Sign-on account or made a separate account on social networking site.

![Log in to Social Networking Site](image)

Fig. 4.7 Log in using Single sign-on on Social Networking Site

User can make an account by providing all the information on Single Sign up form. Through Sign up on Social networking site, they have to fill all the required information which is a lengthy process.
Log in using Single sign-on account requires only Single Sign-on username and password. By clicking on Sign in button, user redirects on Single Sign-on services site and find out the typed username and password exists in the database. If it exists, then Social networking Site retrieve all the required information from Single Sign-on database and some information about user is not present in this database like First name, Last name, Landline no. and photo. then it redirect the user to Blog Answer and find all the information to Blog Answer. Then user successfully log in to Social networking site and profile is created by accessing remote data.

User can make new friends, share status and update the profile. When user wants to leave the account, they can leave by pressing log out button.

V. ENCRYPTED PASSWORDS

To secure the password in database, password must be stored in encrypted form. The proposed scheme uses MD5 hash Algorithm. The message-digest algorithm is a widely used cryptographic hash function that produces a 128-bit (16-byte) hash value. An MD5 hash is typically expressed as a hexadecimal number, 32 digits long. It is an updated version of MD4. It is mainly used for storing small passwords.

There is MD5 Encrypter which is used for encoding the passwords, change the readable password into unreadable text. It is used to ensure the data integrity of files. The MD5 hash algorithm always produces the same output for the same given input. When a user enters their password, the system computes the hash of it and compares it to the hashes listed in the database. Data stored on database can be viewed as following snapshot:
Theoretically, it is impossible to convert encrypted text to original text. But some decrypters convert encrypted text to original text. The main advantage of using MD5 is fast and easy to use. It also ensures security if attacker attacks the system, it will not be easy for them to decode the password stored in the database. Sometimes collision also exist i.e. two different data produce the same hash. An attacker can create two colliding files that both begin with the same password.

VI. CONCLUSIONS & FUTURE WORK

Sign-on in centralized environment, user can only retrieve information from centralized database i.e. all the information about user is stored on single site. All third party websites requests on Single centralized database about user's information. Load increases on this centralized site when number of sites increases and they want to access user's information on this site. So, response time decreases and performance also degrades. Security is also increased by using same password for multiple sites. There is no need to write down password in paper or any other means. They can easily remember one password for login to multiple sites. Data is stored in encrypted form by using MD5 hash algorithm. It converts the typed password into hash value. It is theoretically impossible to recover the original text from given hash value. Future work includes the feature of "Auto-Update". Updating the data at one site will automatically update the data at other sites. It can also save a lot of time of the user and maintain consistency.

References