**A SECURE WEB-BASED ARV PATIENT SERVICE CARE SYSTEM.**

**A case study for people living with HIV/AIDS in Kenya.**

**School of Computing and Information Technology.**

**Joseph Ochieng Awinda.**

**SCT221-0350/2017.**

**A project proposal submitted to the Department of Information Technology in the School of Computing and Information Technology in partial fulfilment of the requirements for the award of Bachelor of Science in Information Technology at Jomo Kenyatta University of Agriculture and Technology.**

**2021.**

# Declaration

This Proposal/Research Project is my original work and has not been presented for a degree in any other University.

Signature……………………………… Date………………………………

Joseph Ochieng Awinda.

This Proposal/Research Project has been submitted for examination with my approval as University Supervisor.

Signature……………………………. Date………………………………

Dr. Dennis Njagi.

# Acknowledgement.

I would like to thank almighty God for his protection upon my life and of my loved ones. I thank him for giving me the free gift of life up to this point. My honest regards go to my school especially the IT department faculty consisting of my able lecturers who have always been persistent in taking me through my course work, the workers who have always make sure that I study in a clean environment, and my supervisor Dr. Dennis Njagi for his patience and guidance throughout my project.

My sincere gratitude goes to my family, for always being there for me, helping me with advice and supporting me financially. Without them I could not have make it this far. To my special friends who were always there for me whenever I got stack thank you so much for making this possible. May the good Lord bless you all.

# Abstract.

Currently the HIV positive people need to go to hospital (public)where they can be able to seek healthcare services and be provided with ARV tablets. At some point the patients miss the drugs and this alters their drag uptake flow. In several occasions, the patients also get to spend more hours queuing at the hospital which makes it impossible for them to do other tasks i.e., reporting at their place of work. This has also led in many people sidelining visiting clinics due to stigmatization which they face when visiting such places (HIV/AIDS wing) of the hospital. There has been also laxity among the health officials in maintaining the patients record about the type of drug they are taking as patients take different types of ARV drugs basing on the viral load of the infection in their body system. Some also fails to know prior the availability of the drags when they arrive or when they are out of stock. This has therefore led to many inconveniences in the patients’ health. The web-based ARV patient service care system seeks to solve this by coming up with a system that will be secure in all levels so as to provide a much secure and confidential access of information, where the data/details of the patients will be protected and the patient will be able to get information about the availability of the drugs in real time manner. The patient will also be able to request change of clinic according to where they preferred most and they can also request for the drugs in a clinic nearby that has more facilities. This will be able to reduce the time wasted on queuing, and reduce stigmatization, and protect confidentiality of people living with HIV/AIDS. It will also help the hospital sector in minimizing the use of paper work which are prone to misplaced. The prototype methodology will allow the system to be developed into stages and finally be integrated into a whole system. Therefore, this system sought to improve the service care of HIV patients by providing a much secure and confidential access of information, where the data/details of the patients will be secured enough and they will be able to get information about the availability of the drugs in real time manner.

# Table Of Contents.

Table of Contents

[Declaration i](#_Toc78135632)

[Acknowledgement. ii](#_Toc78135633)

[Abstract. iii](#_Toc78135634)

[Table Of Contents. iv](#_Toc78135635)

[Acronyms v](#_Toc78135636)

[Chapter 1: Introduction 1](#_Toc78135637)

[1.1 Background. 1](#_Toc78135638)

[1.2 Research Area. 2](#_Toc78135639)

[1.3 Problem Identification. 3](#_Toc78135640)

[1.4 Proposed solution. 3](#_Toc78135641)

[1.5 Objectives. 3](#_Toc78135642)

[**1.5.1** **General objective.** 3](#_Toc78135643)

[**1.5.2** **Specific objectives.** 3](#_Toc78135644)

[1.6 Research questions. 4](#_Toc78135645)

[1.7 Justification. 4](#_Toc78135646)

[1.8 Proposed research and system methodology. 4](#_Toc78135647)

[1.9 Data collection. 5](#_Toc78135648)

[**1.9.1** **Questionnaire.** 5](#_Toc78135649)

[**1.9.2** **Secondary data analysis.** 5](#_Toc78135650)

[1.10 Scope and Limitation 6](#_Toc78135651)

[**1.10.1** **Scope.** 6](#_Toc78135652)

[**1.10.2** **Limitations.** 6](#_Toc78135653)

[Chapter 2: LITERATURE REVIEW. 6](#_Toc78135654)

[2.1 Introduction 6](#_Toc78135655)

[**2.2.2** **Mitigation of Web-Security Vulnerabilities.** 8](#_Toc78135656)

[Resource Requirements. 13](#_Toc78135657)

[Hardware 14](#_Toc78135658)

[Software 14](#_Toc78135659)

[Appendix 14](#_Toc78135660)

[Appendix 1: Project Schedule 15](#_Toc78135661)

[Appendix 2: Gantt Chart 16](#_Toc78135662)

[Appendix 3: Budget 16](#_Toc78135663)

# Acronyms

HIV – Human Immunodeficiency Virus.

AIDS – Acquired Immunodeficiency Disease Syndrome.

AMPATH – Academic Model Providing Access to Healthcare

WHO – World Health Organization.

KEMSA – Kenya Medical Supplies Agency.

ARV – Antiretroviral

# Chapter 1: Introduction

## **Background.**

In a hospital like Mama Lucy hospital, the medical officers use an excel sheet in keeping records of their patients, whereby they first record it in an A4 books, then therefore update the record in an excel form. The drugs are then administered to patients basing on the information recorded.

Only the registered patients are allowed to pic the ARV drugs. And in cases of a new patient. A certain protocol needs to be followed i.e., the patient is required to go through counselling and to give information on whether he/she has been taking the drugs and if yes, he/she will be requested to give doctors remarks inorder to be included in the list. But for a new patient who has tested positive, he/she will undergo a series of counselling in the tents before beginning his/her drug uptake once he’s being registered. Following recent years, the patients, filed some complains to the hospital because there was a rise of stigmatization from the public, and the hospital decided to reallocate the HIV/AIDS boot camps into the backyard of the hospital in order to reduce the publicity and maintain patient’s confidentiality.

This has only reduced the grievances by a fraction but the issue of them overcrowding and spending longer hours in ques has led many to quit the process and the fact that they still have to go to the HIV outpatient department to pick their drugs seems to have not solve the privacy and stigmatization among the affected patients. The secure web-based ARV Patient service care system, seeks to solve these problems by creating a system which will enable the patients to know whether the drugs are available and when they can pick them at the general hospital chemist without the need of visiting the HIV/AIDS wing/department. the patients will also be able to know prior when the drugs are not available therefore, they can seek another alternative basing on the current dosage they’ll be having.

The system will facilitate a good rapport between the patient and the medical officers. unlike the current system where the officer cannot reach all the patients at once in cases of drug shortage. This system will allow them to deliver real time notification about the availability of ARV’s once the patient sigh in his/her secure web-based ARV patient service care system.

## **Research Area.**

The main focus in this case study is about data encryption. According to Eric H. Goldman and CISA, in their book Security+ they describe security as part of a defense-in-depth strategy, where many organizations are expanding their usage of encryption. While encryption can provide protection from unauthorized access and reduce the likelihood of data theft, it is very difficult to implement systems and processes can provide reasonable assurance of confidentiality in real world implementation. In recent years, many software products have begun offering build-in encryption capabilities that are more user friendly and manageable. When it comes to purpose build encrypted communication tools or standard based system to system encryption, the level of maturity is usually quiet high. But many organizations are not prepared for the risks and pitfalls of end user managed (encryption).

Security is part and parcel of our daily lives, people value security more, that is why heavy investments are channeled in security, it is estimated and predicted by (FORBES, 2020) that in the year 2020 cloud security will increase by 33% becoming a $585Million market in the year. Security services is forecast to drive $64.2Billion worldwide in revenue this year comprising of 51.9% of the total market and data security will grow by 7.2% becoming $2.8Billion. That is a lot of money being in this area of security as described by Forbes magazine. Thus, showing the importance of security and how much the world values secure systems.

In theory, encryption is just a matter of applying some math on bits of data before and after a file or message. However, there is a vast ecosystem of encryption technologies, algorithms, configurations, tools and file formats. Complicating matters, end user encryption tools are notoriously unfriendly from the end user perspective. Management and transfer of encryption keys and/or passwords and ensuring secure storage and down ting requirement to place on end users.

Encryption is typically thought of a securing communication between two or more individuals, and only those people involve with the transfer. However, in a business scenario, it is more likely that two organization, rather than individual users, should be considered the owners. Many messages encryption protocols and stand-alone file encryption tools are fundamentally design for personal use scenarios. However, in a corporate environment it is often necessary to have some form of keys. Escrow or ability to view the unencrypted version of data by others outside of the transaction, such as legal of security team (or at least the automated tool).

The system will be a web security on data encryption which is defined as protecting a website or web application by detecting, preventing and responding to cyber threats (GOODFIRMS, 2020) and how we can incorporate it to our system which is “A Secure Web-based ARV Patients Service care system” which is the act of login into the system confirm availability of drug, make an order, request of change of clinic, and getting real time notification about availability of the ARV drags, at the comfort of where you choose to be using your electronic device.

## **Problem Identification.**

In the current state, the government through KEMSA offers the supply of the ARV drugs to public hospitals, whereby the patients go basing on the appointment dates, some are long term takers whereby theirs drugs runs for as long as 6 months, while others are required to pay frequent visits to the clinics on monthly basis. There had been problems where there is a shortage of the drugs and the patients are not being informed prior the shortage. The patients also cover more distance walking to the hospital and spends longer time queuing waiting for the drugs. This has led many people to shy off from taking the drugs due to the fact of spending much time queuing at the hospital which breech their confidence and as well end up them being stigmatize by the community, due to lack of privacy. The unnoticed availability of the drug by the patient in the times of need can lead to much serious conditions in their health. The frequent failure of the health attendant to keep proper records has led to many patients taking the wrong dosage of the drug.

## **Proposed solution.**

The research sought to develop a system that will be secured in all levels so as to provide a much secure and confidential access of information, where the data/details of the patients will be safe enough and they will be able to get information about the availability of the drugs in real time manner. The patients will also be able to request change of clinic according to where they preferred most and they can also request for the drugs in a clinic nearby that has more facilities. This will be able to reduce the time wasted on queuing, and reduce stigmatization, and protect confidentiality of people living with HIV/AIDS. The system also ought to reduce the use of paper work in maintaining the patients record.

## **Objectives.**

### **General objective.**

The general objective of this study will be to design and implement a secure web application for Automated ARV patients service care system.

### **Specific objectives.**

1. To understand about security systems and their functionality in building of a secure system.
2. To investigate vulnerabilities in web-based security and how to prevent and curb them.
3. To analyze about system that have similar functionality.
4. Design a system that will enable HIV positive patients to get registered and their details being added into the system.
5. To develop a functional Secure Web-based ARV Patient Service Care System.

## **1.6 Research questions.**

1. How will a two-factor identification register patients into the system?
2. How to prevent and curb vulnerabilities in web-based applications?
3. How will the proposed system facilitate secure and efficient service delivery to patients?

## **Justification.**

The study sought to improve the service care of HIV patients by providing a much secure and confidential access of information, where the data/details of the patients will be secured enough and they will be able to get information about the availability of the drugs in real time manner. The study also sought to improve how the patients can request a change of clinic and how they can be able to feel comfortable by making their services less publicly and normal in order to avoid the social stigmatization which they undergo. The system will also facilitate accountability in allocation of the drugs because of the availability of accurate data about the people who will be receiving the drugs. It will avoid the incidence of brokers and corruptions on the dispatch of the ARV drugs because all the data about the HIV patients will be secured in a safe database for government through its ministry of health to refer.

The system will reduce time taken for patients in queuing at the hospital for the drug, improve accountability by putting various security levels and generating reports for administrators to see how many patients are registered. All this will benefit the patients and the health sector by saving their time and resources.

## **Proposed research and system methodology.**

System methodology as how the research of the project and development will undertake is quite important as it is critical to its success. The system development for the research project is rapid prototyping.

Prototyping model is a software development model in which prototype is built, tested, and reworked until an acceptable prototype is achieved. It also creates base to produce the final system or software. It is an iterative, trial and error method which takes place between developer and client.

In general, there are four basic types of prototyping models which are: rapid Throwaway prototypes, Evolutionary prototypes, Incremental prototype and Extreme prototype. The security tests that will be incorporated will have an aim of uncovering vulnerabilities so as to patch them and ensure protection of data and maintenance of functionality. This will also ensure the users that are the health officials and patient’s candidates will be involved during the development process of the system to ensure it gives desired results which is free and fair service delivery.

## **Data collection.**

In order to come up with an effective solution, requirements need to be collected from the various stakeholders involved. The techniques used are going to help get a clear picture of what is required in regards with coming up with the solution. Data techniques used:

### **Questionnaire.**

The patients would be issued with a sample of questionnaires’ where they would be required to fill and answer a YES/NO questions and be able to give their thoughts and feedback where possible. This will help in knowing the exact issues which affects them at the ground level and aid in finding the best solution for the problem basing on the answers given.

**A sample of questionnaire include:**

1. How frequently do you visit the clinic in a month?

[very frequently] [seldomly] [only when urgent matter]

1. Do you always receive your ARV drugs in time according to the appointment date?

[YES] [NO].

1. How can you rate the clinic service delivery?

[Good] [Satisfactory] [bad].

### **Secondary data analysis.**

This entails evaluation of data in the form of reports, journals, articles, and books that have been written by scholars pertaining web application encryption and how it can be integrated into our web applications in this case a secure web-based ARV patient service care system.

## **Scope and Limitation**

### **Scope.**

The scope of this study will be in the bounds of Kenya communities and the target audience will be the people living with HIV/AIDS. And how the research will aim to improve the patients ARV drugs uptake and care services and develop a secure, free and fair service care system.

### **Limitations.**

The user interface language of the system will be written in English language therefore limiting the number of people who will be able to understand. Only the English literate individuals will be able to access the system.

# Chapter 2: LITERATURE REVIEW.

## **Introduction**

With the rapid development of Internet and the extensive application of computer technology, the security of information becomes more and more serious, and the information security technology with data encryption technology as the core has also been developed greatly.

Data encryption technology not only can encrypt and decrypt data, but also can realize digital signature, authentication and authentication and other functions, thus ensuring the confidentiality, integrity and confirmation of data transmission over the network. In order to improve the security of data in network communication.

In this chapter the study will seek to explore research material that has already been done on the subject of data encryption. It will seek to elaborate how other scholars have achieved data encryption in their systems.

* 1. **Theoretical/Conceptual framework** 
     1. **web application security (encryption)**

The rapid development of computer network communication technology, to people's work and life provides a great convenience, shortening the distance between people, playing down the boundaries between countries. But also, with the resulting more and more serious information security issues, a large number of sensitive data directly through the public channel for transmission and exchange, to the illegal third party to provide a steal, view, tampering or even attack the possibility of information security has become current and future for a long period of time to be solved a major problem. The economic loss caused by the fragility of the information system security is increasing year by year, and the security problem is becoming more and more serious.

Web application security is defined as the process of protecting websites and online services against different security threats that exploit vulnerabilities in an application code. The targets of attacks are the database administration tools and the management systems (IMPERVA, 2020).

Web applications are considered high priority by hackers due to their inherent complexity of their source code, which increased the likely hood of unattended vulnerabilities and malicious code manipulation, high value rewards including sensitive private data from successful source code manipulation says (IMPERVA, 2020). This consideration by hackers is due to the fact that a lot of businesses have moved their operations online which in our case is cloud storage, thus they necessarily don’t have to break in on premise business but they can get the vital information remotely on the cloud. Which in our case for Automated ARV Patients Service Care system, the sensitive data which will be the patient’s information and the drug records is considered as an information of high value to anyone who can change records to their favor.

Like all software’s web applications contain some inevitable defects (SYNOPSYS, 2020). According to Veracode’s 2019 State of Software Security Report, 83% of the 85,000 applications it tested had at least one security flaw. Their research also found a total of 10 million flaws, and 20% of all applications had at least one high severity flaw with severity being defined in terms of the potential impact to confidentiality, integrity, and availability of the application as defined in the Common Vulnerability Scoring System. This comes from the fact that many companies and organizations are trying to rapidly come up with cutting edge business solutions, in that they are constantly trying to be pioneers in their various fields and unfortunately quite a number of them have a very minimalistic approach towards security threats (Eiw, 2016). The various web application security as described by (OWASP, 2017) are like; Injections such as SQL, NoSQL, OS, and LDAP, which occur when untrusted data is sent to an interpreter as part of a command or query. It tricks it into executing unintended commands without proper authorization.

Another security risk is broken authentication which is application function related to authentication and session management are often implemented incorrectly allowing attackers to compromise passwords, keys or session tokens to assume identities temporarily or permanently. Another vulnerability is using components with known vulnerabilities such as libraries, frameworks and other software modules, run with the same privileges as the application. If a vulnerable component is exploited, such an attack can facilitate serious data loss or server takeover. Applications and APIs using components with known vulnerabilities may undermine application defenses and enable various attacks and impacts. Other worth noting vulnerabilities are insufficient logging and monitoring, Insecure deserialization, cross-site scripting which means when an application includes untrusted data in a new web page without proper validation, Security misconfiguration which is the most common and lastly broken access control.

### **Mitigation of Web-Security Vulnerabilities.**

Thus, in web security it is important to test vulnerabilities, but it is not all about testing authentication and authorization but also testing the business logic and use of proper input validation and output encoding. The goal is to ensure that the functions exposed in the web application are secure. (SYNOPSYS, 2020). In order to get ahead of the situation there needs to be test and prepare the web-application and learn its vulnerabilities and defects as early on before deployment.

(SYNOPSYS, 2020) mentioned some of the security test that can be done in order to test web application for defects. Which are; Dynamic Application Security Test (DAST) which is an automated security test that is best for internally facing, low risk applications that must comply with regulatory security assessments. If you are going to test a medium risk and high-risk application, it is best to combine it with some manual security testing for common vulnerabilities solutions.

Another test is the static application security test (SAST) which offers automatic and manual testing technique, it is best for identifying bus without the need to execute applications in a production environment. It also scans source code and systematically find and eliminates software security vulnerabilities.

Also, one of the common tests is the penetration test, which is a manual application security test and it the best for critical applications especially these undergoing major changes. The assessment involves business logic and adversary -based testing to discover advanced attack scenarios and finally the Runtime Application Self Protection (RASP) which is an evolving application security approach that encompasses a number of technological techniques to instrument and application so that attacks can be monitor as they execute and ideally, blocked in real time.

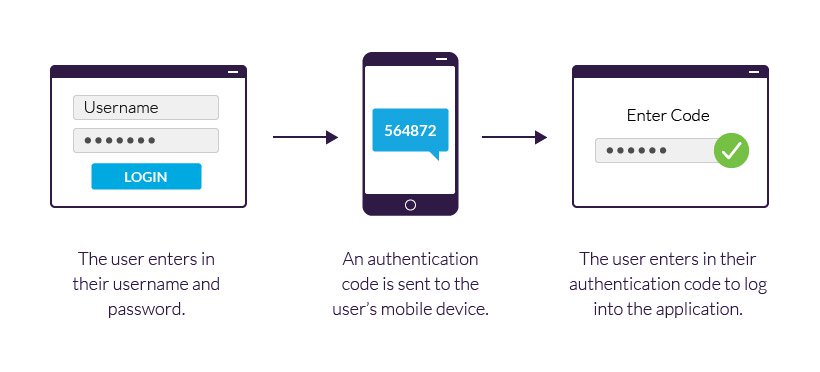
In our case study of researching best practices for implementing online care for people living with HIV/Aids and its security different scholars have written on different technologies that are huge factor in ensuring success of the system. The major technologies used are two factor authentication and encryption which will be expounded by various researches below.

* + 1. **Two Factor Authentication.**

security experts say two factor authentication is one of the best ways to protect your online accounts (WHITTAKER, 2018). Two factor authentications (2FA) as described by (KENTON, 2020) is a security system that requires two distinct forms of identification in order to access something.

Two-factor authentication can be used to strengthen the security of an online account, a smartphone, or even a door. 2FA does this by requiring two types of information from the user, a password or [personal identification number (PIN)](https://www.investopedia.com/terms/p/personal-identification-number.asp), a code sent to the user's smartphone, or a fingerprint before whatever is being secured can be accessed. Two-Factor Authentication is designed to prevent unauthorized users from gaining access to an account with nothing more than a stolen password. The thief will be stuck as he would have just accessed the first layer of security broken and finding another layer of security which no makes the password they have not as useful as a one layered system.

Two Factor Authentication is a combination of the following one something you know which is your password and something you have such as a text with code sent to your smartphone or other devices, or a smartphone authenticator application and finally through the use of biometrics using your fingerprint, face or retina scan. (KENTON, 2020). The three categories mentioned above are namely knowledge factors, possession factors and inherence factor all respectively (IMPERVA, 2019).



**Figure 1 Two-Factor Authentication.**

Two factor authentication as mentioned by (IMPERVA, 2019) bolsters security by making it very difficult for intruders to gain unauthorized access even when the first layer of defense is got past through.

Two Factor authentication is important as Gone are the days where your trusty password can protect you. Even if you have a unique password for every website you use, there’s little in the way to stop malware on your computer (or even on the website!) from scraping your password and using it again. Or, if someone sees you type in your password, they can memorize it and log in as you.

Don’t think it’ll happen to you? So-called “credential stuffing” or brute-force attacks can make it easy for hackers to break in and hijack people’s online accounts in bulk. That happens all the time. [Dunkin’ Donuts](https://threatpost.com/hackers-breach-dunkin-donuts-accounts-in-credential-stuffing-attack/139472/), [Warby Parker](https://www.scmagazine.com/home/security-news/credential-stuffing-attack-focuses-on-glasses-retailer-warby-parker/), [GitHub](https://www.zdnet.com/article/github-warns-some-accounts-compromised-after-reused-password-attack/), [AdGuard](https://techcrunch.com/2018/09/20/adguard-resets-all-user-passwords-after-account-hacks/), the [State Department](https://techcrunch.com/2018/09/18/state-department-confirms-data-breach-exposing-employee-data/) — and even [Apple iCloud](https://www.zdnet.com/article/icloud-accounts-breach-gets-bigger-here-is-what-we-know/) accounts have all fallen victim to credential-stuffing attacks in recent years. Only two-factor accounts are protected from these automated log-in attacks (WHITTAKER, 2018).

Two-factor also protects you against phishing emails. If someone sends you a dodgy email that tries to trick you into logging in with your Google or Facebook username and password to a fake site, for example, two-factor can still protect you. Only the legitimate site will send you a working two-factor code. (WHITTAKER, 2018).

**2.2.4 Database security best practices.**

As we secure the website and put mitigation to prevent access to it one important factor is the database and its security. The database will be the one storing the patient’s credentials and the availability of drugs. thus, being a very vital part in this study. A check list was provided by IST system administrators to provide guidance for securing databases storing sensitive or protected data. This will help prevent data loss, leakage, or unauthorized access to the database. (RUBENS, 2021).

This case study when fully implemented, will need to run on server to operate the database due to the amount of traffic the website is going to be generating as many patients will be accessing the site at same time. The database will need to connect to a remote database as described by (Schandl, 2017) and there are implications to it such as; the database host needs to be reachable from the application servers, the application servers need to know the credentials that they need to connect and finally there is some traffic going over a network that contains data in this case allocation of drugs to patients which are highly sensitive and prone to manipulation. Taking a closer look at what the most critical elements of this part of the application are: access to the network traffic between your application server and the database, access to your database host on the network level, and access to the database itself (which will require having the database credentials). Most definitely we don’t want someone to listen to the traffic between our application servers and our database. If an attacker is able to physically connect to our database server, they probably will not be able to get data out of this. Still, it opens the possibility to cause harm, like Denial-of-Service attacks or brute-forcing database credentials. (Schandl, 2017).

The database credentials (i.e., the username and password that our application uses to connect to the database) are one of the most critical pieces of information in the infrastructure. In combination with physical access to the database, an attacker might be able to read data, or (even worse) modify or delete data in the database (which in this case is drug allocation and patients’ details).

(Schandl, 2017) in his article advises what can be done to avoid the above situations on the database system. One is the database needs to be encrypted, depending on the type of database to use an example MySQL, SSL (Secure Socket Layer which is a protocol for establishing authenticated and encrypted links between networked computers) support is already provided and can easily be embedded. another measure to undertake is to move all the infrastructure to a private network, but it has to allow incoming connections from outside. Amazon web services provide an excellent mechanism to so through technology known as Virtual Private Cloud (VPC) which allows users to segregate their network into sub-networks and control traffic that is allowed between these networks. (Schandl, 2017). Another best practice as described by (RUBENS, 2021) is to audit and continuously monitor database activity which includes logins and attempted logins to the OS and database and reviewing the log files regularly to detect anomalous activity. In auditing and monitoring, creating alerts to notify team members when potential malicious activity is identified.

This database practices when implemented correctly will surely provide away for the case study to develop a system that will provide secure services and will ensure integrity, accountability and better service care is offered to all.

* 1. **Summary.**

Computer information network technology in the world of rapid development, making the information network has been the most widespread, people actively participate in the Internet at the same time, and the computer network security issues are also a serious threat. The problem of computer network security is a long way to go to solve the task, and data encryption technology to solve this problem is the main means for the maintenance of computer network security made a significant contribution. With the development of information era, computer data encryption technology has also made a more in-depth study, researchers should continue to carry out technological innovation, and the data encryption technology has become an effective guarantee for the maintenance of computer network security. The data encryption system designed in this study case makes full use of data encryption technology and digital signature technology, which not only solves the key management problem, but also ensures the integrity and nonrepudiation of the data.

Some worth mentioning practices such as two factor authentication, ensuring the database is secure and performing database encryption will guarantee a secure website, but system is never full proof from vulnerabilities as everyday there are new threats that emerge from the shadows which are unknown and there is no way to combat them, the only way is to be vigilant and always ready, and when that day comes, the loss will be mitigated or prevented.

**References.**

L. Liu. Data encryption technology in the application of computer network security value [J]. Electronic Technology and Software Engineering, 2015.

W. Tang. Cryptography and network security technology foundation [M]. Beijing: Mechanical Industry Press. 2004.

Q. Zhang. Data encryption technology in the computer network communication security application. Electronic World, 2014.

Eiw, N. (2016, March 3). *Online Security*. Retrieved from Ingenium: https://www.ingeniumweb.com/blog/post/why-web-application-security-is-important-in-every-step-of-web-application-development/2432/

FORBES. (2020, August 9). *Cybersecurity Spending To Reach $123B In 2020*. Retrieved from FORBES: https://www.forbes.com/sites/louiscolumbus/2020/08/09/cybersecurity-spending-to-reach-123b-in-2020/?sh=40245099705f

GOODFIRMS. (2020). *What is Web Security?* Retrieved from Good firms: https://www.goodfirms.co/glossary/web-security/

IMPERVA. (2019). *Two Factor Authentication (2FA)*. Retrieved from IMPERVA: https://www.imperva.com/learn/application-security/2fa-two-factor-authentication/

IMPERVA. (2020). *Web Application Security*. Retrieved from Imperva: https://www.imperva.com/learn/application-security/application-security/

Johnson, P. (2020, November 5). *What is application security? A process and tools for securing software*. Retrieved from WhiteSource: https://resources.whitesourcesoftware.com/blog-whitesource/application-security

Kenton, W. (2020, September 28). *Cybersecurity*. Retrieved from Investopedia: 2020

OWASP. (2017). *OWASP Top ten*. Retrieved from OWASP: https://owasp.org/www-project-top-ten/

Rubens, P. (2021, March 5). *Database Security Best Practices*. Retrieved from eSecurity Planet: https://www.esecurityplanet.com/networks/database-security-best-practices/

Schandl, B. (2017, November 3). *Securing your Web Application Database*. Retrieved from Medium: https://medium.com/monsterculture/securing-your-web-application-database-ca7d667cd6ce

SYNOPSYS. (2020). *What is Web Application Security?* Retrieved from SYNOPSYS: https://www.synopsys.com/glossary/what-is-web-application-security.html

VERO. (2021). *2FA – Two Factor Authentication*. Retrieved from VERO: https://www.verovoting.com.au/2fa-two-factor-authentication/

Whittaker, Z. (2018, December 25). *Cybersecurity 101: Two-factor authentication can save you from hackers*. Retrieved from Techcrunch: https://techcrunch.com/2018/12/25/cybersecurity-101-guide-two-factor/?guccounter=1&guce\_referrer=aHR0cHM6Ly93d3cuZ29vZ2xlLmNvbS8&guce\_referrer\_sig=AQAAAJ\_xycEqDoWmzx1YUGYrEjwAlObVLbrU-QYYMFAR9qHLN5V2hcgEOh31ZxkaSwcxZCM76FRtX\_DNAyZfb7JLd0Qubl4kAnwseEBdnVB\_

# Resource Requirements.

## **Hardware**

A Personal Computer with:

HDD Storage:500GB

RAM:4GB

Processor: Intel(R) Core (TM) i5-3427U CPU @ 1.80GHz 2.30 GHz

System type: 64-bit operating system, x64-based processor

## **Software**

Operating System: Windows 10

Browser: Chrome or Firefox

Local Server Application: XAMPP

IDE: Visual Studio Code / PHP Storm

MS Office Suite

# Appendix

## **Appendix 1: Project Schedule**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Task | Duration in weeks | Expected start date | Actual start date | Expected finish date | Actual finish date | Deliverables |
| Proposal writing | 2 | 01/07/2021 | 01/07/2021 | 12/07/2021 | 14/07/2021 | Proposal Document |
| Proposal Presentation | 1 | 15/07/2021 | 22/07/2021 | 16/07/2021 | 23/07/2021 | Project proposal |
| Data collection | 2 | 01/08/2021 |  | 14/08/2021 |  | Data |
| Analysis | 1 | 16/08/2021 |  | 21/08/2021 |  | Requirement |
| Feasibility  Study | 3 | 23/08/2020 |  | 11/09/2020 |  | Study |
| Coding and Testing | 3 | 13/09/2021 |  | 02/10/2021 |  | Error free system |
| System  Implementation | 2 | 4/10/2021 |  | 16/10/2021 |  | Working system |
| System maintenance | 2 | 18/10/2021 |  | 30/10/2021 |  | Maintenance |
| Project Documentation | 2 | 1/11/2021 |  | 13/11/2021 |  | Documentation |
| Project Presentation | 10 minutes |  |  |  |  | Project report |

## **Appendix 2: Gantt Chart**

## **Appendix 3: Budget**

|  |  |  |  |
| --- | --- | --- | --- |
| **Item** | **Quantity** | **Specification** | **price** |
| Laptop | 1 | Hp Elitebook | Free |
| Stationary | 4 | File, pen, hardcover A4 book, fulscaps, | 1,000 |
|  |  |  |  |
|  |  |  |  |
| Flash disc | 1 | Sandisk (8GB) | 2,000 |
| Miscellaneous | - | - | 3,500 |
| Data Bundles | 20GB | 1 month data bundle | 2,000 |
| **TOTAL COST** | **-** | **-** | **8,500** |