Desktop Information System for Employee Management

Milena Karova
Technical University Varna, Bulgaria
mkarova@tu-varna.bg

Abstract: *The report presents a developed Desktop Information System for Employee Management. The system includes database development and encryption using a special algorithm to create an encryption key. The main goal of the development is to provide two types of protection: at the entrance to the system and in the transmission and data storage. The system includes four access levels: Employees, Executives or Managers, Directors and Administrators.*
The information system includes the following functionalities, depending on the access levels: entering tasks, registering users, entering priorities for tasks, entering the status of tasks, reviewing entered tasks, editing tasks and their status, deleting tasks, reviewing , add, edit and delete all users in the system; and others.
Keywords*: INFORMATION SYSTEM, EMPLOYEE MANAGEMENT, PASSWORD PROTECTION, SQL INJECTIONS, ENCRYPTION ALGORITHM, TASKS, SECURE COMMUNICATION.*

1. Introduction

There are a lot of software products that offer services related to personnel management. A research has been done on what some of the better-known software have to offer and based on a research a comparative feature has been made with the current development.

"BambooHR" is a well-designed software solution that helps automate operational tasks. This software collects valuable employee information and provides it to the team so they can streamline processes and be more efficient. Millions of users use "BambooHR" worldwide. It has the following functionalities:

- Centralized employee database;
- Management of job applications;
- Data management, export, reporting, visualization;
- Performance management module;
- Integrations of third party products;
-Information security;
- Online signature;
- Monitoring of working hours.

Advantages:

- Good reporting;
- Good user support;
- Integrated possibility to use the services of third parties.

Disadvantages:

- Difficult to use;
- Not suitable for a large organization with more than 1000 people.

BambooHR strives to assist the workflow as much as possible by extracting reports and reports [1]. The application monitors the time the employee has worked and offers secure storage of the data in the system. A big advantage of "BambooHR" is the ability to integrate third-party software. In this way, the capabilities of the product are expanded without further complicating its logic. However, the product has a limit on the number of employees a business can manage in the system. Like most such developments, there is a monthly fee that increases with each employee.

"IceHRM" is one of the simplest and most effective information systems due to its security and accessibility. Most companies prefer IceHRM because of its centralized support, which makes managing the company and its resources easy. It has a rich user interface that makes it extensible and customizable. "IceHRM" provides the following functionalities:

- Attendance management;
- Cost management;
- Payroll processing;
- Work time tracking;
- Recruitment of candidates;
- Performance review;
- Email integration;
-Information security.

Advantages:

- Convenient for recruiting;
- With its professional version, the software can be deployed locally on the users' system;
- Easy to configure and good customer support.

Disadvantages:

- Some functions are difficult to understand;
- Too many features can sometimes confuse users.
- Some features do not work in the offline version.

"IceHRM" offers a rich interface and multiple functionalities, such as employee time tracking [1]. The big advantage of this product is the automation of monthly salaries, the possibility of insurances and recruitment of candidates. "IceHRM" uses AES 256 data encryption. The software has a 45-day trial period, after which a monthly fee must be paid based on the number of employees in the company. 3D CAD data of a part are imported into the procedural software of the printer EOSINT M 270. Software designed to the data preparation allows choosing the appropriate thickness of production layers with regard to accuracy / resolution and speed of production (0.020 mm or 0.040 mm – thinner layer means higher accuracy, but longer production time) [2].

2. Design of Desktop Employee Management System

The phase of desktop information system development includes: 1) creating a database and 2) design of an encryption algorithm using a special algorithm for creating a key. The main goal of the development is to ensure protection, both at the entrance to the system and in the transfer and storage of data.

The designed information system uses database with 4 tables: TASK_PRIORITIES, TASK_STATES, EMPLOYEES, TASKS_ARCHIVE (Fig. 1).

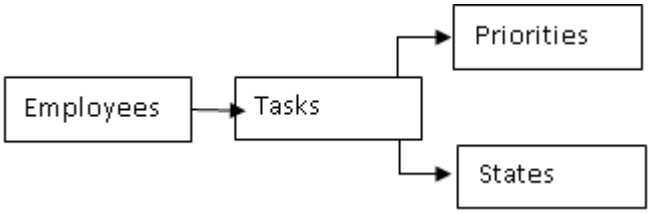

Fig. 1 *Table Relations*

The system must include the following safeguards:

- Control of access to the system by filling in the personal identification number and password, individual for each employee;
- Control over the number of failed login attempts.
- Ensuring the possibility of secure communication between the application and the server;
- Ensuring protection of input data through irreversible encryption of the password with a specially created system key and measures against SQL injections.

The system must include the following levels of access:

- Employees;
- Executives or managers;
- Directors.
- Administrators;

The information system should include information on:
- Introduced tasks;
- Registered users;
- Entered task priorities;
- Entered task states.

Employees must have access to the following functionalities:
- View the data entered for them in the system.

Managers must have access to the following functionalities:
- View the data entered for them in the system;
- View the tasks assigned to them and edit only their status.

Directors must have access to the following functionalities:
- View the data entered for them in the system;
- View, add, edit and delete all tasks;
- Review of all registered users in the system.

Administrators must have access to the following functionality:
- View the data entered for them in the system;
- View, add, edit and delete all tasks;
- View, add, edit and delete all users in the system;
- Setting task status types and task priority types.

Four different levels of access are available in the system (Fig. 2):
- employees;
- supervisors or managers;
- directors;
- administrators.

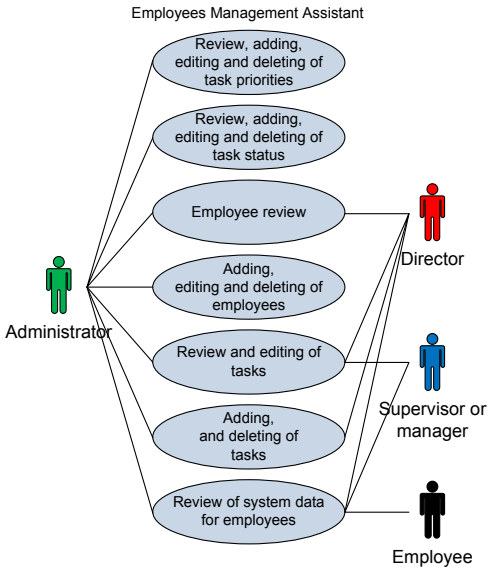

Fig. 2 Use Case Diagram of System

3. Protection types. Encryption algorithm

The current development ensures data protection through the following methods:
- Control of access to the system, by entering the personal identification number and password;
- Control of entered data to protect against SQL injections;
- Password length control;
- Encryption of the access password;
- Ability to maintain an encrypted connection between the application and the server;
- Control of the number of attempts to enter the system;
- Blocking of the account in case of three incorrectly entered passwords.

The access control to the system is achieved with the following steps:

1. When entering the employee's personal identification number and password, it is checked whether the personal identification number is only numbers and 10 characters long, and whether the password is more than 8 characters.

2. If the validation from step 1 is successful, the system opens a connection to the database. It searches for an entry in the table for employees by the entered social security number. If it finds such a record, it reads it and loads it into the system memory.

3. If the record is successfully read, the status is checked to see if it is active.

4. If the status is active, the entered password is encrypted using the same algorithm and key that were used to encrypt the password stored in the database.

5. If the encryption is successful, the two encrypted strings are compared: the entered password and the one loaded into memory from step 2.

6. If there is a match, the employee enters the system. The counter for failed login attempts is reset. Its database ID and privilege level data remain loaded in memory until the application is closed.

In order to provide protection against Traffic Interception attacks, an encryption method has been developed with a key created uniquely for the system [3],[4]. Password encryption is achieved using PBKDF2 (Password-Based Key Derivation Function 2) with 10,000 iterations (Fig. 3) as recommended by NIST (National Institute of Standards and Technology) in their publication "SP800-63B-3" from 02/03/2020. A system-unique key is added to the encryption algorithm for the uniqueness of each user's encrypted password. This also adds an extra layer to security. It is 128 bits or 16 bytes long, and the recommended size from the latest NIST publication is 32 bits or 4 bytes. Entered passwords must be 8 characters long as recommended by NIST. Password encryption is an irreversible process achieved through HMAC (Keyed Hash Message Authentication Code) and the SHA-512 (Secure Hash Algorithm 2) algorithm, using 64-bit words, as opposed to SHA-256, which uses 32-bit.

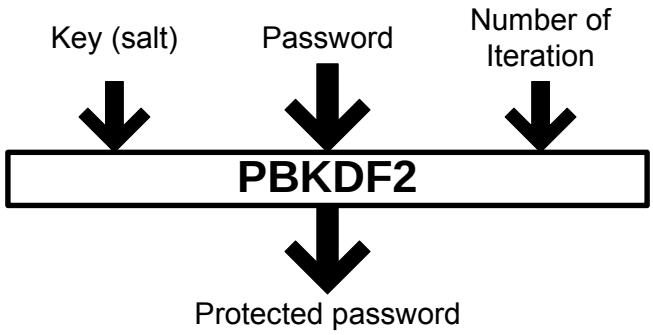

***Fig. 3** A method to store the password in the system*

The unique key is generated when a new user is registered in the system. It is formed from the current date and time of registration in seconds and the last three digits of the EGN in reverse order. The date is a fractional number and the whole part is divided by the fractional part. The three parts: the whole number of the date and time, the fractional number of the date and time and the three digits of the TIN in reverse order, are combined into one common string, separated by a dash, in the order of enumeration. For an example of creating a key, let's assume that the current date is 17.07.2021 and the last 3 digits of the personal identification number are 123. The date in seconds will be 44394,473993. The generated key will have the form: "44394-473993-321". This key is

recorded in the database as a "unique identification key" to the respective user.

4. System Architecture

The current development is based on the Document-View architecture. The document stores the data, manages its printing, and coordinates the updating of multiple data views. The view displays the data and manages the employee's interaction with it, including selecting, adding, editing, and deleting.

In this model (Fig. 4), the document reads and writes data to persistent storage. A document may also provide an interface to data such as that in a database. A separate view object controls the display of data. It can be from displaying the data in a window for user selection to view, add, edit and delete data. The view receives data from the document and reports to the document any changes to the data.

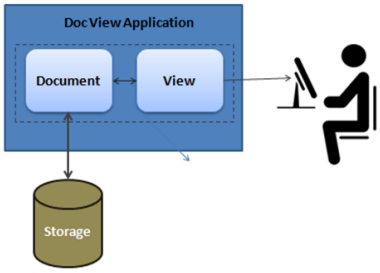

Fig. 4 *The Architecture document View.*

The architecture are the following base classes:

- CDocument – a class for supporting objects used to store or control program data and provides the basic functionality of documents defined by the programmer.

- CView – provides the basic functionality of views. A view is attached to a document and acts as an intermediary between the document and the user. The view renders the document data on the screen and interprets user input as operations on the document. The current development uses the CListView class, a descendant of CCtrlView, which in turn is a descendant of CView, to visualize the data. CListView simplifies the use of the list control and CListCtrl, the class that encapsulates the list control functionality, with the MFC document view architecture.

- CDialog – this class is used to work with a dialog.

- CFrameWnd – supports objects that provide the frame around one or more document views. In current development, it is inherited from CMDIFrameWnd, which in turn is inherited from CMDIFrameWndEx. CFrameWnd's successors build on its base functionality.

- CDocTemplate – maintains an object that coordinates one or more existing documents of a given type and manages the creation of the correct document window, view, and frame objects for that type. It can be either CSingleDocTemplate or CMultiDocTemplate, depending on whether the system uses one or several different documents for different data.

In current development, "Smart" classes have been developed, inheriting from the base classes and upgrading them according to the needs of the application. Additional classes added:

- CSmartTable to work with the data (read, add, edit and delete) directly from a specific table in the database.

- CSmartDataAccessor takes care of the conditions under which it is read, written, deleted, takes care if changes are required on the other tables, except the one on which it is the main one for the class.

4. Conclusion

The current development offers an information system with access control and different levels of access for each profile. It provides information security against some of the better-known cyber-attack methods. The software allows visualization of reports on registered employees and their tasks. A mechanism has been developed to add different priorities and states to tasks, which allows freedom to customize the system according to the needs of the owner and. Despiting the available functionalities, the system can be improved with the following developments:

- Encrypt server access profile password from ServerConfig.ini via AES 256.

- Protect against "Password Spraying" attacks by adding a mechanism to change the password in a certain period.

3. References

1. K. E. Pearlson, C. Saunders, D. F. Galletta, *Managing and Using Information Systems: A Strategic Approach, 7th Edition*, Wiley, ISBN: 978-1-119-56115-6, (2019)
2. K. Sousa, Effy Oz, *Management Information Systems, Seventh Edition*, Cengage Learning EMEA, ISBN: 9781305172180, (2014)
3. R. Maier, Knowledge Management Systems, *Information and Communication Technologies for Knowledge Management*, Springer, ISBN: 978-3-540-71408-8, (2007)
4. R. Stair, G. Reynolds, *Principles of Information Systems 13th Edition*, Cengage Learning, ISBN: 978-1305971776, (2017)