ENHANCING DATABASE SECURITY AND INTEGRITYFOR EMPLOYEES IN AN ORGANISATION

A CASESTUDY OF MUKWANO INDUSTRY, MAKINDYE DIVISION.

BY

NANTANDA IRENE ROBINNAH

REG NO: BIT/17526/71/DU

AND

MASABA RITA

REG: BIT/16734/71/DU

A RESEARCH PROJECT SUBMITTED TO THE SCHOOL OF COMPUTER STUDIES IN PARTIAL FULFILMENT OF THE REQUIREMENTS FOR THE AWARD OF A DEGREE OF BACHELOR OF INFORMATION TECHNOLOGY OF KAMPALA INTERNATIONAL UNIVERSITY

JUNE 2010

DECLARATION

We Nantanda Irene R. and Masaba Rita hereby declare that this graduation project is our original work and has never been submitted to any university or institution for an academic award.

Any similarity to any other project is therefore a coincidence of ideas.

Signature.....Irene.....

Candidate Nantanda Irene Robinah

Date 03./..07.../..2010....

Signature.....Rita Masaba.....

Candidate MASABA RITA

Date 03./..07.../..2010.....

APPROVAL

This is to certify that this research project entitled "Enhancing Database Security and Integrity for Employees in an Organization" was conducted under my supervision and guidance and is now ready to be submitted to the school of computer studies with my approval.

Signature……

Mr. CHEMUTAI GILBERT

Supervisor

Date 28th/06/2010

DEDICATION

I Irene dedicate this research project to my dear parents for all their effort they offered me both morally and financially. And to Mr. Kennedy Patrick and sue Kennedy for their financial support.

I Rita dedicate this research project to my husband Van nick, for his financial support and my children Collin, Mark and Faith.

ACKNOWLEDGEMENT

The following are individuals whom I know have greatly influenced me in the process of this research project; we wish to extend our heartfelt thanks.

We are grateful to the Almighty God for giving us good health, wisdom, intelligence and the ability to carry out studies as well as coming up with this project successfully.

Special thanks to our supervisor, Mr. Chemutai who has worked tirelessly with us to finish this research project. Mostly for the time he took off his busy schedules so as to attend to us, the advices he offered in order to make this research project a success.

TABLE OF CONTENTS

LIST OF ACRONYMS

FMCG	Fast Moving Consumer Goods
RBAC	Role Based Access Controls
DBA	Database Administrator
DBMS	Database Management System
SQL	Structured Query Language
EFS	Encrypted File System
EKM	Extensible Key Management
TDA	Transparent Data Encryption
RAC	Real Application Clusters
PIT	Flashback Database is a new approach to point-in-time

ABSTRACT

Database security refers to protecting the database from user operations that, by their nature would compromise the integrity or security of the database. Some off these problems are caused by user carelessness for example; a user update leaving the database in the state violates one of its integrity constraints. Other problems are caused by malicious user behaviors, for example, a user accessing information he/she is not authorized to obtain; or even modify data with malicious intent

In Mukwano there was a problem of careless scheduling of concurrent database accesses especially when two or more users attempt to access or change the same data. As a result of such problems, user actions perfectly legitimate in their own right might have unlimited consequences, leaving the database in a state inconsistent with reality. Because of such problems, we used the two modes that is windows authentication and mixed mode which has both windows authentication and SQL server authentication. It is emphasized that, with windows authentication, there is no need to have to specify a login name and password, to connect to SQL Server but instead, access to SQL Server is controlled by Windows operating system or the group to which a particular account belongs. With SQL server authentication it is only the database administrator to make changes to the

Database using login as seen in chapter four.

CHAPTER ONE
INTRODUCTION

.0 General Introduction

According to Wenyang (2005), Database security begins with physical security for the computer systems that host the DBMS. No DBMS is safe from intrusion, corruption, or destruction by people who have physical access to the computers. After physical security has been established, database administrators must protect the data from unauthorized user and from unauthorized access by authorized users.

This is an indication that if data is not protected it brings about database crime and biased tendencies.

.1 Background of the Study

R.Elmasri and Navathe, (2003), emphasize that, most of an enterprise's most sensitive and valuable information resides in databases. Yet, in many organizations, database security is often neglected, misunderstood, or even ignored.

This study discovered why databases have become one of the most popular targets for unauthorized users and hackers as well as established how everyday mistakes in database administration contribute to these unauthorized accesses and attacks in order to offer necessary advice on what can be done by the organization to protect its most critical data as well as stopping hackers in their tracks.

With the extensive use of database systems nowadays, everyone is prone to become a victim of database crime, and a single database crime event might even result in a serious consequence on individual or public affairs. Because of that, database developers are always trying to create new techniques to prevent unauthorized, unanticipated or unintentional disclosure of data from happening. No matter how good a security measure or technique is, database administrators always play a very important role in database securities issues. In addition to user account management, database administrator also contributes to developing security policy and enforcing the security-related aspects of a database design. But at the same time, advanced algorithms and technologies used to

increase database security also raise challenges to both database developers and administrators. While databases with inference control, access control, encryption, etc. have become more and more complicated for developers, which will necessitate DBAs to acquire more knowledge to become qualified in the future. (Farrar, 2005).

.2 Background of Mukwano Industry

Mukwano Industries (U) limited was established in the early 1980s with intent to become the supplier of choice for Fast Moving Consumer Goods in East and Central Africa as well as ensuring timely delivery of quality, affordable products to its customers. The industry is located on Mukwano road, a few meters from the Centenary Park. The industry currently employs 6000+ personnel including 100+ functional experts and it has evolved to be one of the fastest growing fully integrated manufacturers of FMCG products with a clear vision to provide superlative products at affordable prices accompanied by unparalleled service levels across the region through which the industries have attained enviable brand loyalty across the great lakes region and command large market shares. The company is committed to maintaining a dynamic integrated Quality and Food Safety Management System that drives business growth, meets the changing needs of customers, employees, suppliers, regulatory Authorities and its Board and because it's driven by the value of integrity of its employees, the employees are treated as an asset because they positively contribute to its growth. Mukwano Group of Companies is committed to creating a workplace that values differences and provides channels to report concerns and has therefore invested to ensure that its employees, the environment as well as facilities are protected.

The Industry relies on a DBMS to execute its duties which system is without a fully protected database from unauthorized users. The insecure data storage system affects employee's privacy and therefore does not enhance their integrity in this organization. It is therefore upon this background that there is a realized need to enhance a database security to promote integrity of employees in order to control the problems experienced in an unprotected database system.

.3 Statement of the Problem

However databases need protection to control the manipulation of information stored therein by unauthorized users which can be done through database security. While most security pros have become painfully aware of the threats posed to their organizations' databases, many of those who create and maintain the databases still don't fully understand the danger. This "security primer" is designed to open the eyes of the DBA to the risks posed by poor database security and to current "best practices" that can help prevent those risks from becoming reality.

It is crucial to note that, there is a connection between database security and integrity of the employees which relationship is not well defined in Mukwano Industry and the confidentiality of the employees is not fully managed reducing employee openness and freedom and affecting informational reports which are of a confidential consideration due to unprotected databases. However, enhancement of a protected database security can be pursued to improve on the integrity of the employees in Mukwano Industry in order to improve on employee integrity and do away with data manipulation practices.

.4 Objectives of the Study

.4.1 General Objective

The general objective of the study was to develop a database security to improve and build employee integrity in Mukwano Industry.

.4.2 Specific Objectives

i) To investigate the need for database security and how it can boost employee integrity.

ii) To investigate the effect of unprotected data on employee integrity in Mukwano Industry.

iii) To develop a database security system that will protect access of data by unauthorized users in Mukwano Industry.

iv) To test system to approve its applicability in data protection.

.5 Scope of the Study

The study was carried out in Mukwano Industry and was restricted to; unauthorized retrieval of data and its effect on employee integrity in order to develop a protected database to promote employee integrity as well as test the system to prove its applicability relying on systems administrator and Human resource Manager.

.6 Significance of the Study

When this study was carried out, it contributed sizeable knowledge and discernment on shortcomings of an unprotected database and has thus availed useful information to different practitioners, database managers and Ministry of Industry and Transport, on issues pertaining to data security systems and the relevance of safely securing data through provision appropriate protection measures of the database.

The study improved the employee integrity, their productivity, performance as well as satisfaction to reduce manipulation of data which can result from an unauthorized access as well as improving on the position of the industry when it relies on more accurate data free from manipulations.

The study is likely to play a positive role towards mukwano industry by providing a resourceful, competent and accurate application of a secure database by reducing employee tendencies to manipulate data which pins them and reduces biased tendencies of some employees against others by protecting the database safely from any unrecognized changes that might arise from unauthorized system users.

The study is likely to act as a base for future research on secured databases where through protecting data management can find it easy to eliminate biased tendencies as well as reducing manipulation of data and thus can rely on more accurate data while making its management, financial and employee decisions.

The study is expected to offer advice on how to educate users on database security, and some common-sense recommendations on how to limit the damages.

The study has also contributed to the researchers' academic qualification since it is vital in the fulfillment of the requirements for award of a degree of Bachelors of Information Technology.

1.7 **Research questions.**

1. Who is the founder of mukwano industry?

2. When was mukwano started?

3. What were the challenges faced at the start being a new company in the place?

4. What type of DBMS are you using?

5. Which security system are you using?

6. What are the major security threats to the system?

7. What type of network system are you using is it client server or peer to peer

CHAPTER TWO
LITERATURE REVIEW

2.0 Introduction

The literature related to relevant knowledge from various authors and websites on the major variables that is; need for data protections and how it can boost employee integrity, disadvantages of unprotected data on employee integrity, developing of a database security to protect unauthorized access of data by unauthorized users and testing of the recommended system.

2.1 Forms of Database Security/ Access Controls

Role-Based Access Control (RBAC) its basic concept is that privileges are associated with roles, and users are assigned to appropriate roles. Roles can be created and destroyed using the CREATE ROLE/DROP ROLE commands. It ensures that only authorized users are given access to certain data or resources (Wenyang, 2005). System is flexible and with a breadth of application which enables users to carry out a broad range of authorized operations. System administrators control access at a level of abstraction typical to the way organizations conduct duties by statically and dynamically regulating users' actions by establishing and defining roles, hierarchies, relationships, and constraints.

Mandatory Access control, Russom (2001), talks about mandatory access controls to address loopholes in discretionary access control. The mandatory access control (Bell-LaPadula model) is described by objects, subjects, security classes, and clearances. Each database object is assigned a security class and clearance for a security class. The model imposes two restrictions on all reads and writes of database objects which include Simple Security Property and Property.

2.2 Need for Database Protection and How it can Improve Employee Integrity

Silberchatz et al (2002) states that databases are designed to manage large bodies of information as well as providing a mechanism for the manipulation of information. **Improve Security;** In conventional systems, applications are developed in an ad hoc

manner. Often different system of an organization would access different components of the operational data. In such an environment, enforcing security can be quite difficult. Setting up of a database makes it easier to enforce security restrictions and to determine a person to bleach security since the data is now centralized. (Chin, 2006).

Improve Integrity; since the data of the organization using a database approach is centralized and would be used by a number of users at a time, it is essential to enforce integrity controls to avoid concurrent updating activities but if data is stored once then it becomes easier to maintain integrity than in conventional systems (Farrar, 2005). Integrity may be compromised in many ways. For example, in an airline DBMS the number of bookings made could be larger than the capacity of the aircraft.

Identify Enterprise requirements; all enterprises have departments and each of these units perceive their unit requirements as the most important. But a database with centralized control identifies enterprise requirements and balances the needs of competing units which makes it possible to ignore unnecessary requests (Farrar, 2005).

Develop Data model; for a secure database an overall data model for the enterprise needs to be built. In conventional systems, it is more likely that files will be designed as needs of particular applications demand. The overall view is often not considered. Building an overall view of the enterprise data, although often an expensive exercise, is usually very cost-effective in the long run (Feuerstein, 2003).

Inference control; is the corresponding countermeasure to statistical database security. Statistical database is a database which contains specific information on individuals or events but is intended to permit only statistical queries which however can not generate all the required information but can be aided with inference control techniques. (E.g. averages, sums, maximums, minimums and standard deviations. (Domingo, 2006).

Flow Control; it regulates the distribution or flow of information among accessible objects. A flow between object X and object Y occurs when a program reads values from X and writes values into Y. Flow controls check that information contained in some

objects does not flow explicitly or implicitly into less protected objects. Thus, S user cannot get indirectly in Y what he or she cannot get directly from X." (Domingo, 2006).

Encryption; it applies an encryption algorithm to the data, using a user-specified or DBA-specified encryption key. The output of the algorithm is the encrypted version of the data. There is also a decryption algorithm, which takes the encrypted data and a decryption key as input and then returns the original data." (Feuerstein, 2003).

Access Control; A database for an enterprise contains a great deal of information and usually has several groups of users. Most users need to access only a small part of the database to carry out their tasks. Allowing users unrestricted access to all the data can be undesirable this can be controlled through DBMS mechanisms (Feuerstein, 2003).

.3 Disadvantages of Unprotected Data on Employee Integrity

Confidentiality, Privacy and Security; Duncan et al (2003)note that, when information is centralized and is made available to users from remote locations, the possibilities of abuse are often more than in a conventional data processing system which necessitates taking technical, administrative and, possibly, legal measures. Most databases store valuable information that must be protected against deliberate trespass and destruction. While much attention is paid to outside attackers' efforts to crack databases, IT often overlooks an even greater threat, the end users. Ignorance and disregard of company security policies may lead employees to expose their organizations' databases to compromise, often without even knowing that they're doing so.

Data Quality; since the database is accessible to users remotely, adequate controls are needed to control users updating data and to control data quality. With increased number of users accessing data directly, there are enormous opportunities for users to damage the data unless there are suitable controls. Most external hacks occur because of flaws in designs that link to those databases. Yet, enterprises are increasingly exposing their most valuable data to these outward-facing interfaces which can be improved by security teams, database administrators and application developers (Delano et al, 2005).

Data Integrity; since a large number of users can access a database concurrently, technical safeguards is necessary to ensure that the data remain intact during operation. The main threat to data integrity comes from several different users attempting to update the same data at the same time; data needs to be protected against inadvertent changes. If the loss of system or data integrity is not corrected, continued use of the contaminated system or corrupted data could result in inaccuracy, fraud, or erroneous decisions. In addition, unauthorized, unanticipated, or unintentional disclosure could result in loss of public confidence, embarrassment, or legal action against the organization. For instance cops tap database to harass and intimidate or even blackmail (Delaney, et al, 2007).

Enterprise Vulnerability, centralizing all data of an enterprise in one database makes database an indispensable resource because the enterprises survival may depend on reliable information available from its database and thus its vulnerability to destruction and unauthorized modification. Not providing real assurance on the satisfaction of the protection requirements and not imposing any restriction on the usage of information once it is obtained by a user makes system vulnerable to attacks (Russom, 2001).

The Cost of using a DBMS; Conventional data processing systems are typically designed to run a number of well-defined, preplanned processes. Such systems are often "tuned" to run efficiently for the processes that they were designed for. Systems are fairly inflexible in that new applications may be difficult to implement and expensive to run. The database approach on the other hand provides a flexible alternative where new applications can be developed relatively inexpensively (Ben-Gann, et al, and 2006).

2.4 Developing a Database Security

Narayana (2004), states that security is a major concern for the modern age systems/network/database administrators. It is natural for an administrator to worry about hackers and external attacks while implementing security. But there is more to it. It is essential to first implement security to ensure the right people have access to the right data. Primarily a security plan must identify which users in the organization can see which data and perform which activities in the database

Accessing Database through SQL Server security model; Narayana (2004) emphasizes that to access data from a database user must pass through two stages of authentication, one at the SQL Server level and the other at the database level. These two stages are implemented using Logins names and User accounts respectively. A valid login is required to connect to SQL Server and a valid user account is required to access a database as below;

Login: A valid login name is required to connect to an SQL Server for instance; a Windows NT/2000 login that has been granted access to SQL Server and an SQL Server login that is maintained within SQL Server and the login names are maintained within the master database and thus essential to backup the master database.

User: A valid user account specific to the database is required to access that database to control permissions and ownership of objects in the database which are associated with SQL Server logins. A login can have associated users in different databases, but only one user per database. During a new connection request, SQL Server verifies the login name supplied, to make sure, that login is authorized to access SQL Server. This verification is called Authentication. SQL Server supports two authentication modes:

Windows Authentication mode: according to the Database Gateway for SQL Server User's Guide, it is emphasized that, with windows authentication, there is no need to have to specify a login name and password, to connect to SQL Server but instead, access to SQL Server is controlled by Windows NT/2000 account or the group to which a particular account belongs which was used to login to the Windows operating system on the client computer/workstation. A DBA must first specify to SQL Server, all the Microsoft Windows NT/2000 accounts or groups that can connect to SQL Server.

Mixed mode: Mixed mode allows users to connect using Windows authentication or SQL Server authentication. DBA must first create valid SQL Server login accounts and passwords not related to Microsoft Windows NT/2000 accounts where an SQL Server

login and password is supplied connecting to SQL Server. If SQL Server login name and password is unspecified, request Windows Authentication. Whatever mode is configured for SQL Server login is by Windows authentication. SQL Server's authentication mode can be changed using Enterprise Manager. Authentication mode can also be changed using SQL DMO object model (Database Gateway for SQL Server User's Guide).sql server authentication is demonstrated below

2.5 Designing a System for Database Security

Feuerstein (2003) emphasizes that database security may be designed to control access to objects within the database and managing permissions. It also implements permissions using roles where a role is nothing but a group to which individual logins/users can be added, so that the permissions can be applied to the group, instead of applying the permissions to all the individual logins/users. There are three types of roles in SQL Server 7.0/2000: Fixed server roles, fixed database roles and Application roles.

Fixed server roles: are server-wide roles in which logins can be added to gain the associated administrative permissions of the role. They cannot be altered and new roles cannot be created.

Fixed database roles: Each database has a set of fixed database roles, to which database users can be added which are unique. While their permissions cannot be altered, new roles can be created.

Application roles: Domingo-Ferrer (2006) notes that, application roles are another way of implementing permissions through creating and assigning the required permissions. The client application activates this role at run-time to get the associated permissions. They simplify the job of DBAs, since there's no worry managing permissions at individual user level. It is a matter of creating an application role and assigning permissions. The application that is connecting to the database activates the application role and inherits the permissions associated to it. Characteristics of application roles include:

- There are no built-in application roles and they contain no members
- They need to be activated at run-time, by the application, using a password
- They override standard permissions. e.g., after activating the application role, it will lose all the permissions associated with the login/user account used while connecting to SQL Server and gain the permissions associated with the application role.
- Application roles are database specific. After activating an application role in a database, if that application wants to run a cross-database transaction, the other database must have a guest user account enabled.

Granting / revoking permissions to / from database users, database roles and application roles.

Chin (2006) specifies that there are three T-SQL commands used to manage permissions at the user and role level where through these commands, permissions can be granted/denied/revoked to users/roles on all database objects. You can manage permissions at as low as the column level. However, there is no way to manage permissions at the row level. These include;

Grant; This grants the specific permission (Like SELECT, DELETE etc.) to the specified user or role in the current database

Revoke: This removes a previously granted or denied permission from a user or role in the current database.

Deny: which denies a specific permission to the specified user or role in the current database.

2.6 Testing System for Validity

Wenyang (2005) notes that there are three main objects when designing a secure database application, and anything preventing DBMS to achieve these goals would be consider a threat to Database Security. These include;

Integrity; Database integrity refers to the requirement that information be protected from improper modification. Modification of data includes creation, insertion, modification, changing the status of data, and deletion. Integrity is lost if unauthorized changes are made to the data by either intentional or accidental acts. According to Farrar (2005), enhancement of security prevents loss of integrity from happening, only authorized users should be allowed to modify data e.g. students may be allowed to see their grades, yet not allowed to modify it.

Availability; Authorized user or program is not denied access. An instructor who wishes to change a grade is allowed to do so through grid computing and SQL Real Application Clusters (RAC). Flashback Database is a new approach to point-in-time (PIT) database recovery. This incomplete recovery strategy is used to recover a database that has been logically corrupted due to human error. Mullins (2004) notes availability to be a great issue to DBAs users want more of their data available more of the time.

Secrecy; Information should not be disclosed to unauthorized users. For example, a student should not be allowed to examine other students' grades. According to Duncan, et al (2003), to achieve these objectives, a clear and consistent security policy should be developed to describe the security measures to be enforced. There is need to determine the part of the data to be protected and which users get access to which portions of the data. The security mechanisms of the underlying DBMS and operating system, as well as external mechanisms, such as securing access to buildings, must be utilized to enforce the policy and emphasis should be put on security measures to be taken at several levels.

Backup and Recovery; According to Russom (2001), backup and recovery is arguably the DBA's most important responsibility

SQL Server Gateway Features and Restriction; in the Database Gateway for SQL Server User's Guide, it is emphasized that, Gateway is installed and configured to access SQL Server data, pass SQL Server commands from applications to the SQL Server database, perform distributed queries and copying data all of which can be enhanced

through Pass- Through Features, known restrictions, known problems, database compatibility issues for SQL Server and executing stored procedures and functions.

Pass-Through Feature; If the SQL statement being passed through the gateway result in an implicit commit at the SQL Server database, the Oracle transaction manager is unaware of the commit and an Oracle ROLLBACK command cannot be used to roll back the transaction.(Database Gateway for SQL User's Guide)

Compatibility; SQL Server databases function differently in some areas, causing compatibility problems such as; Implicit Transactions (Chained Mode); Column Definitions; Naming Rules; Data Types; Queries and Locking. (Delaney et al, 2007).

DDL Statements; SQL Server requires some DDL statements to be executed in their own transaction, and only one DDL statement can be executed in a given transaction. If you use these DDL statements in a SQL Server stored procedure and you execute the stored procedure through the gateway using the procedural feature, or, if you execute the DDL statements through the gateway using the pass-through feature, an error condition might result. This is because the procedural feature and the pass-through feature of the gateway cannot guarantee that the DDL statements are executed in their own separate transaction (Delano et al, 2005).

Performance tuning; keeping your database and SQL queries running quickly and smoothly is one of the most important and demanding tasks for a DBA. (Delaney et al, 2007).

Code review; through review of codes development can be standardized as much as possible by using standard components for low-level aspects of the code base (error management, SQL access, etc.) through use of top-down design to keep the code clean and eminently transparent in meaning as well as test code before it is implemented to automate unit testing process as much as possible in order to be in position to erase the bugs from code and letting other people look at and critique code can be scary, unless the

right culture exists in your group. No code should be put into production unless some other human being has looked at it. There are too many ways that a person, sucked deep into the problem space of their requirements and programs, can mess up without even realizing. . (Delaney et al, 2007).

Installation, upgrades and patches; DBMS rolls out an all-Java open source embedded database with high availability and fault-tolerant capabilities for mission-critical applications. In addition to supporting grid computing features such as resource sharing and automatic load balancing.

Tools; SQLCMD is a command line application that comes with Microsoft SQL Server, and exposes the management features of SQL Server. It allows SQL queries to be written and executed from the command prompt. It can also act as a scripting language to create and run a set of SQL statements as a script (Ben – Gan et al, 2006).

CHAPTER THREE
METHODOLOGY

3.0 Introduction

The study took place in Mukwano Industry because its database is not well protected and therefore cannot enhance employee integrity due to the unauthorized accesses to confidential information. To unearth the challenges experienced the study covered the office of the personnel manager, secretaries and the reception, as well as involved some support staff for sufficiency of data. The procedure followed will sought to avail production process with specific standards, expert instruction and assistance to undermine and eliminate unauthorized access and errors to yield accurate estimates and maintain the quality of outputted data. The following methods were employed;

3.1 Research Design

The study was based on primary data and data collection techniques involved use of interviews as main instruments to enhance and give quality to the findings. Interviews are a useful tool through which data can be acquired by reading the perceptions and feelings while collecting data although at times they yield minor biases, which is an implication that not all information will be proven accurate. The study ensured that interviews were impressive to eliminate suspicious tendencies. Secondary data was also relied upon by reviewing literature of previous writers on the same study and included textbooks, CDs, Internet, Journals and previous research on database security and employee integrity in organizations.

3.2 Study Population and Size

The study was based in Mukwano Industry because it is conveniently located and has different departments which must jointly operate to meet the company's goals and thus due to a big number of employees and the different aspirations they might be having, it is most likely that free access to information may be prone to biased attitudes, and manipulations.

3.3 Research Instruments

.3.1 Interview

The study made use of unstructured interview with the Human resource manager, systems administrator, which allowed for a fair flow of information as they were limited to the expression of some confidential information. Guidelines on database security, unauthorized accesses and their impact on the integrity of the employees were all covered in the interview guide.

3.4 Design Techniques and Tools

The researchers relied on a DFD as the major method to enhance the security as this represented the controlled and protected flow of data through a system by facilitating their break down processes in their minute components all of which were subdivided into smaller processes that comprised of the primary process. It was used because DFD as recommended by Gane (1979) who depicts the flow of events and data within the system.

3.5 Methodology for Development of System

SQL as observed by Chuck and Crawford (1970) is capable of achieving high quality system that meets the requirements of system security development. SDLC can spot deficiencies in an existing system through use of interviews with users and support personnel. It can define requirements of the new system by addressing loopholes in existing system and providing possible interventions for the betterment of the system by addressing issues pertaining to unauthorized access as proposed system is enhanced as well as installing components and programs where system users need to be trained in software usage as testing for applicability of the proposed protection

SDLC was selected as the best methodology for enhancement of database security in Mukwano industry because it was in position to address many activities such examining the need for database security, unprotected data and its impact on integrity of the employees as well as developing ways of protecting data

Different phases of development were;

Analysis; The researchers explored the current database protection system to establish problems it brings about and thus were in position to identify user requirements as well as

inputs to the system and required output. This was through analyzing the current as well as anticipating future problems of the unprotected data on integrity of the employees from which conclusions which helped to enlighten the researchers on the needs of the system protection were drawn.

Design; for validation of performance of the system in data processing, software and user interface in order to specify how the system was protected through use of SQL as the structured methodology tool, to allow for protection of confidential data.

Planning; this was done to guide the study in understanding why the system should be protected through a redefinition of its requirements, establishing how data was protected in the current system, and what effect it caused in order to choose the best security option.

Implementation; Through implementation, validity of the security system was done followed by an installation of the necessary software and system maintenance. And thereafter came up with the concept of data security to improve on the integrity of employees in order to protect the position of the company.

3.6 System Development Tools

3.6.1 Programming Languages (s) and Tools

The researchers used visual studio and SQL server 2005 to develop the database for Mukwano Industry. Each log entry was identified by an increasing *Log Sequence Number* (LSN) which ensured that no event overwrites another.

SQL Server ensured that the log was written onto the disc before the actual page is written back which enabled it to ensure integrity of the data, even if the system fails. If both the log and the page were written before the failure, the entire data is on persistent storage and integrity is ensured. To implement locking, SQL Server contains the *Lock Manager*. The Lock Manager maintains an in-memory table that manages the database objects and locks, if any, on them along with other metadata about the lock. Access to any shared object is mediated by the lock manager, which either grants access to the resource or blocks it.

3.6.2 Operating System

Operating system XP was used due to its flexibility, high performance and its functional ability on PCs as well as on home and business desktops which renders appropriate for the study and also for its additional ability for windows in the use of visual styles to change user interface by presenting a redesigned graphical user interface.

The researchers used XP because it is of improved stability and efficiency over different Microsoft Windows versions as explained by (Kirk, 2006).

XP is able to accommodate a big number of users concurrently as well as introducing several new features and more user friendly interfaces. XP (Service Pack 2) because of the windows security center enhancements it provides security on the overall system, the state of anti-virus software, windows update, and new windows firewall inclusive.

3.6.3 Database Management Systems (DBMS)

We used Microsoft SQL server to come up with a database for human resource

The system has a database to store all the information about mukwano. It has advantages such as security features, protection, maintenance, performance and reliability in operation.

CHAPTER FOUR

SYSTEM ANALYSIS AND DESIGN

introduction

Analysis; The researchers explored the current database protection system to establish problems it brings about and thus were in position to identify user requirements as well as inputs to the system and required output. This was through analyzing the current as well as anticipating future problems of the unprotected data on integrity of the employees from which conclusions which helped to enlighten the researchers on the needs of the system protection were drawn.

At this step, data related to the existing system was collected upon which an analysis was made for specific requirements that would be of help in the development of the new security system upon which analysis specifically focused on how to meet and solve the current employ needs.

Problems with the current system

- Ignorance and disregard of company security policies led employees to expose their organizations' database to compromise, often without even knowing that they are doing so.

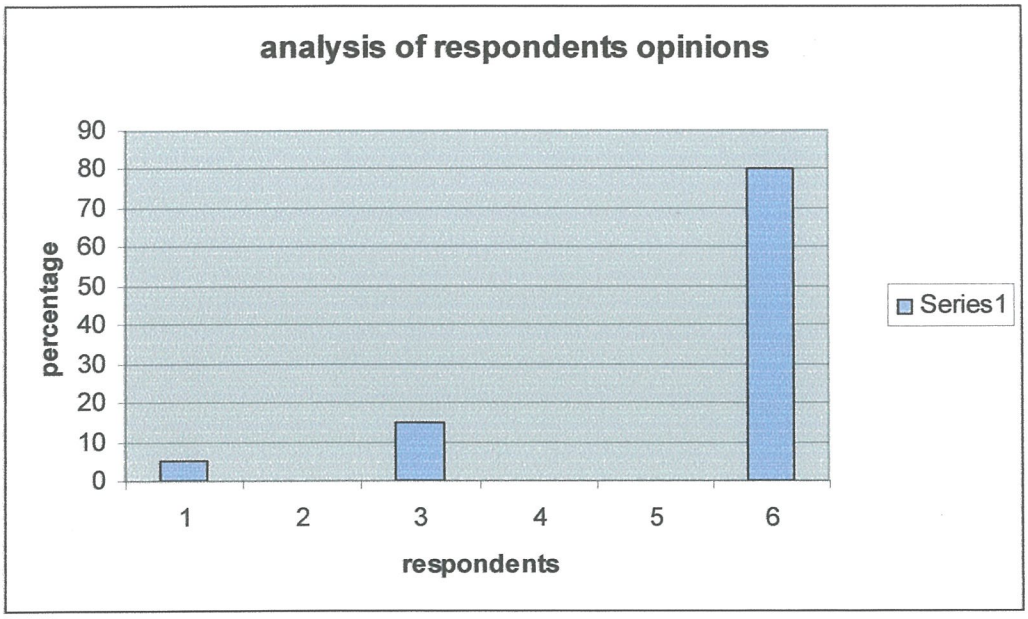
- Not providing real assurance on the satisfaction of the protection requirements and not imposing any restriction on the usage of information once it is obtained by a user made system vulnerable to attacks.

- The main threat to data integrity came from several different users attempting to update the same data at the same time; data needed to be protected against inadvertent changes. If the loss of system or data integrity is not corrected, continued use of the contaminated system or corrupted data results in inaccuracy, fraud, or erroneous decisions. In addition, unauthorized, unanticipated, or

unintentional disclosure results in loss of public confidence, embarrassment, or legal action against the organization.

Need for the new system

Basing on the research question "what are the major security threats to the system?" we found out that 80% of the respondents supported a new security system, 15% were not in support in fear of losing their jobs and 5% were just neutral.



User Requirements Definition

For the system to work well, it required both functional and non-functional user requirements.

Non Functional Requirements

This section introduces some of the nonfunctional requirements that the system should be in position to provide as described below:

Security

The security function required authentication where by provision of login interfaces involving user name and password were made. Giving way of privileges to the person supposed to modify, add, create, access among the developers, systems administrators and users. The Systems Administrator will have exclusive rights. User rights: access, editing personal information and audit trails to keep track of login files.

Interoperability

The system was built in such a way that it can work with other future systems.

Response Time

The system should provide a response time of not more that 10 microseconds. It should also provide required information in real time when it is searched.

User friendliness

i. The system will provide help facility in case some information is not clear.

ii. Uniform flow of tabbing when navigating through the form controls such as text areas, always from left to right.

iii. The system is simple, attractive and easy to use. That is experienced users can use all the system functions after a total of 1 hours training. After this training, the average number of errors made by these users will not exceed 2 per day.

iv. The system shall provide more than one search criteria for the user to search

customer records.

v. The system shall provide an edit function whereby the user will be able to edit specific data as per his privilege.

vi. The system shall enable checking of fields. For example; rejecting incorrect or incomplete data. When a field is left null in an area where the domain is not null, the system should alert the user of the incomplete information

Functional Requirements

Functions to be performed or services provided to the user will include:

i. Enabling the authorized personnel to have access to employees' records.

ii. Capture details of employees.

iii. Retrieve the employees' personal data and transaction records.

iv. Capture the attributes that concern the industry.

v. Enable proper flow of information from one department to another

vi. Ensure the security and privacy of both administration and customers' data.

4.2.3 System Requirements

In order for the system to perform as expected, the following system specification for hardware and software, security and operations are required.

Hardware	Requirement	Software	requirement

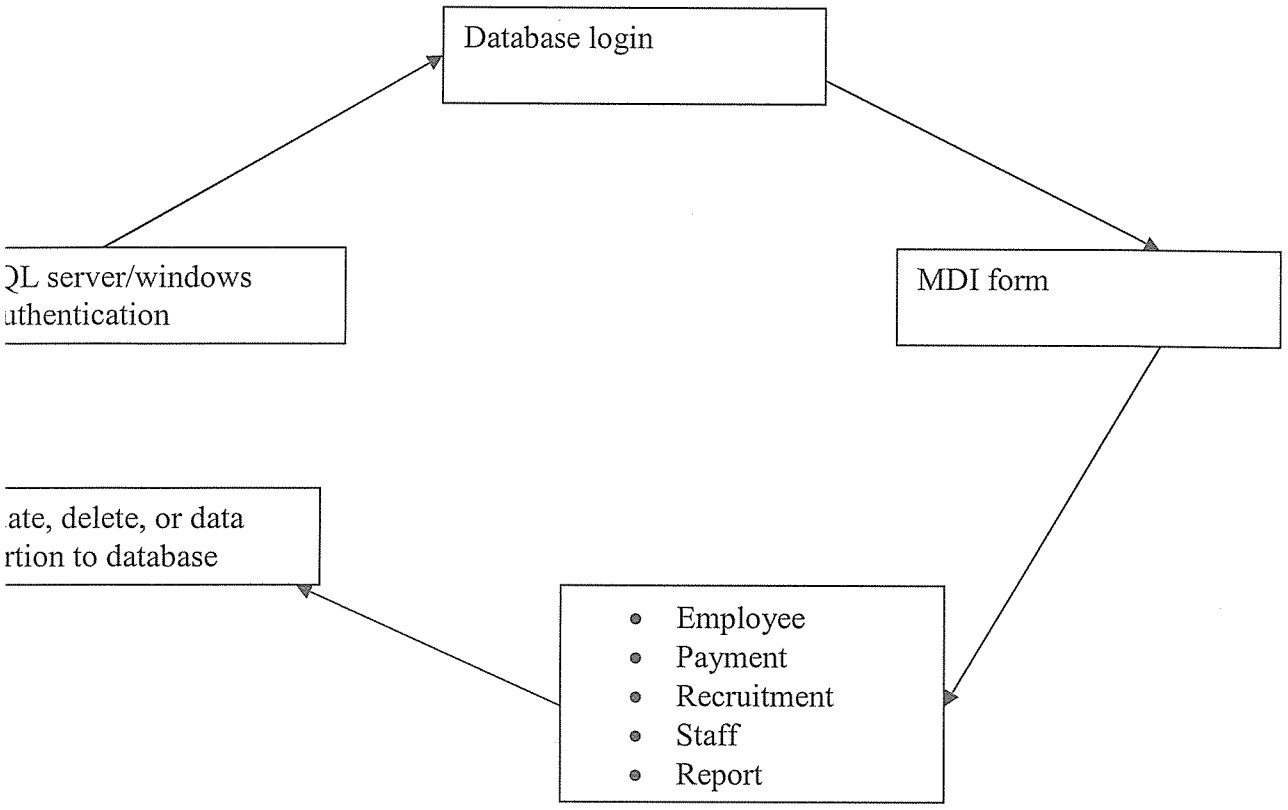


Figure 2 data flow diagram

System's flow chart

It shows the logical flow of information regarding the new system developed.

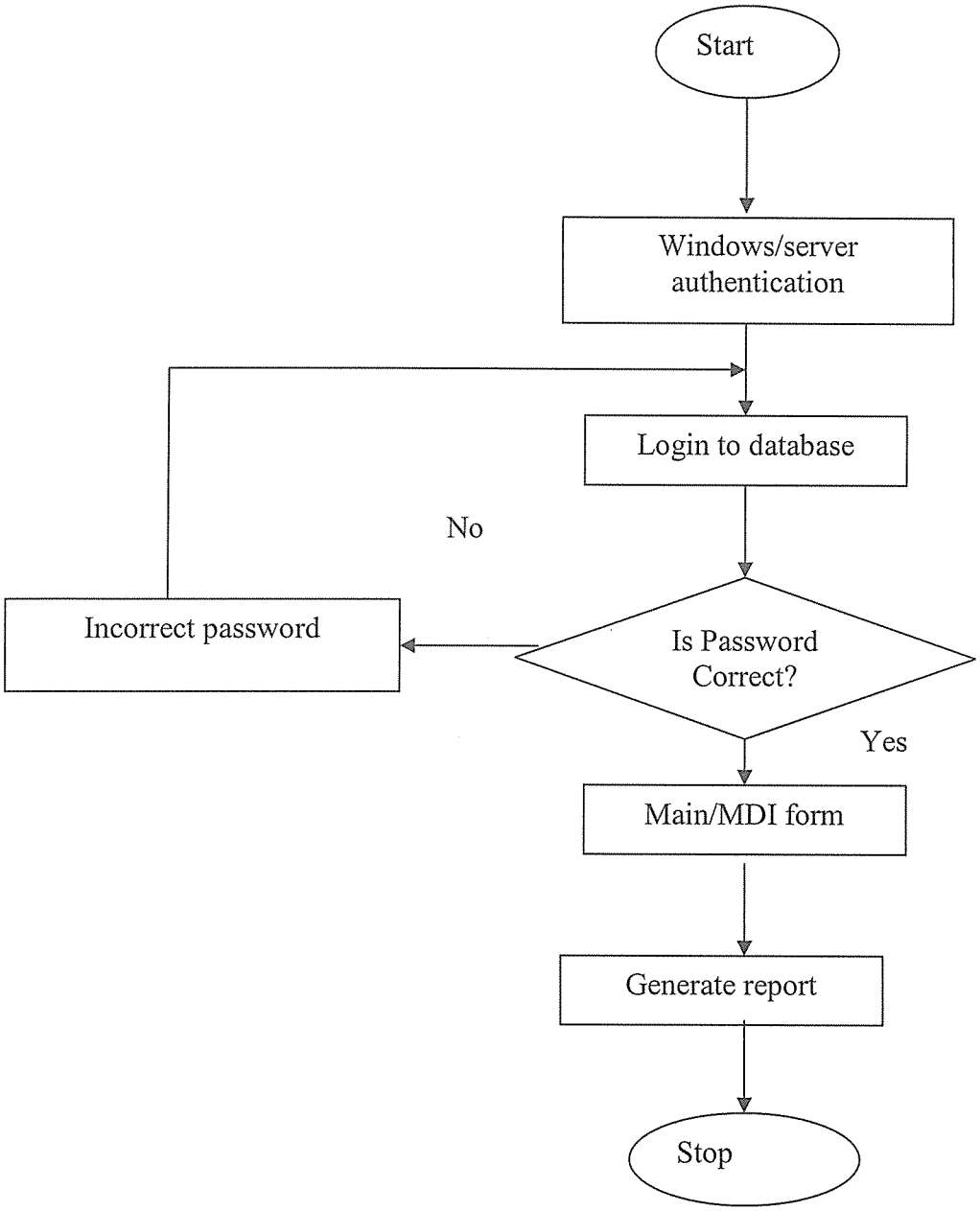


Figure 3: system flow chart

Figure 3: system flow chart

We used Microsoft SQL server to come up with a database for human resource

The system has a database to store all the information about mukwano. It has advantages such as security features, protection, maintenance, performance and reliability in operation.

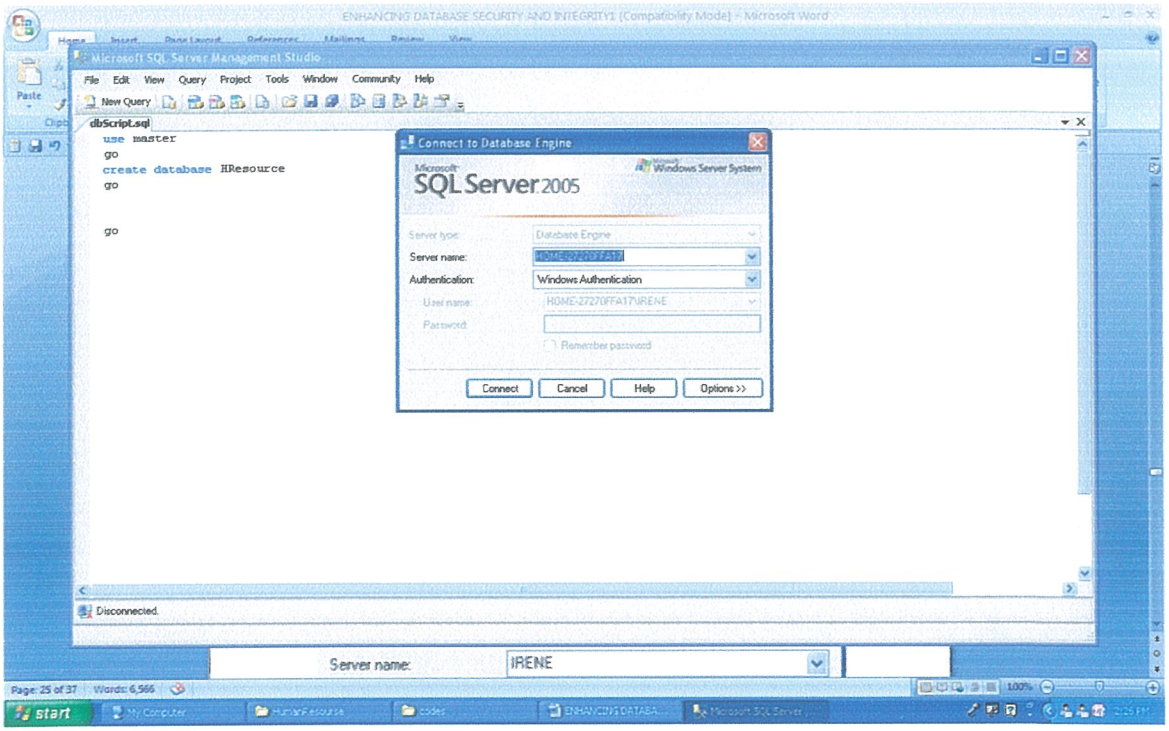


Figure 4 database creation

Windows Authentication mode: according to the Database Gateway for SQL Server User's Guide, it is emphasized that, with windows authentication, there is no need to have to specify a login name and password, to connect to SQL Server but instead, access to SQL Server is controlled by Windows NT/2000 account or the group to which a

particular account belongs which was used to login to the Windows operating system on the client computer/workstation. A DBA must first specify to SQL Server, all the Microsoft Windows NT/2000 accounts or groups that can connect to SQL Server.

Figure 5 windows authentication

Mixed mode: Mixed mode allows users to connect using Windows authentication or SQL Server authentication. DBA must first create valid SQL Server login accounts and passwords not related to Microsoft Windows NT/2000 accounts where an SQL Server login and password is supplied connecting to SQL Server. If SQL Server login name and password is unspecified, request Windows Authentication. Whatever mode is configured for SQL Server login is by Windows authentication. SQL Server's authentication mode

can be changed using Enterprise Manager. Authentication mode can also be changed using SQL DMO object model (Database Gateway for SQL Server User's Guide).sql server authentication is demonstrated below.

Figure 6 mixed mode authentication

Administrator Login system to mukwano database

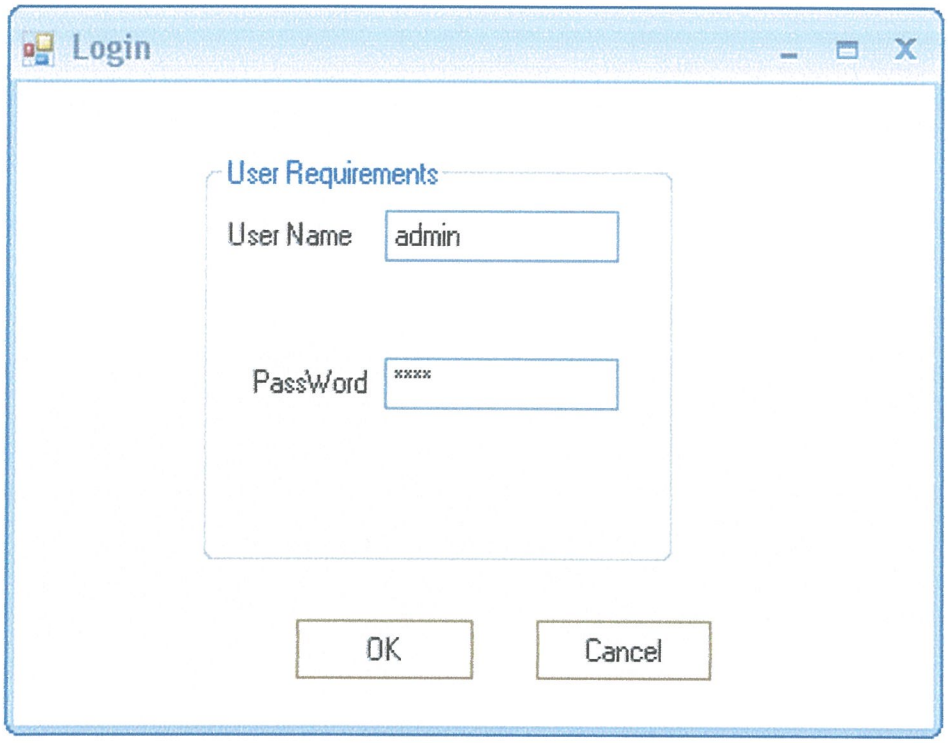


Figure 7 login form

Login: A valid login name is required to connect to an SQL Server for instance; a Windows NT/2000 login that has been granted access to SQL Server and an SQL Server login that is maintained within SQL Server and the login names are maintained within the master database and thus essential to backup the master database.

User: A valid user account specific to the database is required to access that database to control permissions and ownership of objects in the database which are associated with

SQL Server logins. A login can have associated users in different databases, but only one user per database. During a new connection request, SQL Server verifies the login name supplied, to make sure, that login is authorized to access SQL Server. This verification is called Authentication. SQL Server supports two authentication modes:

MDI FORM

The above MDI form helps the user to access different applications/tables in Mukwano database.

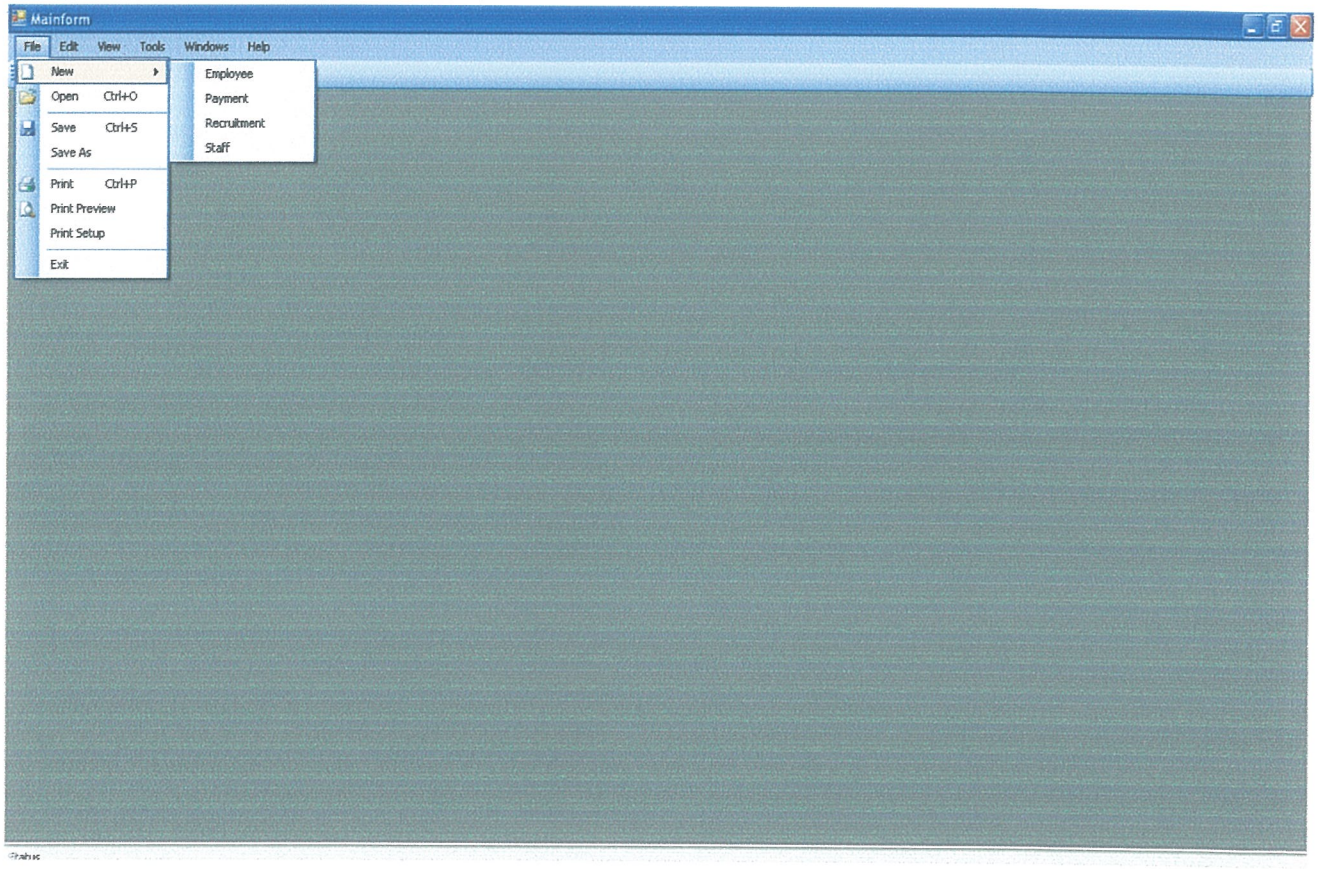
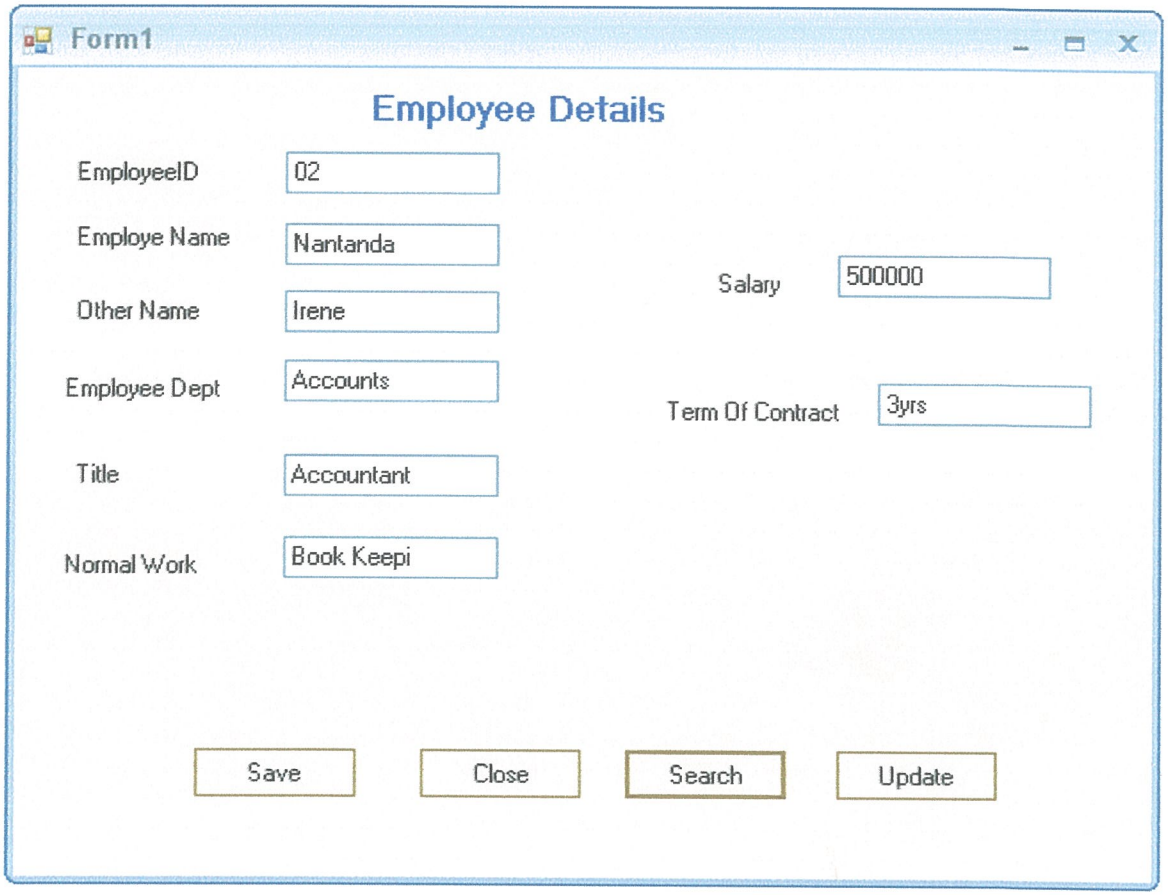


Figure 8 MDI form

Mukwano database tables that can be accessed after proper authentication process



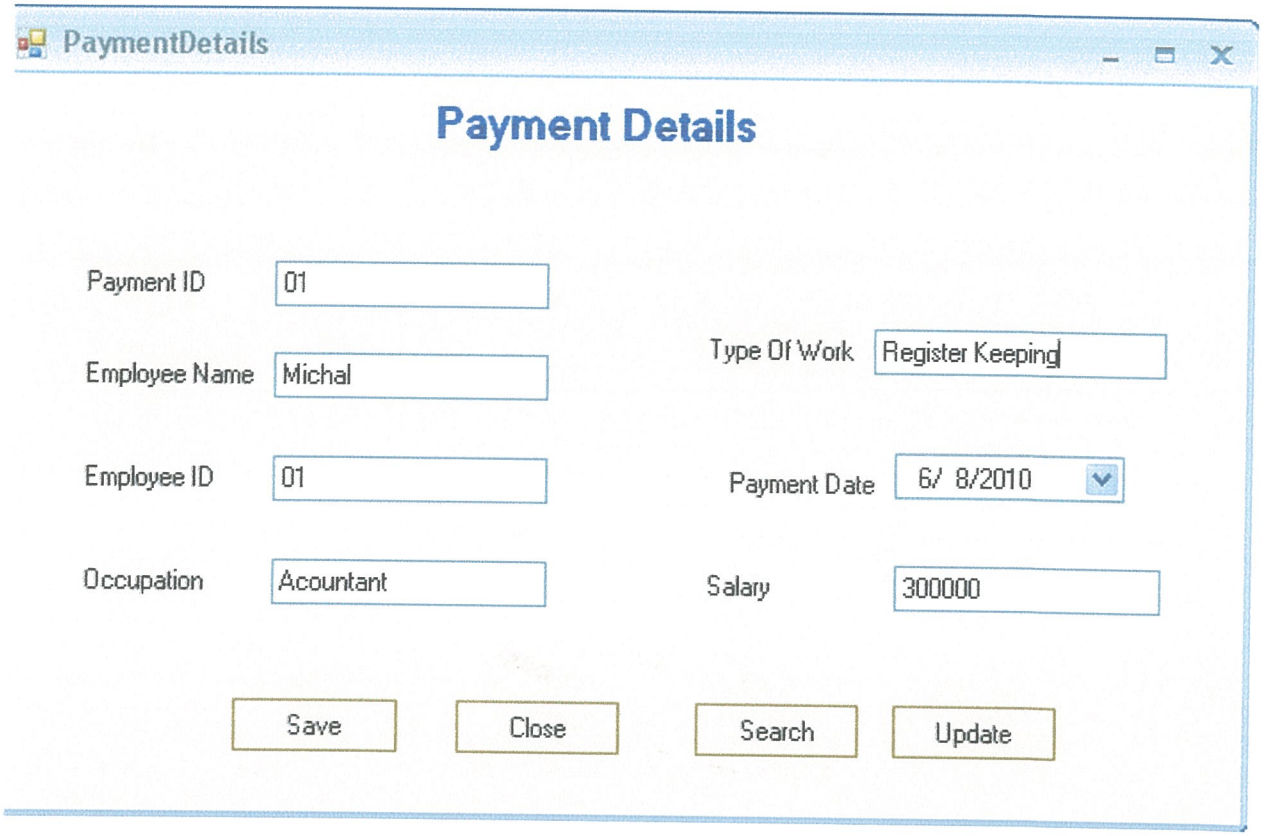


Figure 9 payment details.

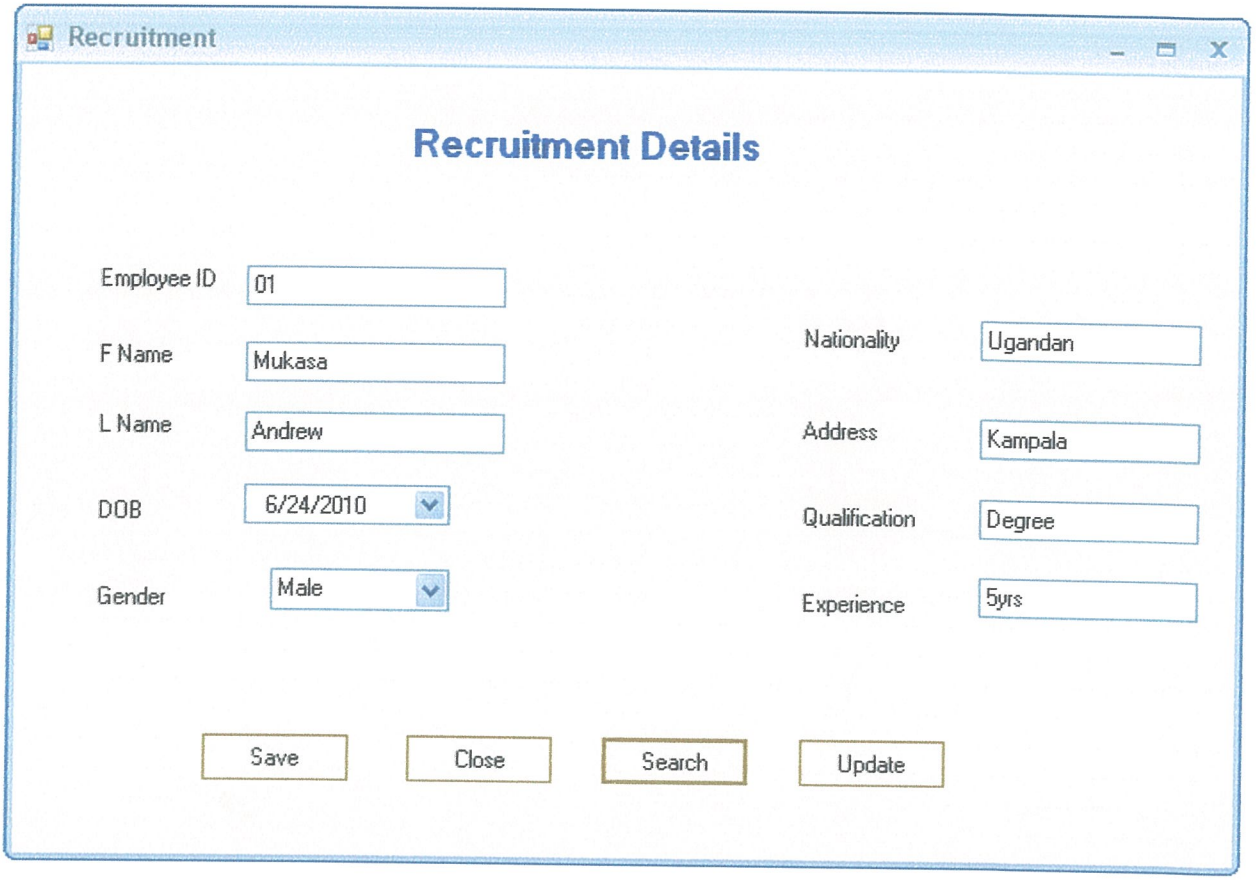

Recruitment
Recruitment Details
Employee ID
01
F Name
Mukasa
L Name
Andrew
DOB
6/24/2010
Gender
Male
Nationality
Ugandan
Address
Kampala
Qualification
Degree
Experience
5yrs
Save
Close
Search
Update

Figure 10

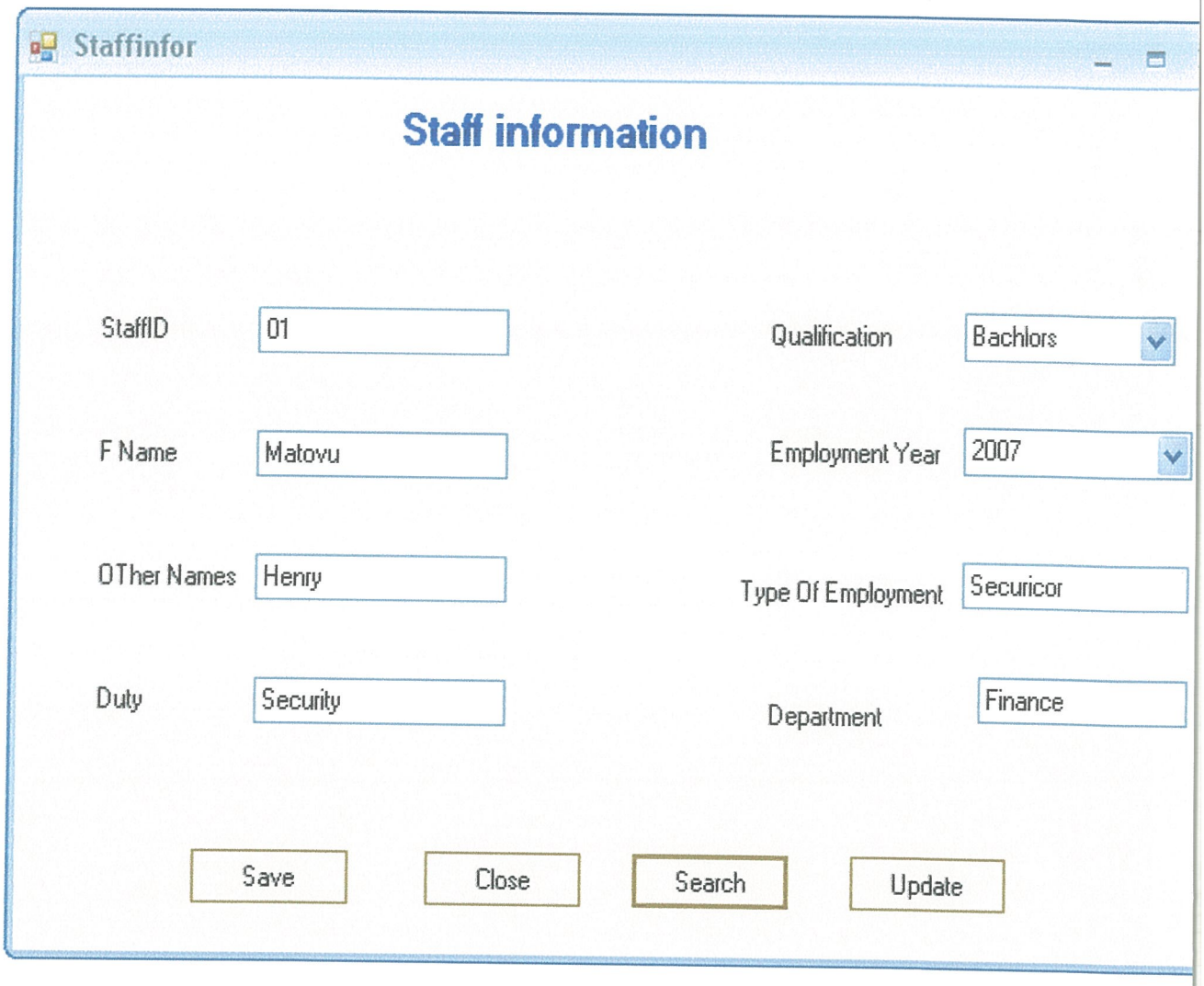


Fig:11 Employee input form.

Below is a sample report for employee details;

:01

yeeID	FirstName	OtherNam	Title	NomalW	TermOfContr	Salary	EmployeeDepart
	rita	masaba	system admin	troublesh	permanent	1,800,000.0	IT
	Nantanda	Irene	Accountant	Book	3yrs	500,000.00	Accounts
	Mushabe	Apollo	Acountant	Supervis	3yrs	200,000.00	Finance
	Shamin	Nansukusa	Secretary	Bookkee	3yrs	800,000.00	Finance
	Muhumuza	wwwwwww	www	ww	3yrs	200,000.00	wwww
	ritah	wwwwwww	www	ww	3yrs	200,000.00	wwww

:12 Employee input report

CHAPTER FIVE

5.0 SYSTEM TESTING AND IMPLEMENTATION

Every new system normally after it has been implemented is then subjected to a series of tests to find out its strength and weaknesses. After proving its effectiveness, it is then left to routine monitoring to ensure smooth operations.

5.1 SYSTEM IMPLEMENTATION

On a successful completion of the testing, the system was ready for the implementation. The system users and the designer worked together to implement this system. This though went through a series of steps:

- Preparation of physical site: this involved choosing the rooms to be used and setting up the necessary furniture to accommodate the computer sets and other devices.
- Acquiring and installing equipment: this involved the buying and installation of the computer sets and all other accessories as per the hardware requirements. This also involved networking the computers.
- Training personnel: the system designer was mainly involved in the training of the users in the application designed. Also an independent individual was hired to train some users on computer basics and applications.
- Selecting and assigning personnel: due to the limited number of personnel, there was no problem in assigning personnel since almost all the personnel were to be involved in the various sections of the department.
- Converting data files: This process was done slowly and carefully to ensure that the manual data files were fed into the computer without any errors.
- Debugging: Errors that were witnessed during the conversion were debugged.

5.2 THE SYSTEM TESTING

The system was tested in order to:

- Ensure that on entering the correct user name and password the user is allowed access to the database.
- Guarantee that only the database administrator has aright to update delete or make changes to the database.
- Find out whether the new system can achieve the objectives it's meant to fulfill.
- Establish whether the components of the system interface are correct.
- Make sure that concurrent access to the database does not compromise its security.

The system was found to react favorably to this testing, thus it was found to be effective.

5.3 SYSTEM EVALUATION

After getting the system operational, it was then evaluated.

5.3.1 Development Evaluation:

The development of the security system was done with little costs and within a short time possible. The development was carried out using SQL sever 2005 and Microsoft Visual studio.

5.3.2 Operational Evaluation:

5.3.3 The system was a good response time and is seen to be far much better than the TFS. The users on the other hand confessed that the system is easy to use.

CAPTER SIX

CONLUSION

Through implementation, validity of the security system was done followed by an installation of the necessary software and system maintenance. And thereafter came up with the concept of data security to improve on the integrity of employees in order to protect the position of the company.

RECOMMENDATIONS

For continuity and improvements of the project, the researchers recommended the following;

- In the future for security and efficiency, modules of editing and deleting should be secured by passwords. This helps a lot in tracking of forgeries and misrepresentation of information.
- The access to the database should be in such away that each person should be availed only the section that he/she is concerned with, not the entire database.

This can be achieved by use of several passwords protected forms covering the various sections instead of a general password.

The system is primarily concerned with enhancing database security and integrity for employees in an organization so that there is proper authentication methods so that the database security is not compromised with.

REFERENCES

Ben-Gan, Itzik, et al. (2006). Inside Microsoft SQL Server 2005: T-SQL Programming. Microsoft Press.

Craig. S Mullins, (2004), Database Trends: How Much Availability is Enough?

Database Gateway for SQL Server User's Guide, 11*g* Release 1 Oracle®

Delaney, Kalen, et al. (2007). *Inside SQL Server 2005: Query Tuning and Optimization. Microsoft Press.*

Francis Chin (2006), Database Security Issues: Security problems on inference control for SUM, MAX, and MIN queries.

Gary Farrar (2005), Maintaining Database Integrity

George T. Duncan, Sallie A. Keller-McNulty . S. Lynne Stokes, (2003), Database Security and Confidentiality: Examining Disclosure Risk vs. Data Utility through the R-U Confidentiality Map.

Joseph Domingo-Ferrer (2000), Advances in Inference Control in Statistical Databases: An Overview.

Lance Delano, Rajesh George et al. (2005). *Wrox's SQL Server 2005 Express Edition Starter Kit (Programmer to Programmer). Microsoft Press.*

Narayana Vyas Kondreddi (2004), Database encryption for SQL Server and MSDE, Copyright © 1997 – 2004, India.

Phillip Russom (2001), Strategies and Sybase Solutions for database availability

R.Elmasri, S. B. Navathe, (2003), Fundamentals of Database Systems, Ed.4, Addison-Wesley, 2003. (Chapter 23)

Steven Feuerstein (2003), Oracle Development Languages.Wenyang Yi (2005), Database Security- Threats and Countermeasures, Database Security overview.

APPENDIX (A):

interview

8. Who is the founder of mukwano industry?

9. When was mukwano started?

10. What were the challenges faced at the start being a new company in the place?

11. What type of DBMS are you using?

12. Which security system are you using?

13. What are the major security threats to the system?

14. What type of network system are you using is it client server or peer to peer

APPENDIX(B): CODES

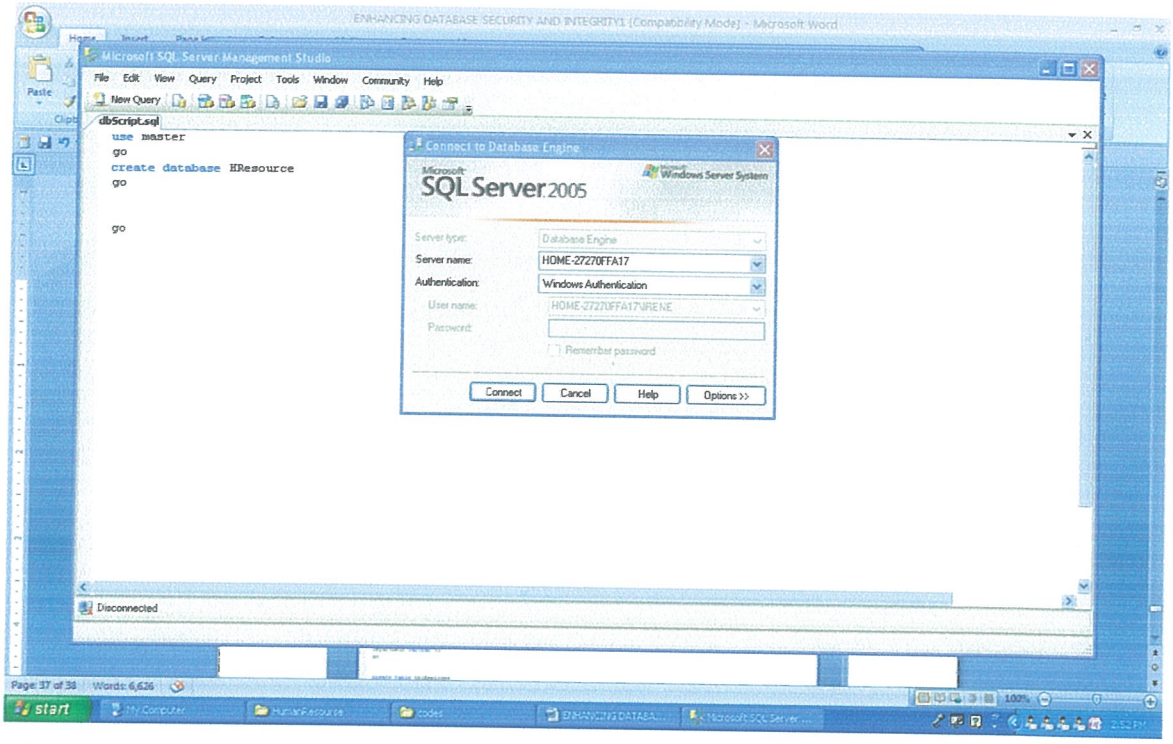


Fig:13 code for HR database creation

Below are the codes that were used to come up with the various database tables in the database.

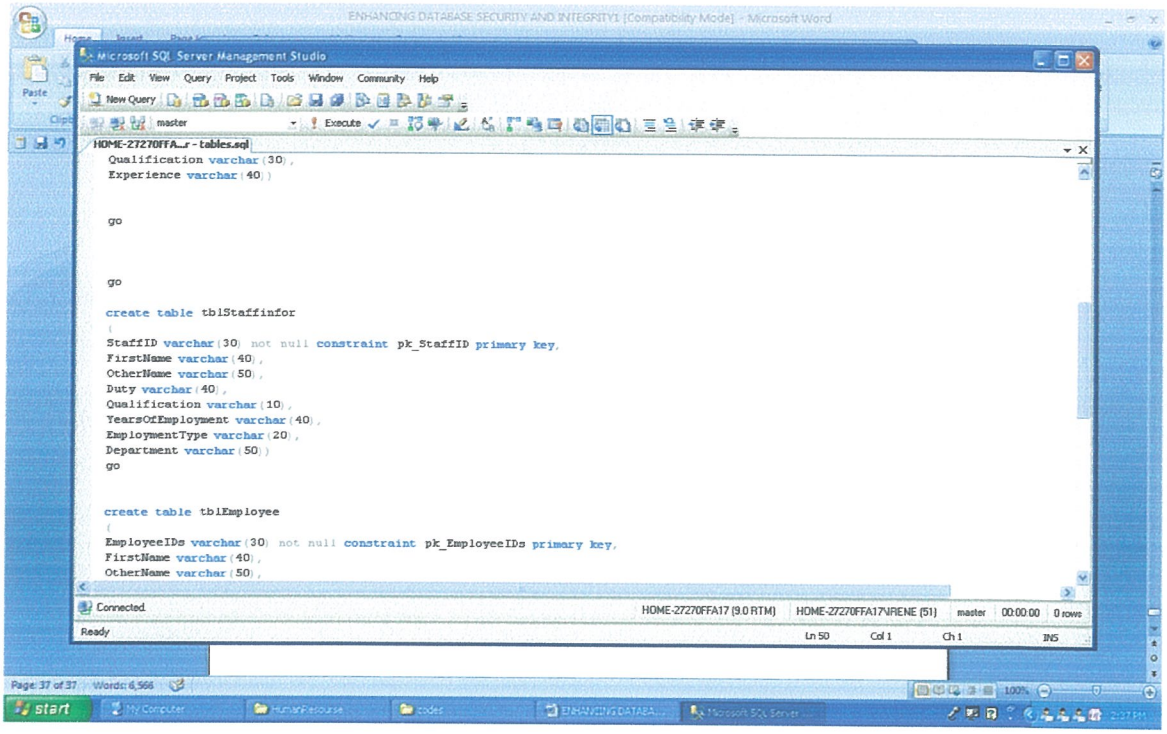


Fig: 14 codes for input tables' creation

```
Qualification varchar(30),
Experience varchar(40))
go
go
create table tblStaffinfor
(
StaffID varchar(30) not null constraint pk_StaffID primary key,
FirstName varchar(40),
OtherName varchar(50),
Duty varchar(40),
Qualification varchar(10),
YearsOfEmployment varchar(40),
EmploymentType varchar(20),
Department varchar(50))
go
create table tblEmployee
(
EmployeeIDs varchar(30) not null constraint pk_EmployeeIDs primary key,
FirstName varchar(40),
OtherName varchar(50),
```

```
Title varchar(40),
NomalWork varchar(10),
TermOfContract varchar(40),
Salary decimal(18.0),
EmployeeDepartment varchar(50))
go
```