WJCMS

Wasit Journal of Computer and Mathematics Science

Journal Homepage: https://wjcm.uowasit.edu.iq/index.php/WJCM

e-ISSN: 2788-5879 p-ISSN: 2788-5879

Data encryption for bank management system

Asst.Prof.Dr. Abdul Syukor Mohamad[1]*

[1]Faculty of Computer Science/Universiti Teknikal Malaysia Melaka (UTEM)/Malaysia

*Corresponding Author: Asst.Prof.Dr. Abdul Syukor Mohamad

DOI: https://doi.org/10.31185/wjcm.83

Received: August 2022; Accepted: October 2022; Available online: December 2022

ABSTRACT: Data breaches are perhaps the single most significant risk that banks face today. In the financial industry. Aside from the direct costs involved in these breaches, like lost funds, increased insurance expenses and fines, and penalties, institutions also must contend with the indirect costs. Loss of reputation and consumer trust are not easy to quantitatively measure, but it's guaranteed the price is very high.

Unfortunately, banks need to face an ever-evolving set of threats because of the nature of their business. They hold sensitive financial records that bad actors are known to target, and with methods that are always shifting. Consequently, security cannot be static to meet these threats. It must be a continuous process to monitor and respond to new risks as they emerge. Also, compliance needs to be built into the overall process to meet the stringent privacy regulations for the financial industry. Data security for banks is undoubtedly a challenge, but a holistic approach may make it easier to manage.

Keywords: data encryption, bank management, database, ER

1. INTRODUCTION

As we know the financial industry is among the most regulated in the world. There are strong data security requirements for banking and financial industries due to the sensitive and private data that they deal with.

The banking sector has been under attack for hundreds of years. First, it was the physical theft of monies. Then it was computer fraud. Today, it's not only fraud but hacks into servers to obtain a customer's personally identifiable information (PII). Hence, the reason why security in banking is of utmost importance. As individuals and companies perform most transactions computer, the risk of a data breach increases daily. This is why there's a greater emphasis to examine the importance of security in banking sector processes [1].

In today's world, banks have to think big when it comes to security. It is no longer enough to secure the system and think everything is safe. With hackers attacking major insurance companies, universities, and even the federal government, a multi-layer approach to data and system security is no longer just suggested, it's necessary [2].

Managing banking threats and monitoring data is much more complex today than it was in the past. Historically, banks only had to control access to physical paper records by placing them in a vault and protecting their perimeter. While the digital landscape made banking much more convenient, it also opened it up to a whole host of threats. Stores of data with valuable personal information attracted the attention of cybercriminals who used a range of attacks to gain access.

Those that don't encrypt put themselves at risk for stiff government penalties, fines, lawsuits, and more.

The obvious reason for the importance of security in banking sector transactions is to protect customer assets. PII can be redirected to other locations and used for malicious activities.

Not only does this affect the customer. It also greatly harms the bank while they attempt to recover the data. When it's taken hostage, the bank might need to pay hundreds of thousands of dollars to release the information. In turn, they lose

the trust of their customers and other financial institutions [3].

That's not the only thing that happens when steps for security banking aren't implemented. The customer needs to cancel all their cards and start new accounts – possibly at another bank. And though their funds are protected by the FDIC, it doesn't stop criminals from trying to use their PII [4].

2. LITERATURE

A database is a collection of information—preferably related information and preferably organized. A database consists of the physical files you set up on a computer when installing the database software [5].

By definition, a database is a structured object. It can be a pile of papers, but most likely, in the modern world it exists on a computer system. Databases and database technology are having a major impact on the growing use of computers. It is fair to say that databases play a critical role in almost all areas where computers are used, including business, engineering, medicine, law, education, and library science, to name a few [6].

In a centralized database, all the data of an organization is stored in a single place such as a mainframe computer or a server [7]. Users in remote locations access the data through the Wide Area Network (WAN) using the application programs provided to access the data. The centralized database to the system, therefore could easily become a bottleneck. But since all the data reside in a single place it easier to maintain and back up data Furthermore, it is easier to maintain data integrity, because once data is stored in a centralized database, outdated data is no long available in other place. A centralized database is one that has all the information of the database stored in one physical location within a network [8].

Database design is the process of producing a detailed data model of database. This data model contains all the needed logical and physical design choices and physical storage parameters needed to generate a design in a data definition language, which can then be used to create a database. A fully attributed data model contains detailed attributes for each entity [6] .

The process of doing database design generally consists of a number of steps which will be carried out by the database designer. Usually, the designer must :

- Determine the data to be stored in the database .
- Determine the relationships between the different data elements .
- Superimpose a logical structure upon the data on the basis of these relationship .

3. BANK DATABASE DESIGN

Database designs also include ER (entity-relationship model) diagrams. An ER diagram is a diagram that helps to design databases in an efficient way . Attributes in ER diagrams are usually modeled as an oval with the name of the attribute, linked to the entity or relationship that contains the attribute.

4. BANK MANAGEMENT DATABASE DESIGN

A database management system (DBMS) is a collection of programs that enables users to create and maintain databases and control all access to them. The primary goal of a DBMS is to provide an environment that is both convenient and efficient for users to retrieve 9 and store information Figure (2.2). DBMS is software designed to store and manage database to gets :-

- Data independence and efficient access .
- Reduced application development time .
- Data integrity and security .
- Uniform data administration .
- Concurrent access and recovery .

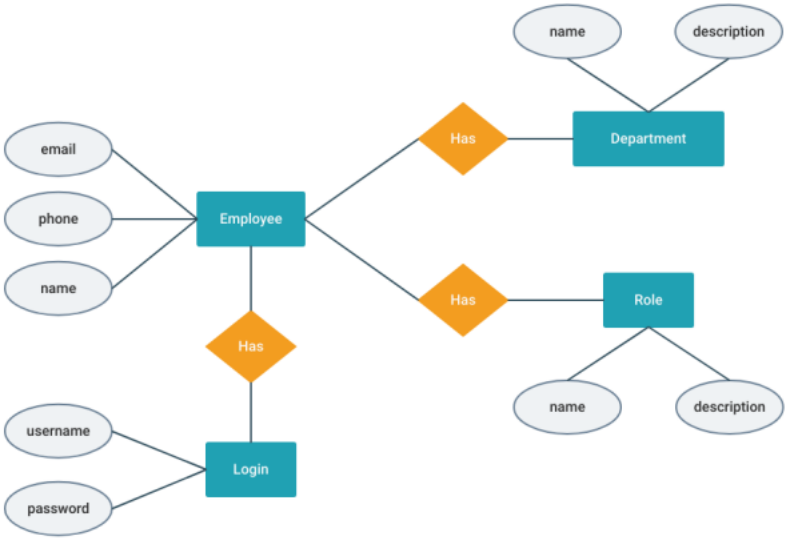


FIGURE 1. bank database

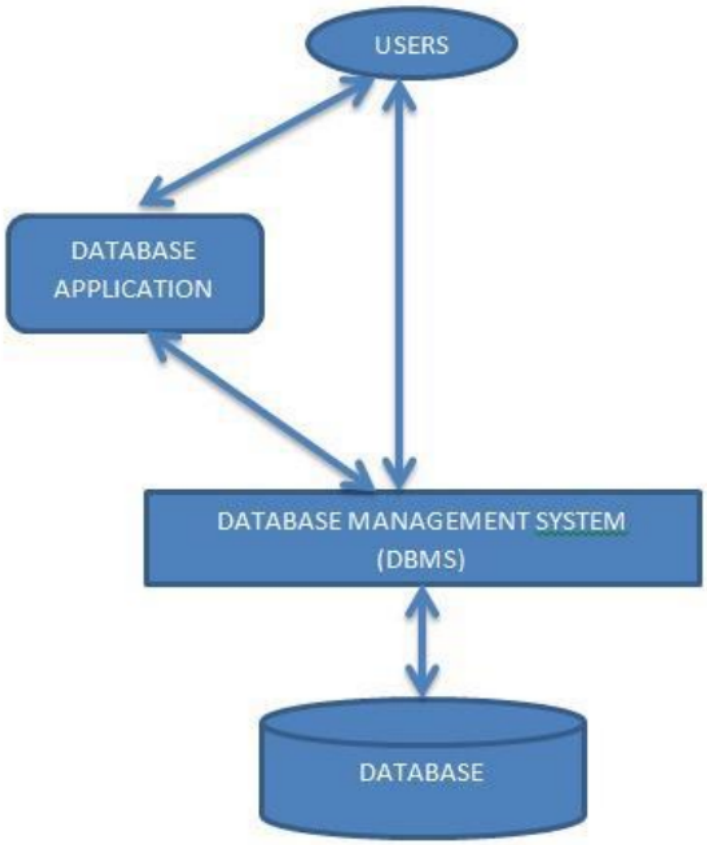
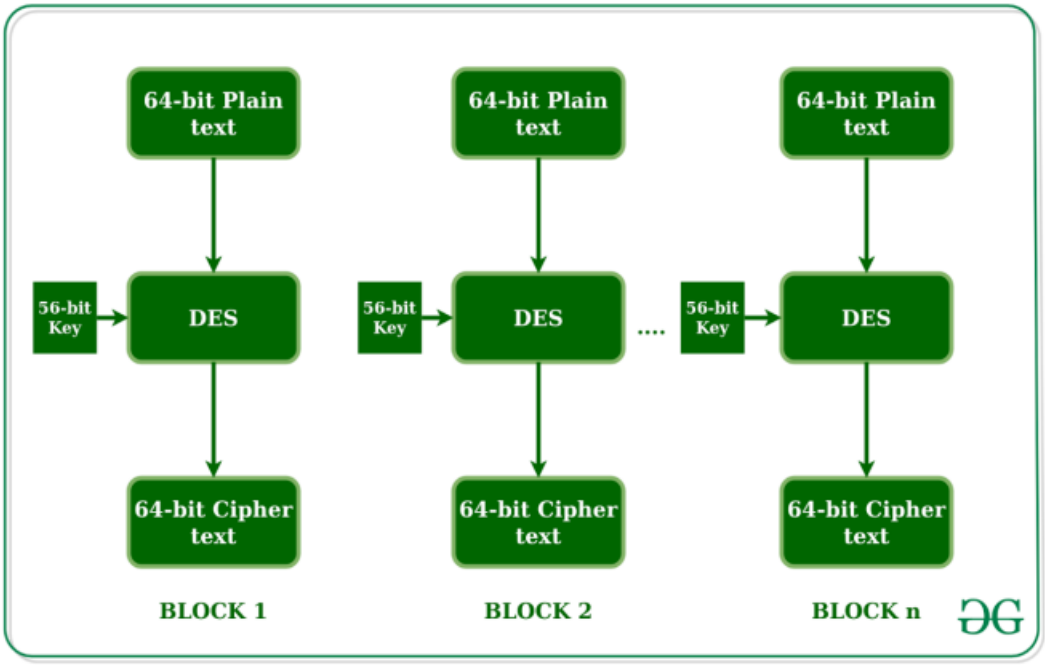


FIGURE 2. bank management system

5. DATA ENCRYPTION STANDARD (DES)

Data encryption standard (DES) has been found vulnerable against very powerful attacks and therefore, the popularity of DES has been found slightly on the decline. DES is a block cipher and encrypts data in blocks of size of 64 bits each, which means 64 bits of plain text goes as the input to DES, which produces 64 bits of cipher text. The same algorithm and key are used for encryption and decryption, with minor differences. The key length is 56 bits. The basic idea is shown in the figure



We have mentioned that DES uses a 56-bit key. Actually, the initial key consists of 64 bits. However, before the DES process even starts, every 8th bit of the key is discarded to produce a 56-bit key. That is bit positions 8, 16, 24, 32, 40, 48, 56, and 64 are discarded

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32
33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48
49	50	51	52	53	54	55	56	57	58	59	60	61	62	63	64

Thus, the discarding of every 8th bit of the key produces a 56-bit key from the original 64-bit key. DES is based on the two fundamental attributes of cryptography: substitution (also called confusion) and transposition (also called diffusion). DES consists of 16 steps, each of which is called a round. Each round performs the steps of substitution and transposition.

6. BANK SYSTEM FRAMEWORK

Banking System consists of database (including several tables) and several forms connected with the tables in the database, these tables information displaying about Banking management and these entire table displaying to the admin these

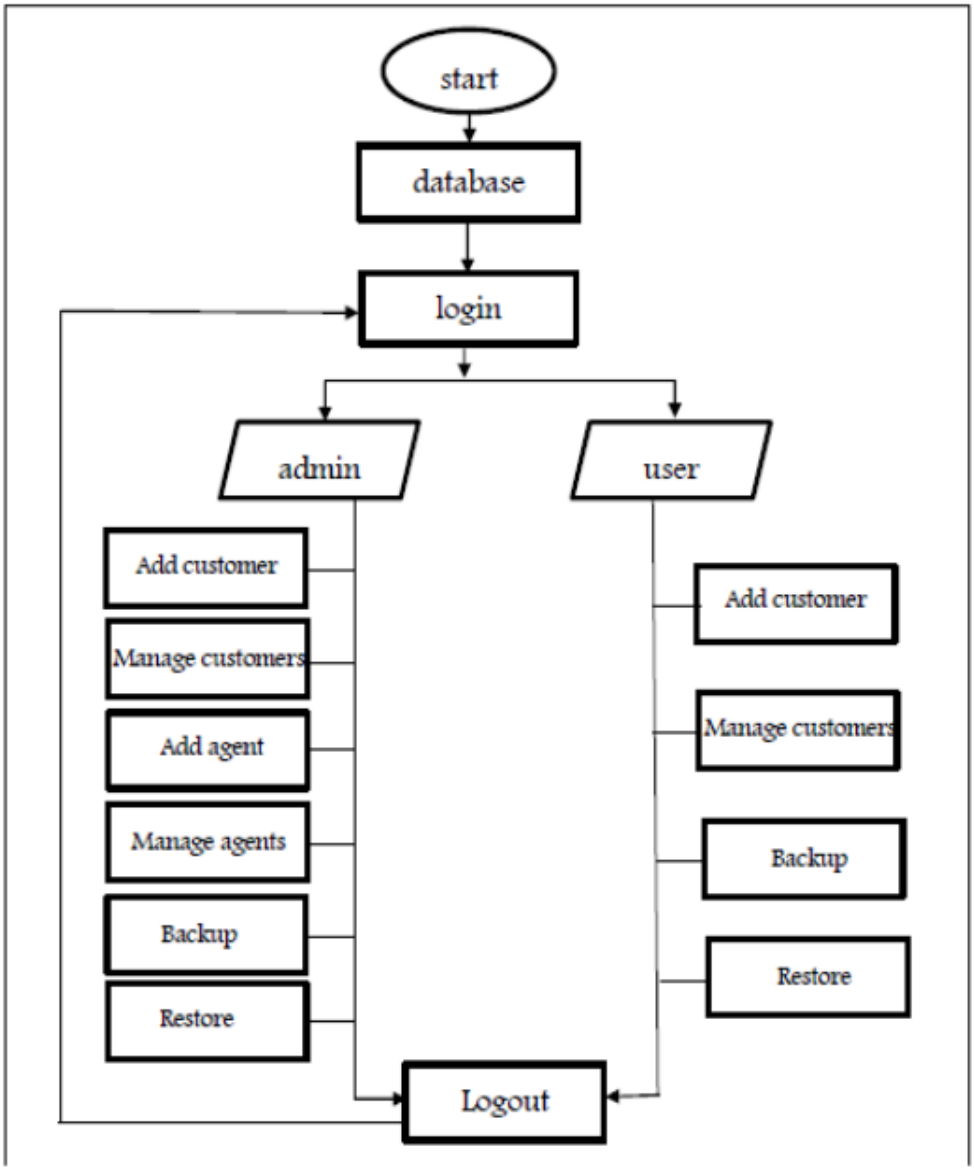


FIGURE 3. **bank framework**

7. CONCLUSIONS

The developed system is capable of storing data and managing processes bank in bank. Encryption customers data is one of the functions of the system. The model was successfully applied by conducting an analysis of each Item, as it was part of the function of the system.

The integrity and confidentiality of the customers data and passwords stored in the bank was successfully secured using DES algorithm by encrypting all the data customers and passwords in the database. Only items selected for after displayed by the data grid view will be decrypted. Main functions like adding, deleting, uploading and searching items are embedded in the system. With the developed system. Full implementation of the developed system is recommended.

In order to allow for future expansion, the system has been designed in such a way that will allow possible modification as it may deem necessary by the Bank management, whenever the idea arises.

FUNDING

None

ACKNOWLEDGEMENT

None

CONFLICTS OF INTEREST

The author declares no conflict of interest.

REFERENCES

[1] G. Powell, “Beginning Database Design. s.l,” 2006. Wiley Publishing.
[2] T. M. Connolly, “Database System, Design, Implementation Management,” 2005.
[3] “Introduction to Database Models. TAFE NSW Sydney eLearning Moodle.” https://sielearning.tafensw.edu.au.
[4] “Database Management System,” http://slideplayer.in.th. [Online] http://slideplayer.in.th/slide/ 2049285.
[5] G. Verma and Mahapatra, “Database Management System,” 2005.
[6] E. Biham and Shamir, “Adi Defferential cryptanalysis of the data encryption standard.” springer Verlag.
[7] K. W. Campbell, J. Michael, and Wiener, *DES is not a group*. 1992.
[8] A. F. Neamah, “Flexible Data Warehouse: Towards Building an Integrated Electronic Health Record Architecture,” *2020 International Conference on Smart Electronics and Communication (ICOSEC)*, pp. 1038–1042, 2020.
[9] S. A. Diwan, S. Perumal, and D. S. Siber, “Smart e-service implementation as mobile agent in a smart e-government platform,” *International Journal of Applied Engineering Research*, vol. 11, no. 7, pp. 5250–5255, 2016.