CHAPTER - 5 MIS Security Architecture Model:

Baidynath Company secures the database involving both policies and mechanisms to protect the data and ensure that it is not accessed, altered or deleted without proper authorization. Security measures taken by the company is as follows:

1) Database Security
2) Network Security
3) Operating System Security
4) General Security.

Fig.No. 11 Baidynath Company Data Security Layers
5.1 Database Security: So far as the Baidyanath company
database security is concerned, it is based on the S/w's used by
the company. Baidynath Uses

Front End: Oracle

Back End: Developer-2000

Platform: Windows-NT

The Oracle includes two independent mechanisms for
database security namely authentication, authorization. The
authentication subsystem requires to supply a username and
password. The authorization subsystem assigns system and
object-level rights and specifies the activities that various
users may engage in. Oracle's powerful view mechanism is
the part of its authorization subsystem. The authentication
mechanisms permit to log on to the Oracle system, while the
authorization mechanisms permit to share database objects
(tables, views, and so on) and allow the DBA to assign
system-wide privileges.
The authorization subsystem allows DBA users to grant and revoke privileges to other users with SQL statements `GRANT` and `REVOKE`. The decisions about which users are granted what privileges are company policy decisions that are merely enforced by Oracle. Oracle ensures that accesses to the RDBMS are always checked against all the authorization constraints it stores and maintains. Oracle maintains two levels of groups of privileges: system privileges and object privileges. System privileges refer to the `CONNECT`, `RESOURCE`, and DBA privileges granted to users by the DBA. The privileges classes determine whether a user can log on to Oracle, whether or not a user can create objects and whether or not a user can authorize others to log on to Oracle.

Object privileges provide detailed control over database objects (tables, views, and so forth) once a user logged on to the Oracle systems. Enforced with object privileges, views allow the user to control table access down to the level of selected columns of selected rows of a particular table.
Object privileges determine what user may do at that level -- whether user may merely "see" a value, alter a value, or create a new value and insert it into a table.

Users can also be granted different object privileges from the seven possible: ALL, SELECT, INSERT, UPDATE, DELETE, ALTER and INDEX. Further Baidynath data security system also covers how to use views in tandem with granted privileges to secure a database by restricting access to specified columns or rows of particular tables.

5.1.1 Changing The Superuser Password:

SQLPLUS SYSTEM/MANAGER

SQLPLUS GRANT CONNECT TO SYSTEM IDENTIFIED BY SHERLOCK;

This changes the system's password to SHERLOCK.

5.2 Network Security: Since the company is working on the homogeneous distributed database system and each department has its own computers connected through LAN is connected with each other by the LAN hence to protect the
data in LAN environment is very important because data in a network is held in a common storage, and anyone is authorized to use the central storage.

The best solution to this potential problem taken by the company by storing the data in an encrypted form then any unauthorized person accessing the file would not be able to read its contents.

An encryption key is used for coding and decoding a message to protect the data from unauthorized users. Keys are basically distributed to authorized users.

Fig. No. 12

Fig. No. 12 depicts the company encryption process when the data is running onto the N/W it is automatically changed to meaningless information called as Ciphertext. Upon reception the ciphertext is transformed back to the original
plaintext by using a decryption algorithms and the same key that was used for encryption.

Network Security Techniques used in Company.

1. LAN Security cannot exist without a management policy.

2. LAN users is positively identifiable before they can access to network resources.

Prevention: passwords, passkeys authorization measures.

3. Data, hardware and software is protected from unauthorized and/or accidental modification, destruction, theft or disclosure.

Prevention: locks

4. Data is reconstructable.

Prevention: Frequent, regular backups of files.

5. Equipment is protected from fire, dirt and natural disasters.

Prevention: smoke detectors, sprinklers, airconditioning.
5.3 O/S Security: The DBA of company has also applied the O/s security techniques to the system is as follows:

5.3.1 Personnel Identification: Since the systems are running on the LAN environments which presents some additional security problems because of its dispersed nature and because many people have access to the network. This is the operating system which identifies the user's identification: personal, such as ID badge; key word such as log-in name and password; or key number.

- Passwords: After logging onto to the network, the user of company has to type a password; Theoretically if users give a password, unauthorised access is prevented.

- Security in Log-in: Password is not displayed back to the screen during log-in process. The no of times a password can be attempted of the company network systems upto three times only then after the log-in name is invalidated temporarily and the network supervisor notifies of a failed log-in.
5.4 General Security:

5.4.1 Human Factors: At the outermost level are the human factors, which encompass the ethical, legal, and societal environments. The company depends on these to provide a certain degree of protection. Thus, it is unethical for a person to obtain something by stealth, and it is illegal to forcibly enter the premises of an organization and hence the computing facility containing the database.

The Baidynath company performs some type of clearance procedure for personnel who are going to be deal with sensitive information, including that contained in a database. This clearance procedure is a very informal one, in the form of the reliability and trust that an employee has earned in the eyes of management or DBA.

The DBA is responsible for granting proper database access authorization to the user community. Inadvertent assignment of authorization to a wrong class of users can result in possible security violations.
5.4.2 Physical Security: Physical security mechanisms include appropriate locks and keys and entry logs to computing facility and terminals.

Security of the physical storage devices within the company and when data is transmitted from one location to another is maintained. Access to the computing facility is guarded, since an unauthorized person can make copies of files bypassing the normal security mechanisms built onto the DBMS and the operating system.

Authorized systems from which database access is allowed is physically secure, otherwise unauthorized person may be able to clean information from the database using these systems.

User identification and passwords is kept confidential, otherwise unauthorized users can "borrow" the identification and password of a more privileged user and compromise the database.
REFERENCES


5.4.3 Administrative Controls: Administrative controls are the security and access control policies that determines what information is accessible to what class of users and type of access is allowed to this class.

The administrative control procedures are the implementation of security policies to provide protection, external to the database, operating systems, and computer hardware. The company administrator has chosen the security features provided by the DBMS to adequately implement the security perspectives.

Since the homogeneous distributed database system is used by the company and then hence chosen the administrative or DBA as security administrator and the access control policy is chosen by the DBA as closed system hence a user is not allowed to access any thing unless access is explicitly granted.

5.4.4 The Floppy diskless PC: To secure the data from external virus or program used by the unauthorized or
authorized user accidentally or knowingly the company has removed all the floppy drives from all the systems except one and CD drive is also attached to one of the system to restore the data if required any time.

5.4.5 Protection Against Cable radiation: Since the information is moving through cable, it should not be intercepted by the unauthorized user hence DBA has protected it by putting out of sight through underground fittings.

This is the power of the security systems used in the company makes the company in more beneficial position.

5.4.6 Management Level Concern:

Fig. No. 13
Fig.No.13 depicts Good security usually reduces case of access to the computer. Managers must weigh the trade offs between convenience and security when implementing a specific systems.

Since company is using the Oracle as front end and developer-2000 as back end. Data is secure Three levels of defense are made for Database security: human factors, physical security, administrative security and the security and integrity mechanisms built into the operating system and the DBMS.

5.4.7 DBMS and OS Security Mechanisms: The database of the company also depends on some of the features of the OS for security perspective.

- The proper mechanisms for the identification and verification of users. Each user is assigned an account no and a password. The O/S ensures that access to the system is denied unless the number and the password are valid. In
addition, the DBMS also requires a number and password before allowing the user to perform any database operations.

- The protection of data and programs is done by the OS both in primary and secondary memories. This is usually done by the O/S to avoid direct access to the data in primary memory or to online files.

The DBMS has the following features for providing security and integrity: mechanisms to support concurrency; transaction management; audit and recovery data logging. In addition, the DBMS provides mechanisms for defining the authorizations for the user community and specifying semantic integrity constraints and checking.
5.5 Access Control by Pictorial Representation:

![Diagram of Client/Server Architecture](image)

**Fig. No. 14** Client/Server Architecture (Three-tier Architecture)
Baidyanath Data processing system security

5.6 Conclusion: Baidynath data security levels guard against accidental or malicious tempering with data; integrity ensure that any properly authorized access, alteration, deletion or insertion of the data in the database does not change the
consistency and validity of the data. Baidynath data security system also covers all aspects of database security provided by the Oracle. More importantly, it covers the authorization subsystems which allows the user to grant and revoke both system-and object-level privileges within Oracle. Various users can be granted varying levels of the system privilege-from the limited CONNECT privilege to the more flexible RESOURCE privilege to the most powerful DBA privilege. Users can also be granted different object privileges from the seven possible: ALL, SELECT, INSERT, UPDATE, DELETE, ALTER and INDEX. Further Baidynath data security system also covers how to use views in tandem with granted privileges to secure a database by restricting access to specified columns or rows of particular tables.
CHAPTER 6: Conclusion & Future Work

To summarize, the role of computers for reducing the uncertainties occurring in organizations, this thesis comprises theoretical as well as practical approach. According to literature survey this research work shows how computers are used as a tools, as machines, as weapons and as channel to reduce the uncertainties like incompleteness, irrelevance, indeterminacy and incommensurability to support the MIS.

To find the practical evidence of the existence of the paradigms and metaphors used in literature survey - A Baidynath Case Study is made. Benefits found in computer based MIS is time saving, data sharing, data security is maintained and cost benefit analysis is made to support the MIS to take the effective decision. Baidynath computer based MIS provides the desired information available in the right form at the right time, supply the desired information at a reasonable cost, keep the information update, store important and confidential information properly, increases the
productivity and efficiency, regularize and maintain disciplinary systems of work.

Hence it can be concluded that computer has power to reduce the uncertainties that organizations faces. Based on the topology of uncertainties developed, this thesis proposed that computer can reduce specific type of uncertainty occurring in organizations.

Since the Baidynath company is presently working under the homogeneous distributed system to support the company MIS to take the better and timely decisions. Each department has its own group of computers having the same o/s and the RDBMS packages to execute and share the data. The system is running into the distributed data processing environment. Company's database is the relational database.

In future the Baidynath can use the heterogeneous distributed system. Each department of the company can use different type of O/S and RDBMS packages to execute the queries required to support the Baidynath MIS for taking
effective decisions and then company can use the online analytical processing (OLAP)- through which company can generate summary tables with multiple combinations of dimensions. Basically an OLAP server is connected to the databases or data warehouses server at one end, and to the user's computer at the other. Multidimensional database can also be used in future.

In future the Baidynath company can influence the environments, altering their product or service mix, changing the relationship with outside partners and customers and even can change the rules of competition in their company by using the internet services. Baidynath Company can directly access their final customers, bypassing traditional intermediaries or depots centre, and collecting a wealth of information about actual and prospective customers. Baidynath can redefine their traditional environments by using their web sites on the internet.