UNIVERSITI TEKNOLOGI MARA

SECURING THE HUMAN RESOURCE DATABASE SYSTEM USING ENCRYPTION AND DECRYPTION (AES-128)

NOR ASYIKIN BINTI ALIM

SUPERVISOR:
ENCIK KAMARUL ARIFFIN BIN ABDUL BASIT

BACHELOR OF COMPUTER SCIENCE (HONS.)
NETWORKING AND DATA COMMUNICATION

JANUARY 2021

SUPERVISOR APPROVAL

SECURING THE HUMAN RESOURCE DATABASE SYSTEM USING ENCRYPTION AND DECRYPTION (AES-128)

By

NOR ASYIKIN BINTI ALIM

2019472714

This thesis was prepared under the supervision of the project supervisor, Encik Kamarul Ariffin Bin Abdul Basit. It was submitted to the Faculty of Computer and Mathematical Sciences and was accepted in partial fulfillment of the Bachelor of Computer Science (Hons.) Data Communication and Networking.

Approved by

……

Encik Kamarul Ariffin Bin Abdul Basit

Project Supervisor

JANUARY 14, 2021

STUDENT DECLARATION

I certify that this thesis and the project to which it refers is the product of my own work. Any idea or quotation from other people's work, published or otherwise, is fully acknowledged according to the discipline's standard referring practices.

……..

NOR ASYIKIN BINTI ALIM

2019472714

JANUARY 14, 2021

ACKNOWLEDGMENT

Alhamdulillah, and because of His Almighty and His utmost blessings, thank you to Allah, I was able to finish this research within the specified time frame. First of all, my special thanks go to my supervisor Encik Kamarul Ariffin Abdul Basit for always directing my project creation process, offering the best opinion and proposal. All of the patience and understanding are given in guiding me to accomplish this proposal could only be replaced with million thanks.

Finally, an honourable mention goes to families and friends, especially my parents, who have given me all the support from various aspects such as money sprite and confidence level throughout this journey.

ABSTRACT

Data security is one of the most crucial and a major challenge in the digital world. Security, privacy and integrity of data are demanded in every operation performed on internet. Whenever security of data is discussed, it is mostly in the context of secure transfer of data over the unreliable communication networks. But the security of the data in databases is also as important. In this paper we will be presenting some of the common security techniques for the data that can be implemented in fortifying and strengthening the databases. Advanced encryption Standard (AES), could be a scientific discipline rule that may be used for secured data and communication in an organization, it uses same key that's isobilateral key for transmission additionally as reception. The AES rule is capable of using cryptographic keys of 128, 192, and 256 bits, this paper implement AES block cipher of 128 bits and developed with Java as a front-end client machine and PHP MYSql used for the database as a back-end machine.

TABLE OF CONTENT

CONTENT	PAGE
SUPERVISOR APPROVAL	ii
STUDENT DECLARATION	iii
ACKNOWLEDGMENT	iv
ABSTRACT	v
LIST OF FIGURES	viii
LIST OF TABLES	viii
CHAPTER 1	1
1.1 Project Background	1
1.2 Problem Statement	2
1.3 Objectives	2
1.4 Scopes	3
1.5 Significant	3
CHAPTER 2	4
2.1 Database system	4
2.1.1 Database Security	4-5
2.1.2 importance of database security	6
2.1.3 Security controls for database security	7-8
2.2 Encryption and decryption	9
2.2.1 Types of encryption	10-11
2.2.2 Differences between symmetric and asymmetric	12
2.2.3 Advanced Encryption Standard (AES)	13
2.2.4 Description of the ciphers	14
2.2.5 High-level description of the algortihm.	15
2.2.6 Security in Advanced Encryption Standard (AES)	16
2.2.7 Side-channel attacks in Advanced Encryption Standard (AES)	16
2.3 Related works	17-30
CHAPTER 3	31
3.1 Project Methodology Framework	31-33

3.1.1 Information Gathering **34**

3.1.2 Information Analysis **34**

3.1.3 Design **34**

3.1.4 Implementation **34**

3.1.5 Testing **35**

3.1.6 Evaluation and Validation **35**

3.1.7 Documentation **35**

3.2 Proposed Design **35**

3.2.1 Flowchart **36**

3.2.2 Interface Design **36-38**

3.3 Experimental Design **39**

4.0 Hardware and Software Requirements **40**

4.1 Software **40**

5.0 Project Schedule **41**

References **42-43**

LIST OF FIGURES

Figure 1: Encryption **9**

Figure 2: Decryption **9**

Figure 3: Symmetric Encryption **10**

Figure 4: Asymmetric Encryption **11**

Figure 5: Schematic of AES Structure **14**

Figure 6: Proposed Design **18**

Figure 7: Interface of the system **18**

Figure 8: Unencrypted Data **19**

Figure 9: Encrypted Data **19**

Figure 10: Architecture of Lavarel **22**

Figure 11: The upload process designed to ensure the file entegrity. **23**

Figure 12: The download process designed to ensure the file integrity. **23**

Figure 13: Encryption within database **25**

Figure 14: Encryption at application layer **27**

Figure 15: Research Methodology Framework **31**

Figure 16: Flowchart **36**

Figure 17: Admin welcome page **36**

Figure 18: Admin Login Page **37**

Figure 19: Admin Page **37**

Figure 20: Employee Salary Details **38**

Figure 21: Employee Data Inserted **38**

Figure 22: Encrypted Data **38**

Figure 23: Encryption and Decryption Flow Process **39**

LIST OF TABLES

TABLE		PAGE
Table 2.1	**Advantages and disadvantages of protection**	**27**
Table 2.2	**Related Works**	**28-30**
Table 3.1	**Research Methodology Framework**	**32-33**
Table 4.0	**Hardware and Software Requirements**	**40**

CHAPTER 1

INTRODUCTION

1.1 Project Background

Computers and technology have become a part of human life. In our daily lives, computer plays a major role. We use them for education, research, shopping, news, weather, social networking and so on. For integrated business processes, the rapid growth and proliferation of information technology has provided many opportunities.

In the digital world, data protection is one of the most important and substantial challenges. This information may be sensitive and confidential and may be subject to strict agreements on the protection of privacy, including those referred to above. In any operation carried out on the Internet, protection, privacy and data integrity are needed. When data protection is addressed, it is mainly in the sense of securing data transmission over insecure communication networks. But data security in databases is also as important as that. Basically, database security is used to safeguard the databases and the information they contain from compromise in any form of security. Sufficient security of the database prevents data from being lost or compromised, which may have serious consequences for the company or the individual himself. There are many different types of databases today, not only traditional relational databases, but also several other architectures designed to handle various data types.

A data violation goes undiscovered for an average of 197 days, according to the 2018 Cost of a Data Breach study by the Ponemon Institute. The data breach needs a further 69 days to be remedied. The damage is already done by the moment the security failure is discovered and fixed. Unrestricted access to databases full of valuable data will be available to the criminals responsible. In many instances, until years later, an organization or company won't even know they've been violated. Data violation results from a cyberattack that allows cybercriminals to gain unauthorized access to the computer system or network and to steal the private, sensitive or confidential personal and financial data contained within the customers or users. Within the system code, these vulnerabilities lie hidden. These vulnerabilities lie hidden within the code of the system. Common cyberattacks used in data breaches are spyware, pishing, broken or misconfigured access control and many more.

1.2 Problem Statement

Database security is a growing concern evidenced by an increase in the number of reported incidents of loss of or unauthorized exposure to sensitive data. Database security refers to the collective measures used to protect and secure a database or database management software from illegitimate use and malicious threats and attacks. Authorization and authentication are to major processes that are being used to protect data from the front end that is being accessed by the user, where the authorization means whether a person has the rights to access the data or not. While authentication means identifying the user if he/she is the owner of the data which is generally done by the use of username or passwords. Another important way to protect the data is by encrypting the data that has been saved in the databases. In providing data confidentiality to data stored within the databases, encryption plays an important role. However, the problem with the adoption of standard encryption methods is that they can cause damage to existing databases and change the data format as well.

In order to preserve the encryption method, formats of the data as well as the length of the input data is by applying Advanced Encryption Standard (AES) into the database.

1.3 Objectives

The main objectives of this project are as below:

1. To study the AES algorithm technique
2. To implement Database Encryption/Decryption using AES algorithm.

1.4 Scopes

This project will focus on providing the confidentiality of data against attackers in the organization where the data in the database will be encrypted. Other than that, this project also focused on database Encryption/ Decryption in SQL server. The keys used to decrypt the text can be 128-, 192-, or 256-bit long. The 256-bit key encrypts the data in 14 rounds, the 192-bit key in 12 rounds, and the 128-bit key in 10 rounds. Each round consists of several steps of substitution, transposition, mixing of plaintext, and more.

1.5 Significant

This project will help server admin to ensure the confidentiality by protecting the data from unauthorized exposure. It is also to sustain access control mechanism through encryption/ decryption scheme.

CHAPTER 2

LITERATURE REVIEW

A literature review is a type of reviewing articles. A literature review is a scholarly paper that presents the current knowledge including substantive findings as well as theoretical and methodological contributions to a particular topic. Literature review will provide a guide to that particular topics. It is often associated with academic-oriented and will be likely to be found in academic journals and not to be confused with book review Most often associated with academic-oriented literature, such reviews are found in academic journals and are not to be confused with book reviews, which may also appear in the same publication. Literature reviews are a basis for research in nearly every academic field. Review usually precedes the methodology and results sections of the work.

2.1 DATABASE SYSTEM

A database is a collection of information typically stored in a computer system that have been organize so that it can be easily accessed, managed, controlled, modified and updated. Computer database usually containing data records or files, containing information of customers, employer, employee, etc.

2.1.1 DATABASE SECURITY

In this era of modernization, most of our works done by the computers. From chatting with friends on social networking, ordering food, to making online payments through Net Banking, everything is done online through computers. Since everything is done by computers, database security also growing concern. The number of reported incidents of data loss or unauthorized

exposure to sensitive data is rapidly increasing. As the amount of data collected, retained and shared expands, the security of database also should be tightly monitored. The Defense Information System of the US Department of Defense (2004), in its database Security Technical Implementation Guide, states that the database security should provide controlled, protected access to the content of a database as well as preserve the integrity, consistency, and overall quality of data. People in the computing disciplines must develop an understanding of the issues and challenges related to the database and must be able to identify the possible solutions to the certain problems. (Education, 2019)

Information can be considered as a company's most valued assets and should be protected from unauthorized users. In the past, mostly companies allowed very limited access to corporate information. Today, the number of companies making their corporate information available to remote users through the Internet is increasing. Users are given access to corporate information through web-enabled databases. (Pressbooks, n.d.)

In the computing discipline curriculum (Looker, n.d.), database security is an important topic to be included in the introduction of database or introductory computer security course. This is because, securing database is very important in protecting the users sensitive data from being exploited. To provide a good, strong, and more efficient method to prevent unauthorized users in accessing the database, manage computer risk, prevent weakness in security management and additional measures of security by developing a method to encrypt sensitive data before storage in the database. (Looker, n.d.)

2.1.2 IMPORTANCE OF DATABASE SECURITY

Database security is more than just important not only for large business but also for small business. Hackers do not care how large the business is or what industry are you in, hackers only looking for vulnerabilities that they can exploit. Unfortunately, mostly small businesses lack of knowledge and experience with database security which can lead their data being expose to the public. Databases are used to provide personnel information, customer information, credit card numbers, financial data, etc. The information is very sensitive and highly confidential (Maurer, 2015) .It is depending on the companies to make avail their information assets online through databases. However, the policy must be followed which is dividing the level of users with to which extent they can asset the information. It is a vital to not to give the opportunities to mischievous intruders. It is essential to any company with any online component. Database security will help to prevent data loss or compromised. Database security also can help protect companies from: (UKEssays, 2018)

- Database injection attacks
- Excessive privileges
- Unmanaged sensitive data
- Backup data exposure
- Weak authentication

2.1.3 SECURITY CONTROLS FOR DATABASE SECURITY

Every cybercriminal has the same intend when attacking a particular databases and it is to gain access to the possible system settings, sensitive data through bypassing security implementations. (Kapersky, 2021).

Hackers also can attack through harmful software, script or other systems involving the use of malware or viruses. This behaviour could grant the hackers unauthorized access to the database systems. To make sure it doesn't happen, various controls are in place. (2019)

Security Controls For Database

- Data in Transport

  It is referring to the security system that will make sure that no one can read or interpret the data when it is being transferred between various servers or configuring networks. The main objectives if this system security is to limit any potential breach or unauthorized access to the server. This data setting is also known as Access Control.

- Authentication

  This type of data security is next in line and should be in effect after the data is being transferred in the transport protocol. In general , this system security is a way to verify the authorized user. There are many different methods that can be used for authentication, such as using multi-factor authentication method or else using two-factor authentications which is authenticating via username and password. This is also considered as granting access authenticating the users as well.

- Authorization

  The next type of database security is authorization. This layer of security specifically what elements the dedicated user has access to. This security step more crucial of them all because it makes sure no one is peeking or stumbling in the unchartered

areas or exploring the areas that they aren't supposed to be looking for.

- Data at rest

  After the data is being shared or accessed by the users, it remains within the server and known as data at rest. The data remain sit even after the server is shut off. Unique encryption will be deployed to ensure that the data is still encrypted even when it is out of reach.

- Auditing

  Auditing the system is a must to ensure what we had in the inventory, such as delicate information that was lost in the attempt of attack. Continuous audit reports should be done to get the proper record at the end.

- Recovery

  Recovery is also considered as the primary system that is related to the security of the database. Need to make sure that the backed up data is stored within the database. Also need to ensure that the backup files are fully encrypted and secured.

2.2 ENCRYPTION AND DECRYPTION

Encryption is the process of encoding plain text data into an unrecognizable and meaningless message form. Encryption does not itself prevent interference but also denies the intelligible content to a would-be interceptor. Whereas Decryption is the process of converting the meaningless message into its original form. Data is encrypted to make it safe from being breach. (TechTarget, 2020). The main objective of every encryption algorithm is to make it as difficult as possible to decrypt back the file. If a really good encryption algorithm is used, there is no possible way to try to decrypt the data. It is difficult to determine the quality of the encryption algorithm. If the algorithm looks promising, it has a chance to be very easy to break. When choosing an encryption algorithm, it is good to choose the one that has been used for a long time and has successfully resisted all attacks. (Developer, 2018)

Figure 1 : Encryption

Figure 2 : Decryption

2.2.1 TYPES OF ENCRYPTION

Two types of encryption are available, symmetric and asymmetric. Symmetric is used to encrypt more than a small amount of data when you want to. To encrypt and decrypt the data, Symmetric utilizes the same cryptographic key. Symmetric encryption is an old and well-known method and the simplest type of encryption that includes a secret key for the messages to be ciphered and deciphered. To allow them to communicate, the sender and the recipient should know the secret key that is used to encrypt and decrypt the messages. (Thakkar, 2020)There are many types of symmetric algorithm, Blowfish, AES, RC4, DES and RC5. The most widely symmetric algorithm used is AES-128, AES-192 and AES-256.

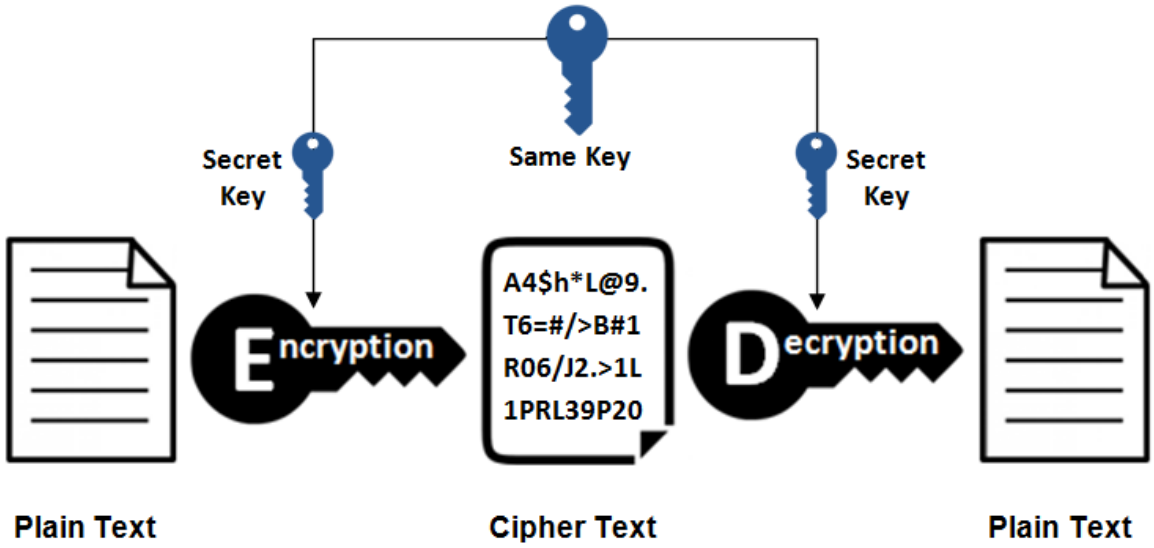


Figure 3 : Symmetric Encryption

Compared to symmetrical encryption, asymmetric encryption is also known as public key cryptography, which is a relatively new method. The notation of a key pair is used for Asymmetric encryption. To encrypt and decrypt the information, a different key is used. One key is known as a private key, which is only kept and used by the owner to decrypt the message, and the other key is known as a public key, where this key is shared between those authorized or exchanged over the internet or a large network. (TechTarget, 2020) For anyone who might want to send a message, the public key is freely accessible. Only the private key can be used to decrypt messages which are encrypted using the public key. Public key security is not required because it is made public and can be transferred over the internet. On day-to-day communication channels, asymmetric encryption is mostly used. (Fox, n.d.) The popular asymmetric key encryption algorithm includes EIGamal, RSA, DSA, Elliptic Curve Techniques, PKCS

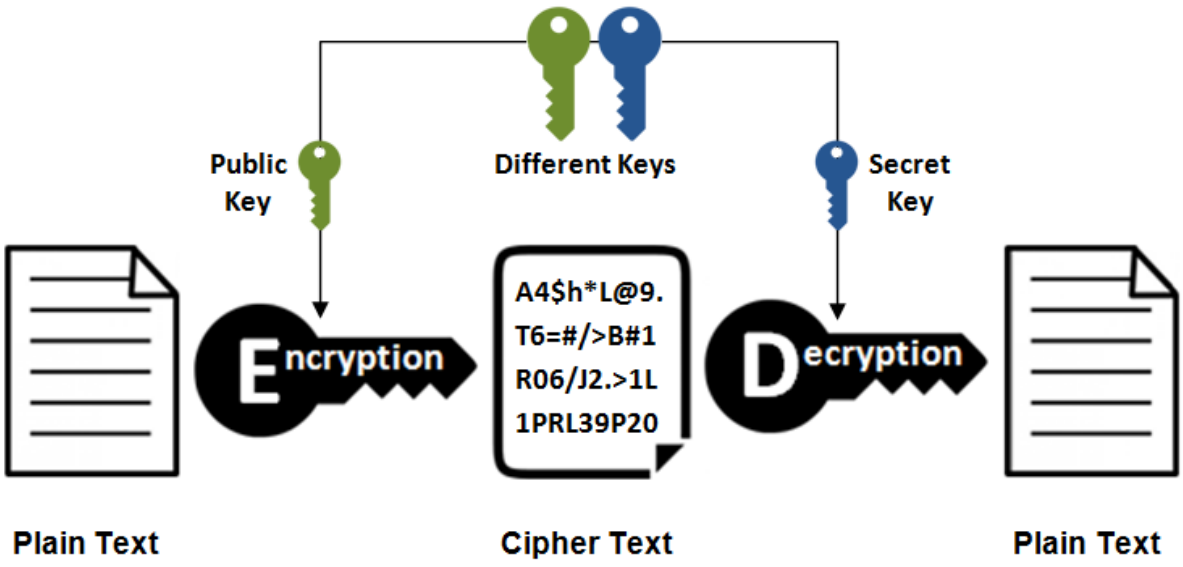


Figure 4 : Asymmetric Encryption

2.2.2 DIFFERENCES BETWEEN SYMMETRIC AND ASYMMETRIC

The differences between these two encryptions is that for both encrypting and decrypting processes, symmetric encryption uses one key. While asymmetric encryption uses the public key for encryption, the decryption process uses the private key.

The simplest and well-known encryption and decryption techniques are said to be symmetric encryption because the algorithm behind symmetric encryption is less complicated and runs faster. When transmitting data in bulk, these techniques are preferred. Using a key, the plaintext is encrypted and the same key is used to decrypt the received message at the receiving end. The host would have obtained the key through external means in the communication processes. Once an encrypted connection has been negotiated between a client and a server with an SSL certificate installed, the most common form of symmetric encryption occurs.

A new and complex mode of encryption is asymmetric encryption. Because two cryptographic keys are used to implement data security, it is complicated. It is also known to be safer than symmetric encryption. In everyday communication over the internet, this type of method is used. Digital certificates can be used to discover public keys in the client-server model. Since this algorithm is more complicated, execution takes more time than symmetry. Symmetric is therefore more suitable for use in bulk data transmission.

2.2.3 ADVANCED ENCRYPTION STANDARD (AES)

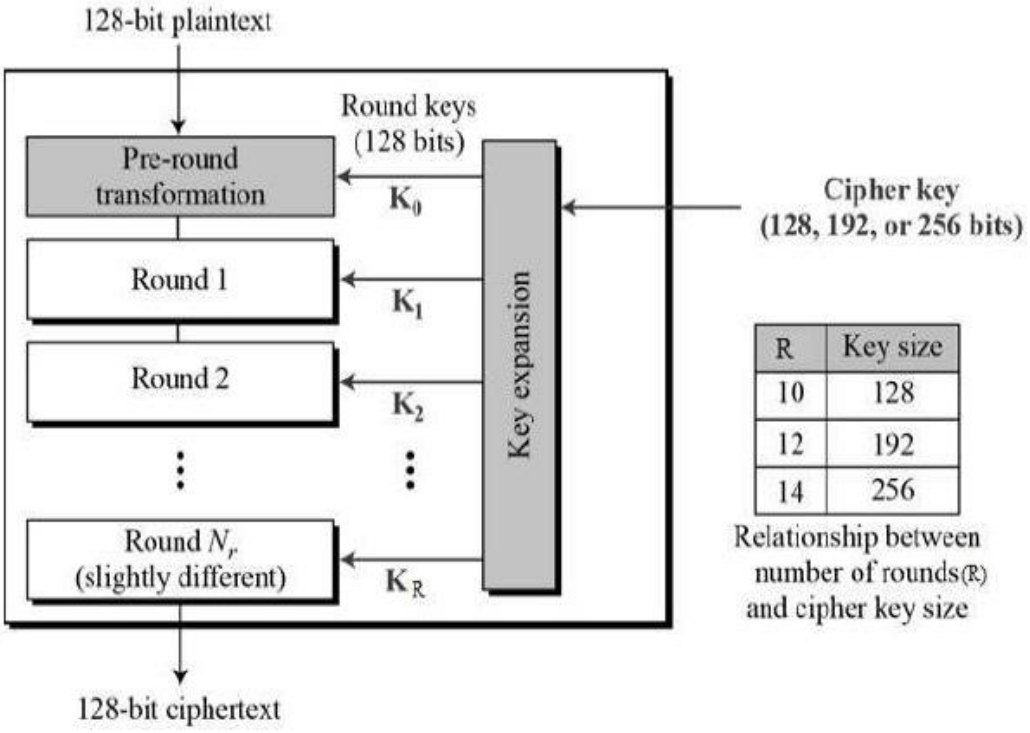
A symmetric key block cipher algorithm and the US government standard for securing and classifying encryption and decryption data is the Advanced Encryption Standard (AES). In December 2001, the Federal Information Processing Standards Publication (FIPS PUB) 197 of the National Institute of Standards (NIST) approved AES, which specifies the application of the Rijndael algorithm to all sensitive classified data.(Morris J. Dworkin, 2001) Originally, the Advanced Encryption Standard was known as Rijndael. Rijndael is a cipher family with different key and block sizes. Each one has a block size of 128 bits but three different key lengths: 128, 192 and 256 bits. (Dhandhania, 2014)

The Advanced Encryption Standard (AES) has been adopted and is now used worldwide by the US government. A better version of the Data Encryption Standard is the Advanced Encryption Standard (AES) (DES). The Advanced Encryption Standard (AES) operates simultaneously on multiple network layers. The Advanced Encryption Standard (AES) is available in many different encryption packages and is the first cipher approved by the US to be publicly accessible.(Craven, 2020)

2.2.4 DESCRIPTION OF THE CIPHERS

The Advanced Encryption Standard (AES) design is based on a design principle and is known as a network for substitution-permutation and is effective in software and hardware. Unlike DES, Feistel's network is not used by AES. AED is a Rijndael variant with a fixed 128-bit block size and 128, 192 and 256-bit key sizes. It includes a number of related activities, some of which involve replacing the inputs with specific outputs, while others involve shuffling bits around them. (wikipediacontributors, 2021)

It is interesting to note that AES converts all of its computation into bytes rather than bits. The 128 bits of the plaintext block are therefore treated as 16 bytes by AES. All of these 16 bytes are arranged in a fourth column and a fourth row to be processed as a matrix. The number of rounds in the AES is variable for the DES case and depends on the length of the key. For 128-bit keys, AES uses 10 rounds, 12 rounds for 192-bit keys and 14 rounds for 256-bit keys. A distinct 128-bit round key is used for each of these rounds, which is calculated from the original AES key. The input is called plaintext and the ciphertext is called the final output. (wikipediacontributors, 2021)



R	Key size
10	128
12	192
14	256

Figure 5 : Schematic of AES Structure

2.2.5 HIGH-LEVEL DESCRIPTION OF THE ALGORTIHM.

i. KeyExpansion – round keys will be derived from the cipher key using the AES key schedule. AES requires a separate 128-bit round key block for each round plus one more

ii. Initial round key addititon:
    1. AddRoundKey – each byte of the state is combined with a byte of the round key using bitwise xor

iii. 9, 11, or 13 rounds
    1. SubBytes – a non-linesr substitution step where each byte is replaced with another according to the lookup table,
    2. ShiftRows – a transposition step where the last three rows of the state are shifted cyclically a certain number of steps.
    3. MixColumns – a linear mixing operation which operates on the column of the state, combining the four bytes in each column
    4. AddRoundKey

iv. Final round (making 10, 12, or 14 rounds in total)
    1. SubBytes
    2. ShiftRows
    3. AddRoundKey

2.2.6 SECURITY IN ADVANCED ENCRYPTION STANDARD (AES)

There are always cyber criminals on the prowl, looking for a chance to break and crack. One of the most common ways to protect sensitive data is encryption. (Inc, 2020)

To protect classified information up to the SECRET level, the design and strength of all key lengths of the AES algorithm are sufficient. Implementing AES in products for the protection of national security systems. (wikipediacontributors, 2021). AES has never been cracked yet and is secure against any attacks by brute force. Nevertheless, the larger the encryption key used, the more secure it is. It should be large enough so that modern computers cannot crack it. (Wood, 2011)

2.2.7 SIDE-CHANNEL ATTACKS IN ADVANCED ENCRYPTION STANDARD (AES)

Like a black box, side-channel attacks do not attack the cipher. On hardware or software systems that inadvertently leak data, hackers will attack the cipher implementations. In April 2005, D.J Bernstein announced a cache-timing attack that he used to break down a custom server using OpenSSL AES encryption. The server was designed to provide as much data as possible. (wikipediacontributors, 2021)

Dag Arne Osvik, Adi Shamir and Eran Tromer presented a paper in October 2005 showing several cache-timing attacks against AES implememtations found in the dm-crypt partition encryption function of OpenSSl and Linux. After only 800 operations triggering encryptions, one attack was able to gain an entire AES key. The attacker needs to be able to run programs on the same system or platform that performs AES for this type of attack. (wikipediacontributors, 2021)

Ashokkumar C, Ravi Prakash and Bernard Menezes presented a side-channel attack on AES implementations in March 2016 that can recover the completed 128-bit AESkey in only 6 to 7 plaintext/ciphertext blocks, which is a significant improvement over previous works requiring between 100 and one million encryptions. Many modern CPUs have integrated AES hardware instructions that protect against timing-related side-channel attacks. (wikipediacontributors, 2021)

2.3 RELATED WORKS

Below are the related works that relate to this project.

a) Field Programmable Gate Array(FPGA)

The implementation of the AES algorithm based on the FPGA has been proposed. The design uses an iterative block looping technique and a 128-bit S-box key size.(Isaac Kofi Nti, 2017) The architecture is low in complexity and easily achieves low latency and a high output of 1054 Mbit/sec for encryption and 615 Mbit/sec for decryption. Proposed implementation of the 128-bit AES standard on a Field Programmable Gate Array (FPGA) for a significant level of security similar to a faster time interval to secure ATM communication, optical disc content similar to ensuring the storage of confidential company documents or government documents. (Isaac Kofi Nti, 2017)

Tools and Methods

For the development of the interface, Microsoft Visual Studio 2010 (C#) was used, where the client used it to communicate via a web browser with the server. The database was developed using Server 2008 Microsoft Structured Command Language (MSSQL). A wireshark hacking tool used to test the encrypted data. (Isaac Kofi Nti, 2017)

Design Concept

Below shows the pictorial view of the proposed layout and the other process for the implementation of the AES algorithm with 256 bits key length for organizational data protection. (Isaac Kofi Nti, 2017)

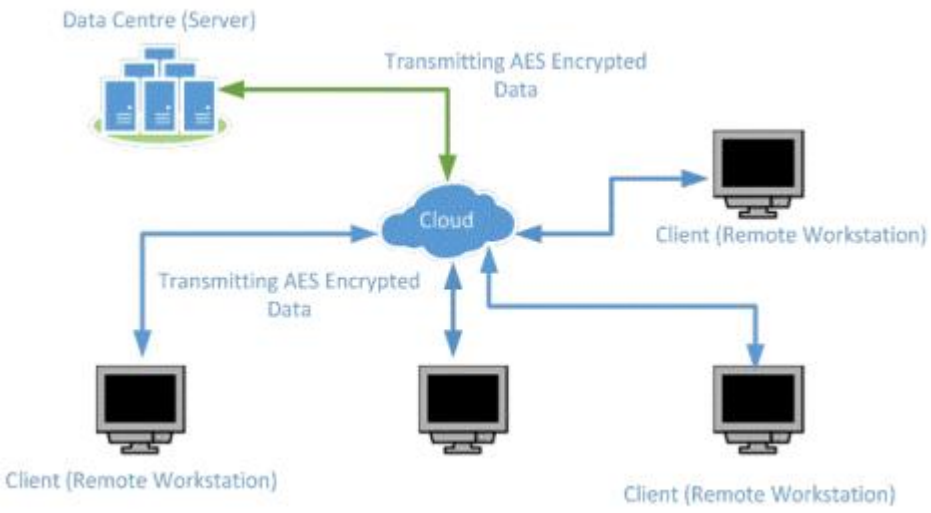


Figure 6 : Proposed Design

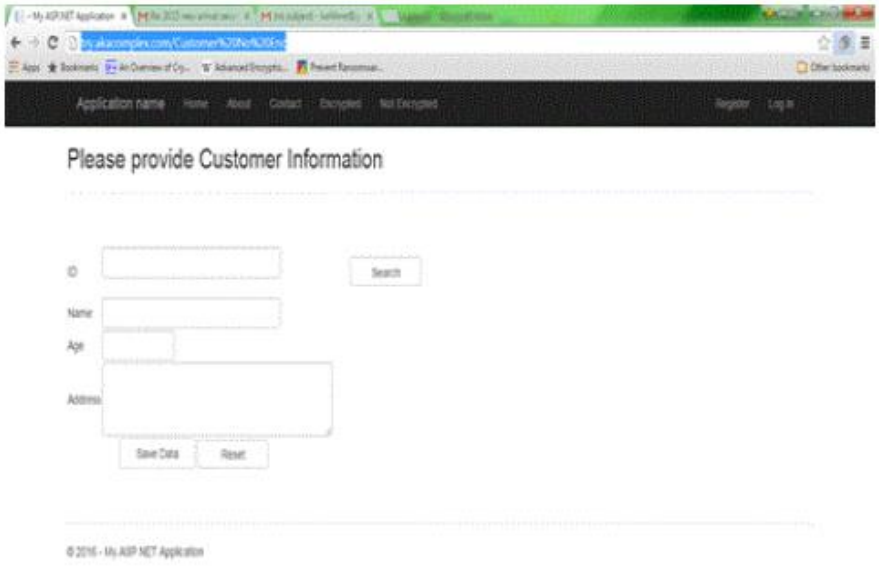


Figure 7 : Interface of the system

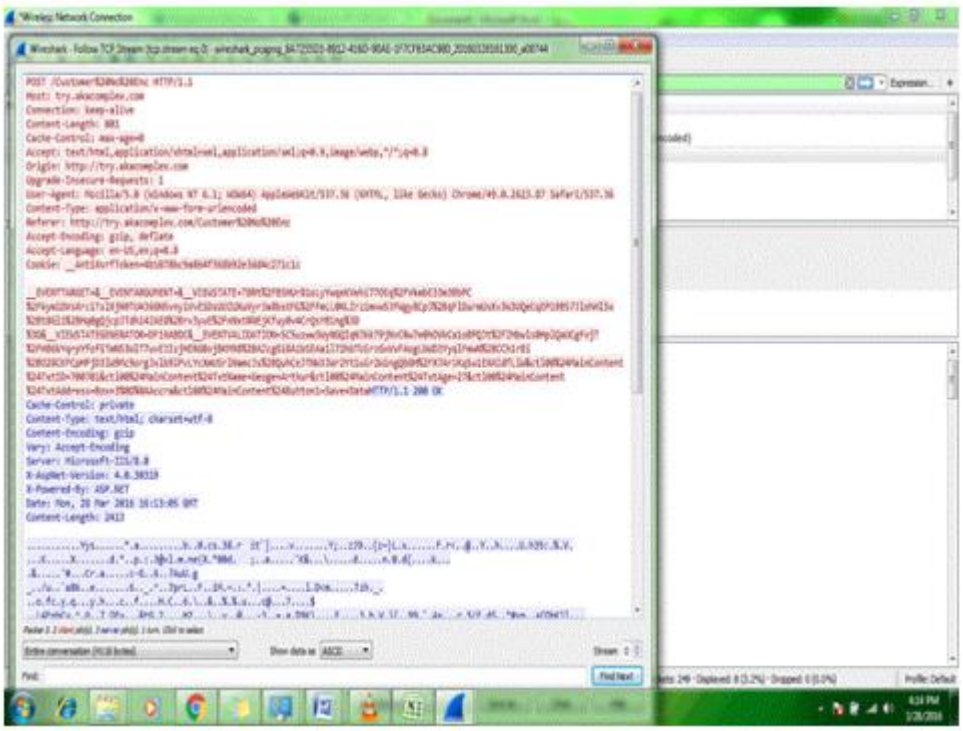


Figure 8 : Unencrypted Data

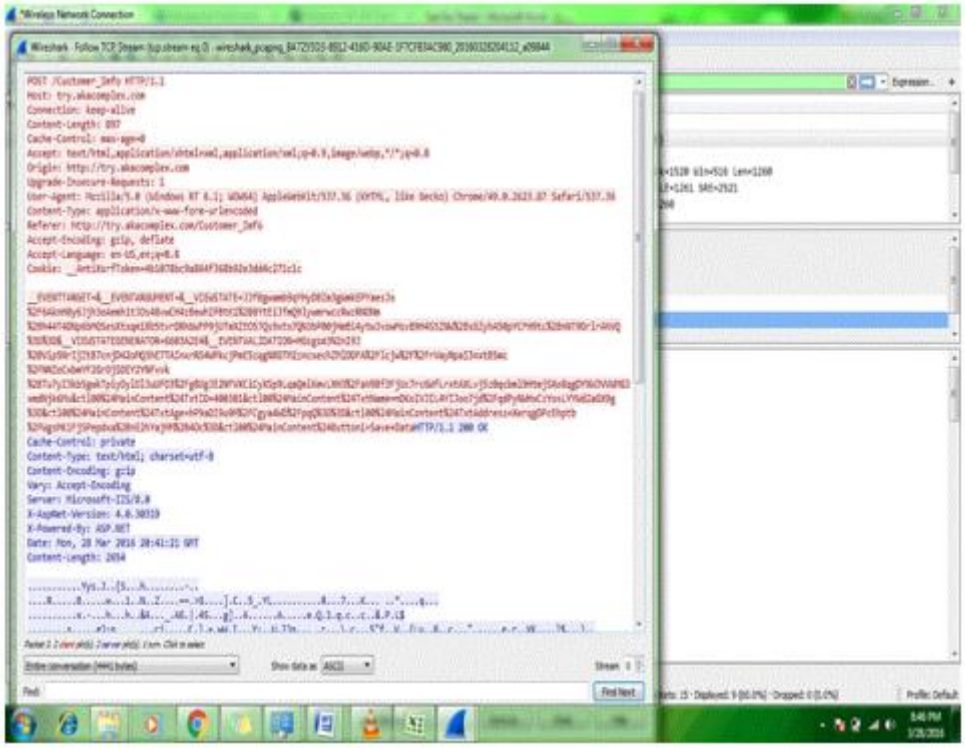


Figure 9 : Encrypted Data

Results

Five different data for testing purposes were collected from the front end. The wireshark hacking tool was used by the network packet analyzer to intercept the data packets between the transmission and the raw format of the packets, as shown in Figure 8, in plain text. Figure 9 shows an organization's saved data that has been transferred and encrypted. The server's input data, intercepted data and saved data are different. The AES256 Bits Block Cipher Algorithm scuttled the input data. The saved data in the server is therefore entirely protected by the application.(Isaac Kofi Nti, 2017)

b) AES-256 and SHA-256

Without user management being directly active, cloud computing uses Internet technology to provide data storage and computing power. The term is generally used to describe data centers that many users across the world and across many locations can access from central servers. This cloud computer provides quick access to flexible and low-cost IT resources. (M Husni, 2015)

Due to the rapid growth of digital technology, the threat is also increasing. The interconnectivity from any device can also increase the threat through the use of the Internet such as this cloud computing. There are so many kinds of threats, such as spoofing, pishing, network incidents, malware, etc., based on the Cloud Computing Survey in 2018. 73 percent of organizations have cloud-based computer infrastructure. An important issue that needs to be given more attention is how data is managed, stored and secured in this era of digital technology. The privacy and security of the database also needs to be ensured. (M Husni, 2015)

To solve the issue of the integrity of data stored in the server, hash functions SHA-256 and AES-256 were suggested. As a strategy to check the integrity of the data, the encryption mechanism will be combined with this scheme. There will be an encrypted server file. As Myo Zaw et al are implementing AES, Elliptic Curve Encryption and Signature to secure the database, and the results of this study show that because it generates many keys, it is difficult to attack the proposed method. In this suggested method, each element is represented as

a key. Despite the complicated method, this technique also has its disadvantages. This produces thousands or millions of keys that can make handling difficult. In order to propose an encryption/decryption system for IoT communication, Iqra Hussain et al uses Binary bit sequence and Multistage Encryption. This algorithm can be classified as a symmetric algorithm. At different stages, this method will encrypt the data and a key will be generated for the encryption process to convert plain text into cipher text. The same key will be used to decrypt the cipher text back into its original text. (M Husni, 2015)

Method

To verify the integrity of computer files, the process of file verification is used. The process of verification will compare the generated hash file with the original hash file. It is possible to make sure the file is not broken or has been modified by using the hash function. The function in it is used in many applications to encrypt the file and to ensure that it changes after modification. (M Husni, 2015)

The hash function is used in the process of transferring or saving files to prevent a file from being modified. Sometimes there is a malware or malicious code or virus that is used to change the content of the information. It will be prevented by hash functions from being modified. The Laravel framework was used in order to implement the hash function. Laravel is a PHP framework designed by Taylor Otwell. Laravel has a different method with the other structure and it uses the routing class to provide interaction in the system.(M Husni, 2015)

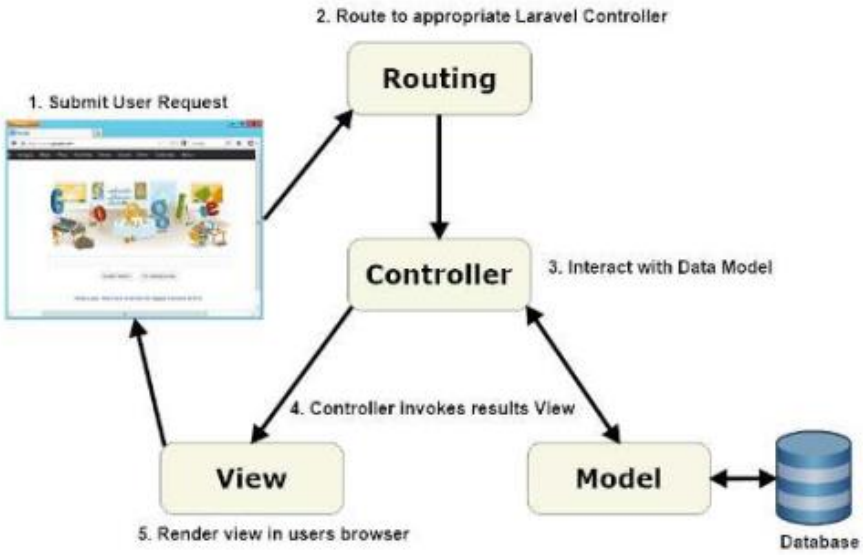


Figure 10: Architecture of Lavarel

In Lavarel and MySQL, the system is created as a database. Python was used to implement the script to verify the data integrity and return the data backup to the system. One of the languages for programming is Python. Python is an easy language for programming that can be read clearly. For differential attack, truncated differential attack, linear attack, interpolation attack and square attack, AES is selected because this algorithm is strong. (M Husni, 2015)

Front-end and back-end systems exist. Using Lavarel, the front end of the system is implemented, while the back end is implemented using the programming language of Python. The database server, application server and backup server are three servers of the system that have been developed. To stimulate the process of transfer and verification, these servers are used. The front-end system consists of a file system for the application server and the verifier. The application provides the ability to upload, download and verify a file. The verifier application is stored on the server of the database. (M Husni, 2015)

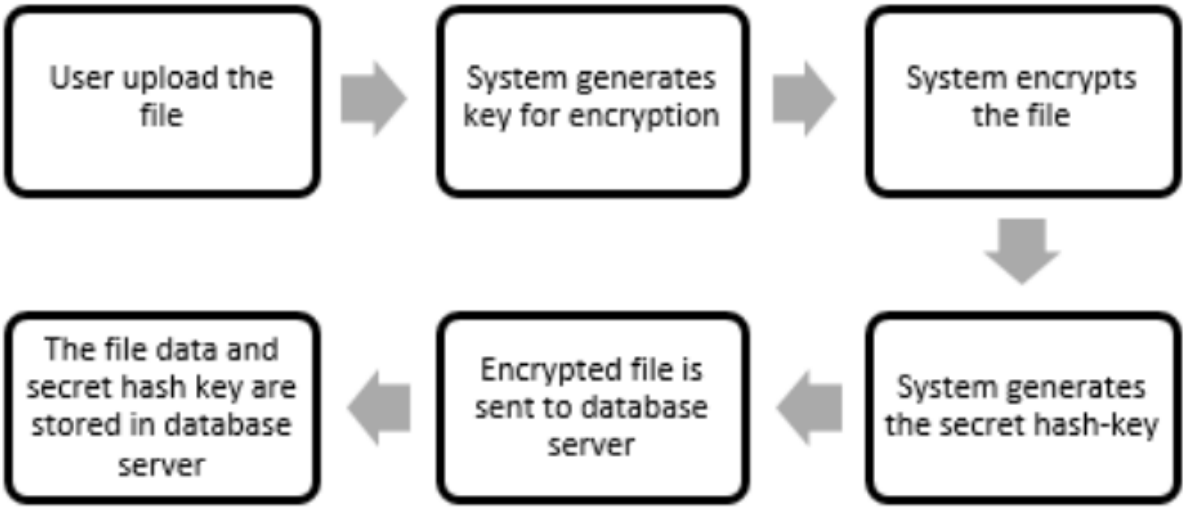


Figure 11: The upload process designed to ensure the file entegrity.

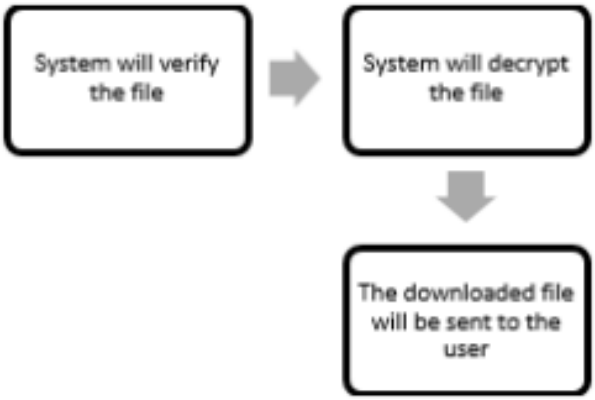


Figure 12: The download process designed to ensure the file integrity

Results and Discussion

Functionality tests have been conducted to test the reliability of the software. The functionality test was designed to check the system for any errors, bugs or defects. It checks the file upload, the file download, the file verifier, and runs a script to get the file back to the backup server. Each step has its own way of verifying that. There are four different file types to test the performance of the developed system, which will be uploaded and downloaded to check the encryption and decryption algorithm performance. The system will be tested by three users. Each user attempts to upload and download a file of various sizes and file types. The file will be decrypted in the download process and sent to the user. The file will be encrypted and stored on the database server during the uploading process. (M Husni, 2015)

Conclusion

From the reliability test conducted:

- AES algorithm implemented for encryption and decryption process. A web-based system developed using Lavarel framework.
- The system will verify the file integrity to ensure the file stored is not modified
- The system has functionality to return mofified or deleted data back into its own original file.
- From the functionality test, no error was found or fault in the system developed.

c) AES and DES

Introduction

The goal of each organization is to secure their sensitive information in databases containing informations about their customer and their business as well. Local protection achieved by installation of cryptographic modules in application server or by using the internal cryptographic module within the database. With this encryption mechanism is performed only on the server side. The main objective of this mechanism is to protect the data on the server. Data is stored in

encrypted from in the disk to avoid unauthorized access to the disk. Such cryptography mechanism used by the popular standard cryptographic algorithm (AES, 3DES …). (Saša Ž Adamović, 2009)

The two most common encryption algorithms, AES and DES, are used by MySQL in its cryptographic modules. The AES algorithm was chosen to encrypt and decrypt information using AES ENCRYPT() and AES DECRYPT(). MySQL can be 128 or 256 bits in length. This study used a 256-bit key to increase the system's security. The function AES ENCRYPT() returns the result of a binary string (ciphertext) while the function AES DECRYPT() returns the original string (plaintext).

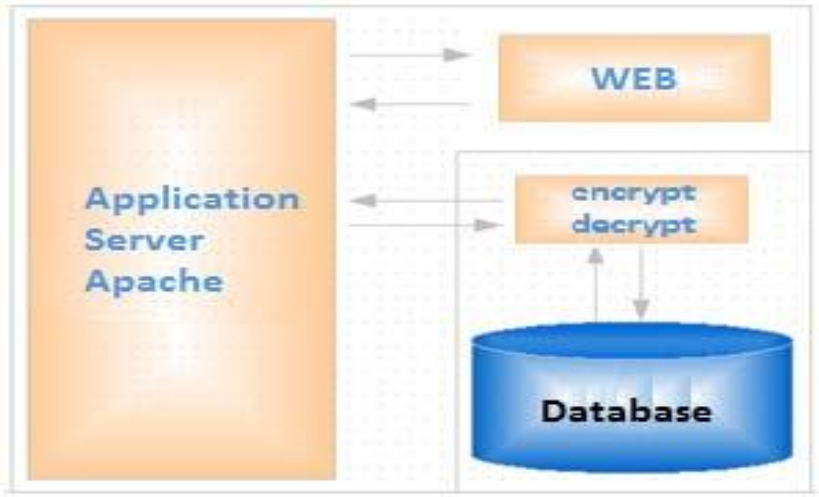


Figure 13 : Encryption within database

For the realization of AES-ENCRYPT() functions passing text encryption algorithm as arguments and 128 or 256-bit key length encrypted with whom, and for the realization of AES-DECRYPT() as arguments passing the cipher text and the key we used with encryption for the AES-ENCRYPT() functions. The benefits and disadvantages of applying this concept of protection are shown below:

Advantages:

- Implementation of AES algorithm in C programming language.
- Data stored in the database is in encrypted form

Disadvantages:

- Unavailability of source code
- The key is encrypted with the data.
- Key changes (a process that requires decoding and re-encrypt the complete the database).

Encryption at application server.

This is accomplished by installing the application server using local protection. In order to make it fully work, client/server architecture components must confirm their basic principles. In the components of the client, server and intermediaries of communication, these principles must be unique. The principles must comply with the criteria below: (Britannika)

- Hardware and software independence
- Open access to services.
- Distribution process.
- The PHP programming language is used for the development of cryptographic modules. PHP was used because of its advanced characteristics and also because it belongs to an open source language group. The algorithm is written on the basis of FIPS standards (Federal Information Processing Standards). 3 key lengths can be supported by AES (128, 192,256). (Saša Ž Adamović, 2009)

Given that a large number of users can categorize the client-server architecture used in the form of a web application simultaneously, performance and competitive approach to the two questions that need attention during implementation. Different servers have different kinds of strategies to improve their efficiency. (Saša Ž Adamović, 2009)

The number of possible client server architectures that can be used for data protection in databases has been shown in Figure 14. The architecture of the display consists of two servers. Server for databases and application servers. The application server will implement the PHP module with an encryption and decryption module. Direct communication exists between these two servers. Data to be exchanged in cipher text format.

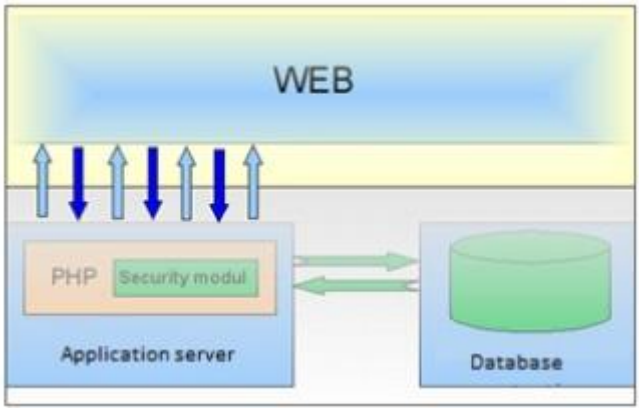


Figure 14 : Encryption at application layer

Advantages and disadvantages of this concept of protection:

Advantages	Disadvantages
Data communication are protected	Implementation AES algorithm interpreter language
The key is not in encrypted data	Key changes
The availability of the source code	

Table 2.1: Advantages and disadvantages of protection

Results

This paper examines data cryptographic protection directly over the base and on the server of the application. Showing an experimental comparative outcome. They both have access to their benefits and their drawbacks. With local protection intervention on the database, including encryption and decryption modules. The data in the database is written in an encrypted form and provided either by the possible theft of a hard disk or by unauthorized access

to the database. The results of this study show that the PC's performance is not sufficient to make full use of cryptographic mechanisms to encrypt the levels described. The obtained experimental results indicate the need for additional hardware for encryption instead of software solutions. The need for studying and developing methods of cryptography is all the greater since the applicable computers, computer networks and with them and databases as only the form of archiving data and control among people. (Saša Ž Adamović, 2009)

The summarization of related work are shown in Table 2.2 below.

Table 2.2 Related Works

EXISTING SOLUTION	METHOD	IMPLEMENTATION	STRENGTH	LIMITATION
Database Security with AES Encryption, Elliptic Curve Encryption and Signature	AES 256 and ECC encryption	RDBMS	• Row level encryption, column level encryption and elements level encryption • Security system more reliable. • More effective for access control system	• Database performance decrease. • Thousands or millions of keys to manage. • When an attacker obtain one key for the column, whole data of the column will be gone.

Encryption and Decryption of Mobile Security using AES and GOST algortihms	GOST encryption	Internet of Things (IoT)	• Low power consumption for encryption and decryption process • CPU power consumption fro AES and GOST is lowest.	• Encryption and decryption speed is lowest for DES
Secure Database Access Through Partial Encryption	Partial Encryption	DBMS	• Secure the sensitive information in database transaction	• Slow and computatinaly expensive
Database System Providing SQL Extensions for Automated Encryption and Decryption of Column Data	Chaotic map and genetic operation	Databases	• Can secure and retrieve a large amount of records from the database. • Encrypted records will be secured by a key-encrypting.	• More complex on intereface

Data Protection in Databases at the Local And Server Level	AES and DES	DBMS	• Data communication are protected • The availability of the source code	• Performance of the system decreasing. • Key changes (a process that requires decoding and re-encrypt the complete database)

The experimental results obtained show the need for additional hardware for encryption instead of software solutions. Since this project's computer network review focuses on securing the Human Resource Database using encryption and decryption for the applicable computers, the need to study and develop cryptography methods is all the greater. As the solution, the AES-256-bit encryption algorithm was chosen. This is because the AES algorithm is familiar to others and more secure compared with DES and 3DES. In addition, it is also the most commonly used algorithm compared to other types of algorithm. Besides that, the AES algorithm had the advantages of more secure encryption in securing databases. The encrypted and decrypted data was unbreakable using the AES algorithm until today. This provides a clearer perspective on what this project is about. The related work of this project is displayed in Table 2.2

CHAPTER 3
METHODOLOGY

This chapter provides an overview of the approach to project methodology, description of project methodology framework data collected, suggested design and experimental design will also be discussed in this chapter. Each phase involved in this project will be discussed in detail in the project methodology framework section: information gathering, information analysis, design, implementation, testing, evaluation and validation, and documentation. The last section is the experimental design to show how the experiment will be carried out in order to achieve the correct results.

3.1 Project Methodology Framework

A project methodology framework is a very important part to explain where we are coming from and why we want to do the research in a particular way. There are seven phases in conducting this research as outlined in Figure 3.1.

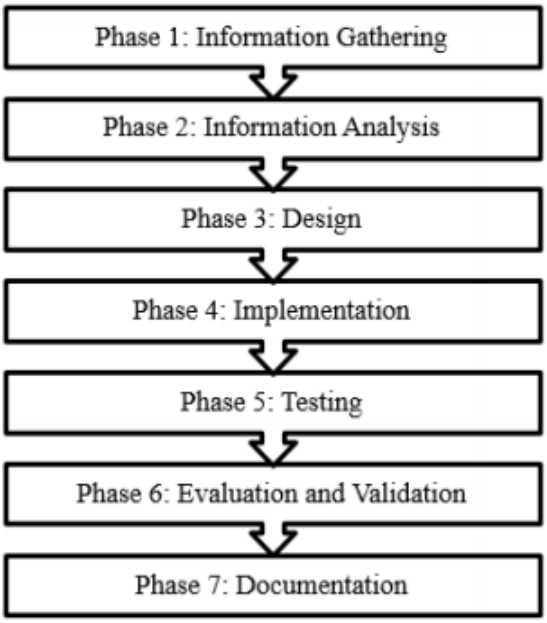


Figure 15: Research Methodology Framework

The first phase is Information Gathering, a phase in which literature review related to the definition of database security, database security using various methods, common AES attacks,

encryption definition, encryption types, how AES works, and how to implement AES in database security is used to find out. The second phase is Information Analysis, in which the appropriate types of encryption are found to secure the database. The third stage is design, which is a stage in which the database is designed to defend the database from unauthorized users along with the implementation of the AES algorithm into the database. Implementation is the fourth stage, where the proposed algorithms are implemented by executing the proposed algorithms to detect and defend the database from unauthorized users. Testing, a critical stage for testing the system before making it available to users, is the fifth phase. It should guarantee that the algorithm works well, that the functions work properly, and that the performance runs smoothly. Evaluation and validation is the sixth stage, where the experimental outcome is presented with a final discussion of the outcome. Documentation is the seventh stage, where the final outcome is documented together with the details.

The details tasks and activities for every phase of research methodology as shown in Table 3.1.

Table 3.1: *Research Methodology Framework*

Phases	**Activities**	**Outcomes**
Information Gathering	• Identifies the definition of database security system and its importance of securing it. • explain the definition of encryption and decryption. • Identifies the diffrences between symmetric and assymetric. • Study the types of AES encryption method.	• Understanding the definition of securing database. • Observe and understanding how several types of encryption and decryption works.

Phases	Activities	Outcomes

Information Analysis	• Investigate several current database encryptions and how the algorithm works.
	• Determine and select the suitable encryption and decryption algorithm based on the selected criteria.
	  ➢ Security
	  ➢ Efficiency in software
	  ➢ Flexibility and Simplicity
		• Understanding the current way in securing databases using AES encryption.

Design	• Design a database system to implement the AES algorithm into it.	• Friendly user interface database system. • Human Resource Database System
Implementation	• Implement the AES algorithm into the database system. • Execute the proposed algortihms in the database.	• Implement the proposed AES algorithms which is AES-128 fro encryption and decryption process.
Testing	• Test the proposed algorithms. • Execute the proposed algorithms to check the process of encryption and decryption.	• Test and measure the proposed algorithms in terms efficiency, effectiveness and security
Evaluation and Validation	• The results will be compared between the database without any encryption method and the proposed algorithms	• Present the proposed algorithm results in a chart to show that the proposed algorithm is much better than without any encryption method.
Documentation	• Document the problem statement, research objectives, literature review, research methodology, implementation, testing and results.	• A complete report will be documented with its full details.

3.1.1 Information Gathering

The task of Information Gathering phase is to study the definition of security in database system, definition of AES. This phase also study on how the AES algorithm works.

3.1.2 Information Analysis

The task of Information Analysis phase is to investigate, determine and select the best encryption method and prevention algorithms based on the following criteria:

- Security
- Efficiency in software
- Flexibility and Simplicity

3.1.3 Design

The task of the design phase is to develop a database system for human resources that can be protected from intruders using AES-128 encryption and decryption methods.

3.1.4 Implementation

The task of the implementation phase is to execute the proposed encryption algorithms to identify and protect the database system against unauthorized users. There are several steps in how to perform the implementation tasks as follows:

i. Derive the round key set from the key of the cipher.
ii. Initialize the state array with data from the block (plaintext).
iii. To the starting state array, add the initial round key.
iv. Perform nine state manipulation rounds.
v. Perform the tenth and last round of manipulation of the state.
vi. Copy out the final state array as the encrypted information (ciphertext).

3.1.5 Testing

In terms of intelligent detection, detection effectiveness and defense compatibility, the task of the testing phase is to test and measure the proposed algorithms. Java and MySQL will be used for testing. Data is presented as encrypted information.

3.1.6 Evaluation and Validation

The task of Evaluation and Validation phase is to compare results between without any encryption method algorithm and proposed algorithm to determine the proposed algorithm better than current algorithm.

3.1.7 Documentation

The task of Documentation phase is to to document the whole research activity in a particular thesis format.

3.2 Proposed Design

This research will focus on designing database system and defense algorithms to secure the database from any attacks.

3.2.1 Flowchart

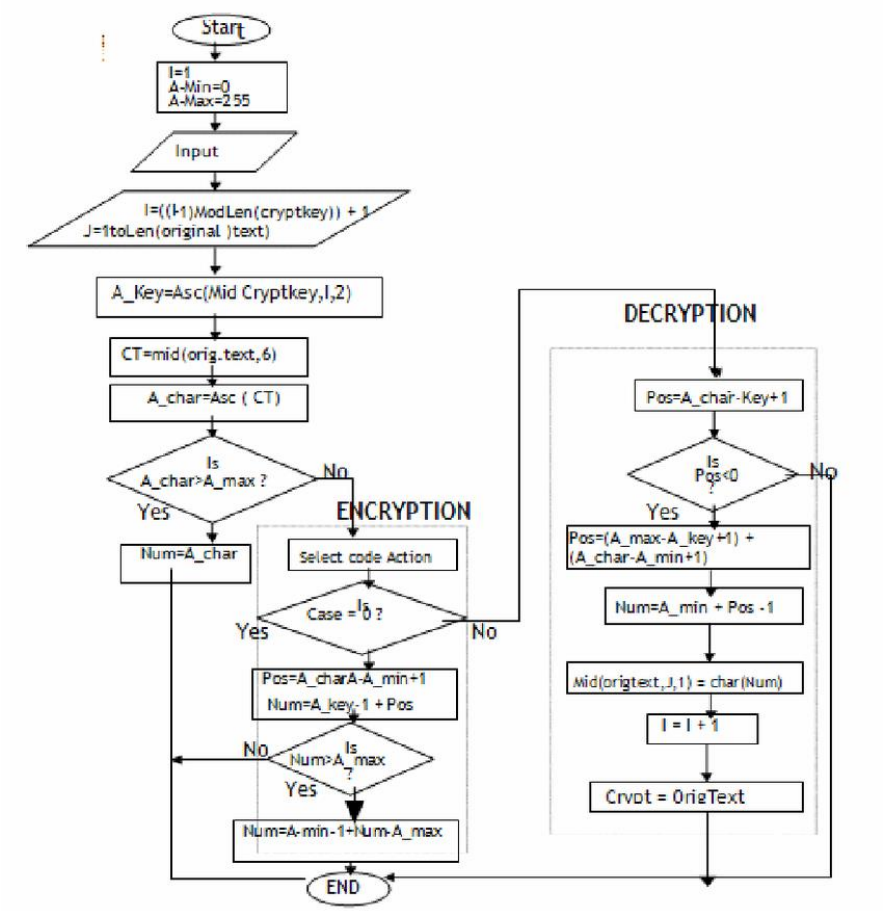


Figure 16: Flowchart

3.2.2 Interface Design

Figure 17: Admin welcome page

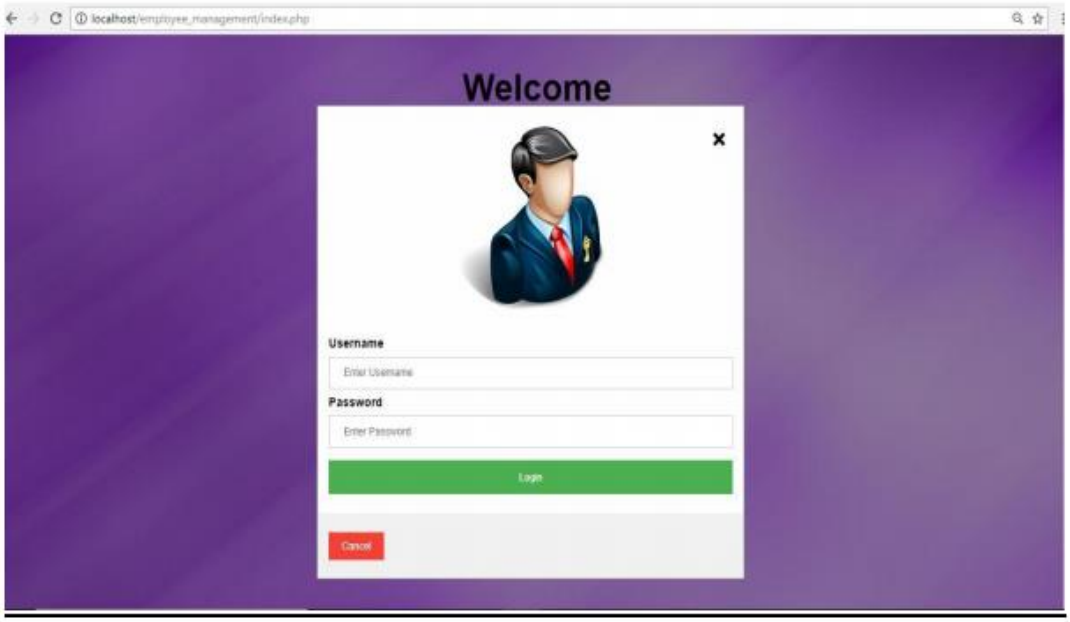


Figure 18: Admin Login Page

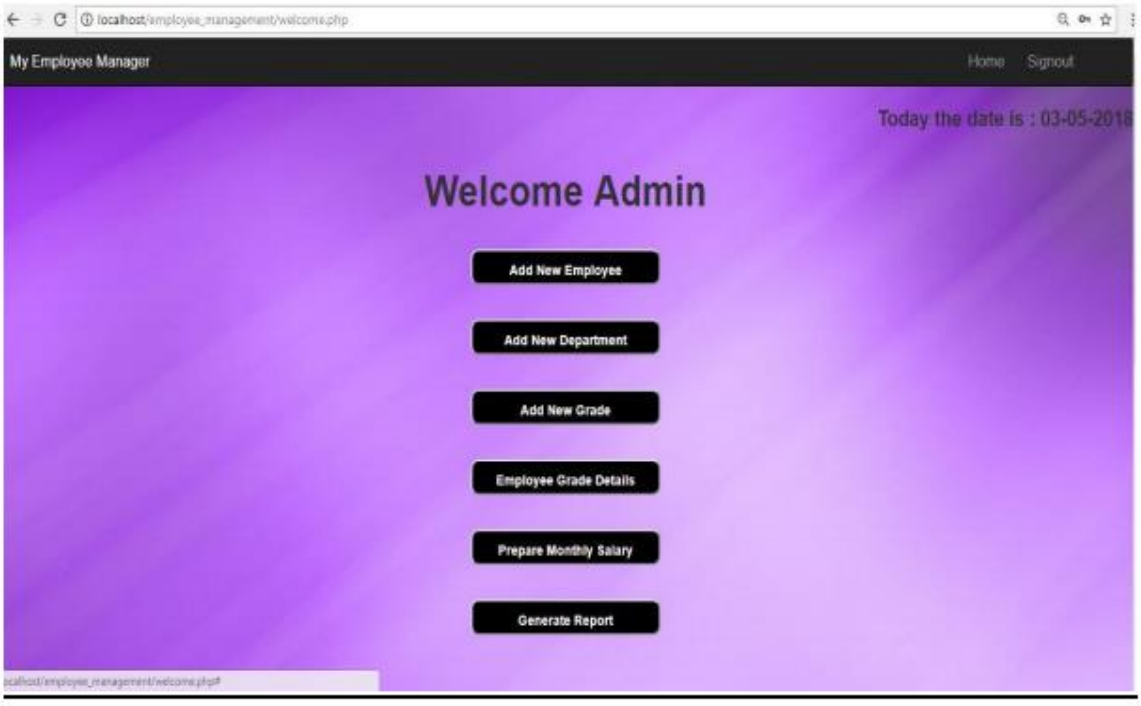


Figure 19: Admin Page

Figure 20: Employee Salary Details

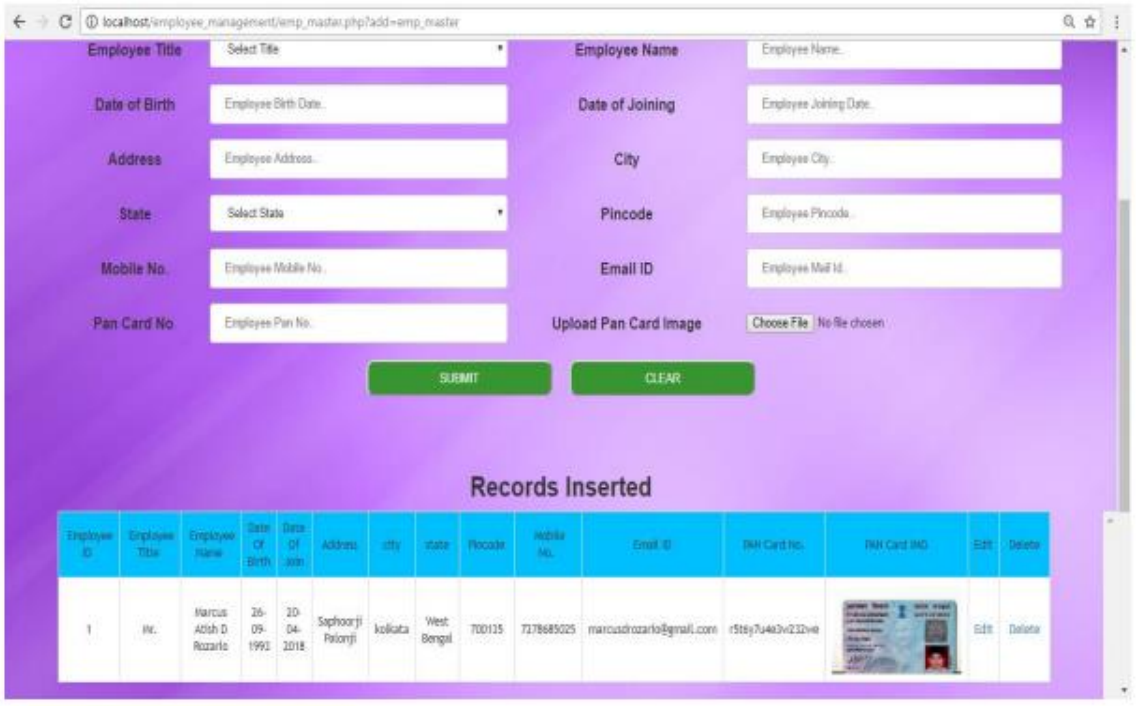


Figure 21: Employee Data Inserted

Figure 22: Encrypted Data

3.3 Experimental Design

This section is produced to present how the encryption and decryption process occur will be conducted practically as shown in Figure 23.

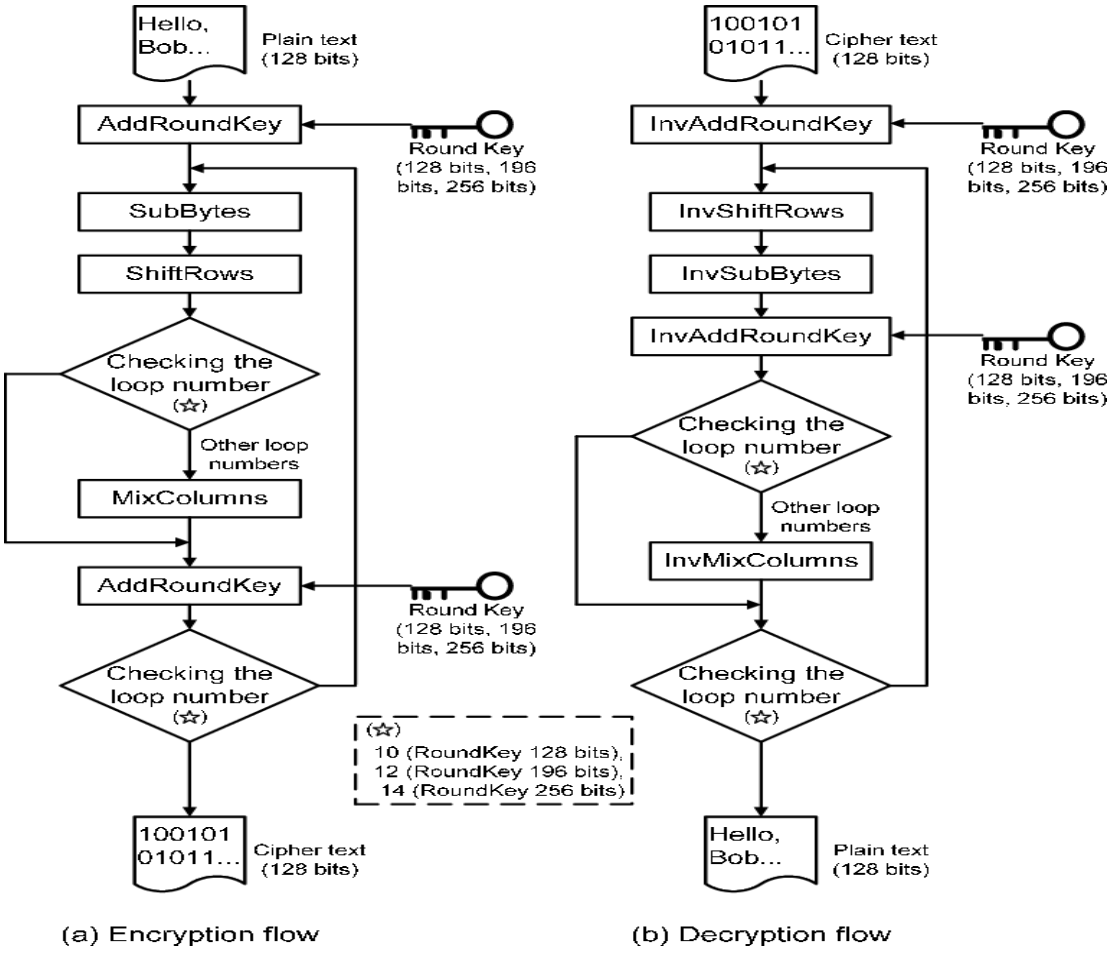


Figure 23: Encryption and Decryption Flow Process

.

4.0 Hardware and Software Requirements

4.1 Software

	Specification	Function
PHP MySQL	• 32-bit or 64-bit. • Requires Visual C runtime(CRT).	• Performs system functions. • Add, delete,modify, elements within database through PHP.
Java	• 64-bit Microsoft Windows • 8GB memory • Java Development Kit(JDK) ver 1.7	• Text-based programming language used both client-side and server-side. • Adding interactive behavior to web pages

Table 4.0 Hardware and Software Requirements

5.0 Project Schedule

Research Activities	2020						2021							
	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
Information Gathering														
Information Analysis														
Design														
Implementation														
Testing														
Evaluation and Validation														
Documentation														

References

(1 may, 2019). Retrieved from https://mind-core.com/blogs/cybersecurity/types-of-cyber-security-threats-and-how-they-will-impact-your-business/

Britannika. (n.d.). Client-server architecture.

Craven, C. (13 may, 2020). Retrieved from https://www.sdxcentral.com/security/definitions/what-is-advanced-encryption-standard-aes-definition/

Developer, W. (31 5, 2018). Retrieved from https://docs.microsoft.com/en-us/windows/win32/seccrypto/data-encryption-and-decryption

Dhandhania, K. (2014). Retrieved from https://www.commonlounge.com/discussion/e32fdd267aaa4240a4464723bc74d0a5

Education, I. C. (27 august , 2019). Retrieved from https://www.ibm.com/cloud/learn/database-security#:~:text=Database%20security%20refers%20to%20the,compromised%20in%20most%20data%20breaches.

Fox, P. (n.d.). Retrieved from khanacademy.org/computing/computers-and-internet/xcae6f4a7ff015e7d:online-data-security/xcae6f4a7ff015e7d:data-encryption-techniques/a/public-key-encryption

Inc, A. E. (2020). Retrieved from https://www.atpinc.com/blog/what-is-aes-256-encryption

Isaac Kofi Nti, E. G. (16 march, 2017). Implementation of Advanced Encryption Standard Algorithm with Key Length of 256 Bits for Preventing Data Loss in an Organization.

Kapersky. (2021). Retrieved from Database security is a fundamental security input. It is referring to the measures that are being used to protect the sensitive data, unauthorized access and potential attacks administered by the cybercriminals

Looker. (n.d.). Retrieved from https://looker.com/definitions/database-security

M Husni, H. T. (february, 2015). Security audit in cloud-based server by using encrypted data AES - 256 and SHA-256.

Maurer, R. (30 july , 2015). Retrieved from https://www.shrm.org/resourcesandtools/hr-topics/risk-management/pages/top-database-security-threats.aspx

Morris J. Dworkin, E. B. (26 november, 2001). Retrieved from https://www.nist.gov/publications/advanced-encryption-standard-aes

Pressbooks. (n.d.). Retrieved from https://bus206.pressbooks.com/chapter/chapter-6-information-systems-security/

Saša Ž Adamović, M. Š. (21 november, 2009). DATA PROTECTION IN DATABASES AT THE LOCAL AND SERVER LEVEL.

TechTarget. (april, 2020). Retrieved from https://searchsecurity.techtarget.com/definition/encryption

Thakkar, J. (25 april, 2020). Retrieved from https://sectigostore.com/blog/types-of-encryption-what-to-know-about-symmetric-vs-asymmetric-encryption/

UKEssays. (november , 2018). Retrieved from https://www.ukessays.com/essays/computer-science/database-security-threats-and-countermeasures-computer-science-essay.php

wikipediacontributors. (7 january, 2021). *Advanced Encryption Standard*. Retrieved from https://en.wikipedia.org/w/index.php?title=Advanced_Encryption_Standard&oldid=998858677

Wood, L. (21 march, 2011). Retrieved from https://www.computerworld.com/article/2550008/the-clock-is-ticking-for-encryption.html