Abstract:

the present study discusses data security management in service provider/client systems and distributed systems and the critical situation of secure access. In this paper, data security management in distributed systems has been suggested in the form of explaining security systems, examining their weaknesses and providing appropriate solutions. The following is a summary of concepts such as authorization, documentation, encryption and access control which are the main topics in data security of distributed systems. In line with the discussions above, a new method is proposed for secure access based on service provider/client architecture mechanized with security applications. The model describes a secure access server and a user relationship. This study is a heuristic approach in the field of data security management for distributed systems regarding exclusive security access of clients. Given the increasing importance of secure access in distributed domains, considering the various issues associated with this sign, thus, the present study introduces application and theoretical problems.

Keywords: Distributed systems, security management, access security.

1. Introduction

Concern of every organization in the world is recently data security against potential attacks. In every enterprise, systems are intended to establish security in order to prove their ability to prevent attacks on the availability, integrity and reliability of the proven [7].

Security is a complicated problem in development of computer networks and personal computers. Currently, the relationship between local networks and the relationship between small and large computers are identified as an application [1]. Applications are considered as a single system. In fact, any application or any computer can have access to the entire system including different computers and storage devices [6, 20].

Unfortunately, most companies and organizations do not pay attention to the issue of data security until a report of hole in the network. A suggestion is to establish a sound system of security on the network to do its task which is warning when security attack occurs. This issue is along with a few tips: 1) identifying security risks, 2) a significant declaration 3) educating the users for awareness system [16].

1.1. Distributed Systems

The most important part of distributed systems is their intersect point with data which is the heart of organization. This is only managed by maintenance and development team of the organization called as the technology development.

In some cases, a network of independent computers in different organizations under different management and service providers forms a distributed system. For example, it can be organizational network relationships in a large organization with multiple divisions and departments [14, 9].

1.2. Client Server Systems

Typically, distributed systems allow users to use the data and applications even from miles away without identifying networks and their relationship.

In current distributed systems, the concept of distribution is divided into two parts:
1. a user interface and a kernel on one or two applications called as clients
2. Database management and a part of active applications on other systems introduced as a service provider

According to this classification, a component in the network may include a component which is the most useful one. Applications are connected to each other by an important part which is a utility with the task of transferring data between the server and the client. One client system/service-provider application is highly flexible; so that, it allows the user to access the database of multiple networks with support for high graphic interface. This access is not available at the Central Processing System [5].

1.3. Data Security Management- Main Problems

Unfortunately, the development of data management in distributed systems has coincided with the development of computer networks. This development causes problems such as security-sensitive parts of the network [11, 4, 8]. The mechanism of some manual and non-automatic systems is that the user is prompted to enter a User ID and password. This approach not only makes the system inefficient, but the trend and safety approach of the system is revealed. Users may even record their password on the part of the paper in their office in the organization to remember the password. Most users often do not use one password for all current accounts.

1.4. Computer Security Components in Distributed Systems

In distributed computer systems, there are 4 main contracts for security system components [17,18,19]:

1. Document Security
2. Authorization
3. Access control
4. Encryption

**Document Security:**

Document security is usually a ‘smart sign’ in the size of a small, handheld device or a credit card. The device automatically generates a password which is delivered to the ‘checking server’. Checking server is connected directly to the network.

**Authorization:**

The purpose of this section is to allow users access to resources that are approved by the administrator. Authorization criteria is assessed by the service-provider application. According to this assessment, client computers are permitted to operate and identify the user as a service-provider system. Hence, it creates the local security without sending information throughout the network.

**Encryption:**

Encryption implements complex algorithms such as DES-PGP-RSA based on confidential-public key.

**Access Control:**

Access control monitors the access lists and the list of features. This approach specifies the accuracy of the contents available in the database for the user access.
1.5. Aspects of Data Security in Client/Service-Provider System

From an administrator's perspective, the following potential threats may occur for a client/service-provider system [24, 10, 15]:
1. Evaluation mechanism of user workstations may be very small or absent.
2. It is possible to face the automated logging process.
3. Workstations may have limitations, for example, they may be installed in public places, or where the risk is great.
4. Workstations may take advantage of hardware and powerful tools; hence security systems are likely to be ignored.
5. In most cases, a user may pretend to be another user to penetrate the system. As was discussed earlier, security requirements of distributed systems is completely different from requirements of client/service-provider systems; therefore, the process is more difficult to implement. According to Figure 1, this concept is obvious.

![Figure 1: distributed security approach](image)

2. A Model of System Access Security

An efficient system access security is described here on a local network, along with a number of stations and users.

In general, our proposed model is suitable for systems in which users use a high number of queries and transactions, such as update, cancel and add. This operation is based on access and user behavior toward database. For example, we can use information from a database [22, 12, 21].

The system includes a large number of tables in a query and banking transactions managed by an employee in a branch. Localization of transaction and users takes place in a hierarchy: the director, the deputy, local director and staff or based on a hierarchy of money in the bank: currency, security, current accounts.

In a bank, an employee can only access current account information and their transactions. This is when all other transactions have closed on him. In this paper, we present a model as a perfect solution to solve this problem.

The proposed model includes two main characteristics for safe access: eligibility and authorization. Eligibility of a user is very important and it is again developed in a hierarchical mode. For example, eligibility and the core agency are initially with the bank chairman, then president, followed by the rest of the staff. However, authorization means localization of authorization to each user with respect to activities in an area that is in line with the objectives of an organization. For example, a special authorization is given to users of
currency, current accounts and security in a bank that is limited to users in that field. Given the scope of the model, it includes cases such as users who work in workstations as well as transactions which may occur.

2.1. Software Architecture
Our model is based on the client/service-providersystem as shown in Figure 2. Access security of serving software is considered at each network station as an independent application [2, 23]. Each of the applications or clients will receive access security services through a unified user interface when needed.

![Figure 2: software architecture based on server/client system](image)

The operating environment for OS/2, Windows or NT systems are programmed with few changes. Communication mechanism between the user interfaces on a part of the client system with the server software is called PIPE. The term is derived from a method to transfer data from one computer process to the other processes. The most striking feature of PIPE is utilization of the queue FIFO (first in, first out). The first data renewed on the PIPE is the first data read through that.

Access security system provides conditions that users face with a number of transactions on their workstations. Per a transaction occurring in the system, a security label will be defined with two main symptoms: 1) security level 2) types of security. Authority system gives the highest level of security access to a station and it will consider the highest level of security access for the user. To better understand this, we will refer to Figure 3.

3.1. The Basic Rules of Security

Some basic rules should be established for access comprehensively, but some of these rules are optional [3, 13, 25]. Among the basic rules, we can mention the following:
1) All users can connect to the workstations even if their approved access level is less than the limit defined in the system.
2) Facing a transaction in the system, a condition needs to be provided that does not reduce authorities of the transaction. A workstation must have the best service per transaction.
3) Facing a transaction in the system, a user must have sufficient authority and does not reduce the authority of a transaction.

3.2. Services Evaluated by the System

The proposed security system provides services for a number of client applications which can provide relatively good access security. In addition to the server, a backup copy is provided of any services. A serial number of service and customer demands as shown below is demanded from the system. At the following, you can see specifications of the access security services:

- Staff
- New employee profile
Layered design [26] is a technique by which very complex programs can be developed in a hierarchical form. Each layer has a functional interface which provides an operation in the layer. It is also possible to add stronger layers to the upper layers. The downstream layers should be evaluated in each instance. In the following, it can be noted that the layered system has a very strong framework. This property measures the relationship between two independent programs in the system. The relationship between the two programs may be implemented in a single layer. Below, see three important factors in forming the foundation of a layered system:

1) Each parallel layer in both server and client system jointly provides a service. The protocol specifies how to divide the work, the general format of messages and transactions.
2) Each layer is made by its substrate. System interface specifies how each layer requests or receives from the lower layer. User interface is clearly hidden from the lower layer and keeps all details hidden. It is also responsible for giving a series of services.
4) In the upper layers, the task of layers is the easier. For example, the lowest layer is responsible to access the hardware resources in the system. While the purpose of the topmost layer is to examine access as well as to transfer files.

Our proposed model used layered design system to create an active security structure with client/server approach. In this model, the server system is capable of storing all kinds of data with particular goals. Data such as documents, images, video and audio files and... . The layered mechanism of security system in client/server program includes three parts: the application layer, exchange or conversation layer, communication layer

4.1. Application Layer

A part of a client in the system is the communication layer. By definition, the communication layer is a program requiring data security services by a distributed active approach in each service in the upper layer. Application of the application layer in the client system ends to sending staff profile service, object profile, validating staff etc.

The application deals with customer demand, file path, qualified users, checking the password, changing the password and staff profile.

4.2. Conversation Layer

This layer represents the application logic of access security. This layer, as a part of a server, is responsible for analysis of the requests sent by the client, identification of the requested service, preparation of the suitable parameters in the case of transactions and reference to the application layer to examine what requests will be performed against transactions.

This layer, as a part of client, is also responsible for composing a message including all required details and giving it to the server. For example in a request with the purpose of examining the user password, this layer is responsible to prepare profile of that user; it also encrypts the password and adds the required details. Once the request is made, these details will be transferred to the communication layer.
4.3. Communication Layer

This layer is responsible for transferring data between processes. If the server and client are both on a computer, the connection will be made via Pipe IRC. If the server and client are on two separate computers, they will be connected through a protocol on OS/2 based on LAN. Communication layer is an integrated layer which can work with Pipe, Netbios, TCP/IP and Appc/CPI.

4.4. Architecture of Access Security Software

Access security server includes some layers and parts communicating a large number of software.

- Communication Layer: Communicating with face to face customers, receiving messages and sending replies.
- Conversation Layer: Identifying and evaluating incoming messages from customers based on different message. This layer also creates a response box to customer requests.
- Application layer: administering three pillars including: handling requests for services from users (specifications, reviews, cleaning), handling the requests based on stations and handling the demand based on the transaction service. Figure 4 shows a schema of the software architecture of the access security.

4.5. Conversation Layer

This layer is responsible to analyse demands sent by the client. Tasks of this layer include identifying the demanded service, examining that the request is legal (or the user access level, stations through which users
send their messages or the demanded domain). In the case of problem or failure to send a message, this layer sends a message involving unacceptance to the user (as Figure 5 shows). This layer also evaluates factors or parameters sent for a demand in a transaction by the application layer. Once the demand is made by the access security port of the application layer, the conversation layer starts to compose a message which needs to be sent to the client application.

4.6. Server-Side Application Layer

The server-side application layer implements access security for server transactions. Inputs in this layer include high demands by the client; in addition, the outputs include messages involving information demanded by the client.

5. Conclusion

Concerns of corporate executives against possible intrusion to the system can be reduced by providing proper solutions. A new and innovative way is to implement access security models. The model presented in this study is a unique security model in client/server system. Currently, there are many proposed models implementing access security; however, no model considers all security aspects in the client/server system. Although the proposed model in the present study responds to four security components of the distributed systems: 1) security credentials, 2) authorization, 3) access control and 4) encryption. However, the security requirements in distributed systems is quite different from the concentration requirements on a system. This model suggests a particular structured solution using the efficient PIPE software, a layered security model and the triple-queue software architecture. Several experiments on different services show the availability of our proposed model. It also emphasizes on the access security. Implementing our proposed model, the administrators of the vast local networks with large number of users and stations provided a better understanding of concepts on service classification, password exchange and authorization of users and stations.
Figure 5: conversation layer

References