

**SECURED ONLINE EXAMINATION RESULT SYSTEM (USING PUBLIC KEY
INFRASTRUCTURE (PKI))**

CASE STUDY: KAMPALA INTERNATIONAL UNIVERSITY

BY

**KIMANI WILSON MBURU
BCS/14564/71/DF**

AND

**FATUMA NG'AARI
BCS/14558/71/DF**

**A GRADUATION PROJECT REPORT SUBMITTED TO THE SCHOOL OF
COMPUTER STUDIES IN PARTIAL FULFILLMENT OF THE
REQUIREMENTS FOR THE AWARD OF THE DEGREE
OF BACHELOR OF COMPUTER SCIENCE**

OF

KAMPALA INTERNATIONAL UNIVERSITY

JUNE 2010

DECLARATION

This is to confirm that we, Kimani Wilson Mburu and Fatuma Ng'aari, undertook this project as our third year project that was carried out in partial fulfillment of the requirements for the Degree of Bachelor of Computer Science. We also confirm that this is our original work and has not been presented in this or any other university for examination or for any other purposes.

Kimani Wilson Mburu

BCS/14564/71/DF

Student

.....*Wilson*.....

Date.....*02/07/10*.....

Fatuma Ng'aari

BCS/14558/71/DF

Student

.....*02/07/2010*.....

Date.....*[Signature]*.....

Signed:

Mr. Kimani Njoroge

Supervisor

.....

Date.....

DEDICATION

We dedicate this research work to our parents Mr. and Mrs. Tirus Mburu Chege who continually gave us moral and financial support to undertake our studies. You have indeed helped us come this far and with lots of love to you we say God bless.

ACKNOWLEDGEMENTS

Our special thanks go to Mr. Kimani Njoroge, who offered his time and guidance, and for sharing with us his profound professional insight. Without him we wouldn't have reached where we are today in our research.

We thank all those individuals and organizations around the world who are contributing in a positive manner to network security. Your efforts, ranging from Internet discussions and press clippings to extensive resource archives and in-depth studies, have been an important source of inspiration to our work.

We would also like to thank our guardians Mr. and Mrs. Kimani Mwangi, Mr. and Mrs Holden, Mr. and Mrs. Ng'aari Gatibaru, Mr. and Mrs. Kagiri Njoroge and all our family members for always giving us hope that there will be light at the end of the tunnel and continually encouraging us all through.

Finally, our thanks go to our friends Kamochu, Alice Wambui, Gideon, Tony Kimz and Chybz, Jeff, Hassan, Nelson and all our friends since we can't mention all for mentoring us and always being there for us.

Thank you all and may God bless you abundantly.

TLS

Transport Layer Security

VOIP

Voice Over Internet Protocol

TABLE OF CONTENT

DECLARATION	ii
DEDICATION	iii
ACKNOWLEDGEMENTS	iv
ABBREVIATIONS	v
TABLE OF CONTENT	vii
LIST OF FIGURES:	xii
LIST OF TABLES	xiii
ABSTRACT	xiv
CHAPTER ONE	1
1.1 Background	1
1.2 Statement Of The Problem	2
1.3 Objectives	3
1.3.1 Main Objective	3
1.3.2 Specific Objectives	3
1.4 Research Questions	3
1.5 Scope	4
1.6 Justification	4
1.7 Limitations Of The Study	5
1.8 Conclusion	5
CHAPTER TWO	7
LITERATURE REVIEW	7
2.1 Introduction	7
2.2 Information System	7

2.2.1	Types Of Information Systems	7
2.2.2	Benefits Of An Information System	9
2.2.3	Designing A Management Information System	9
2.3	Software Development.....	12
2.4	Security.....	14
2.4.1	Classification Of Encryption Algorithms	14
2.4.2	Security Threats & Requirements	15
2.4.3	Security Services & Mechanisms	16
2.4.4	Network Security Protocols	17
2.4.5	Secure Socket Layer & Transport Layer Security (SSL/TLS).....	18
2.5	Emergence Of Public Key Cryptography (Pkc).....	20
2.5.1	Emergence Of Public Key Cryptography (PKC).....	21
2.5.2	Public Key Cryptography (Asymmetric Key Cryptography)	22
2.6	Application: Secure Electronic Transaction (SET)	22
2.6.1	Description.....	22
2.7	Certificate Authority	22
2.8	The Digital Certificate (Public Key Certificate)	23
2.8.1	Description.....	23
CHAPTER THREE		25
METHODOLOGY		25
3.1	Introduction	25
3.2	Procedure Of The Study.....	25
3.3	Population Of The Area Of Study.....	25

3.4	Data collection methods	26
3.4.1	Primary Methods.....	26
3.5	Analysis Of The Current System	26
3.5.1	Strengths of the current system.....	26
3.5.2	Weaknesses Of The Current System.....	26
3.6	The Proposed System	27
3.7	System Requirements.....	27
3.7.1	Hardware Requirements.....	27
3.7.2	Software Requirements	28
3.7.3	Security Requirement.....	30
3.8	Feasibility Study.....	31
3.8.1	Introduction.....	31
3.8.2	Technical Feasibility.....	32
3.8.3	Operational Feasibility.....	32
3.9	Feasibility Report.....	33
3.10	Recommendation	34
3.11	Benefits Of The Feasibility Study.....	34
3.12	Conclusion	34
CHAPTER FOUR.....		36
SYSTEM DESIGN		36
4.1	Introduction	36
4.2	E-R (Entity Relationship) Model	37
4.3	DFD For The New System.....	39

4.4	Data Dictionary	39
4.5	Data Description.....	40
4.6	Data Structures	41
4.7	Data Elements	42
4.8	Data Stores	43
4.9	Relational Model	43
4.10	Physical Model.....	44
4.11	Database Design.....	47
4.12	Interface Design	47
4.13	Website Sitemap.....	48
4.14	Conclusion.....	48
CHAPTER FIVE		49
SYSTEM IMPLEMENTATION		49
5.1	Introduction	49
5.2	Main System Components	50
5.2.1	User Registration	50
5.2.2	User Authentication	52
5.2.3	Changing Profile	52
5.2.4	Recording Examination Marks	54
5.2.5	Reports.....	55
5.3	Security Implementation	57
5.4	System Implementation Summary	58
5.5	Conclusion.....	58

SIX.....	59
RECOMMENDATIONS AND CONCLUSIONS	59
6.1 Introduction.....	59
6.2 Recommendation.....	59
6.3 Conclusion.....	59
6.4 Future Work	61
APPENDIX A: QUESTIONNAIRE.....	62
REFERENCES	65

LIST OF FIGURES:

Figure 1.0: Conceptual Database (E-R) Model.....	36
Figure 1.1: Data Flow Diagram - Context Diagram	38
Figure 1.2 : Website sitemap	47
Figure 1.3: student registration details.....	51
Figure 1.4: User verification.....	51
Figure 1.5: User authentication.....	52
Figure 1.6: User profile.....	53
Figure 1.7: Staff units	54
Figure 1.8: Class list	55
Figure 1.9: Class report.....	56
Figure 1.10: Graphical report.....	56

LIST OF TABLES

Table 1.0: Research Budget	33
Table 1.1: Data Description	39
Table 1.2: Data Elements	41
Table 1.3: Data stores	42
Table 1.4: Course relation.....	43
Table 1.5: Unit relation.....	43
Table 1.6: Student relation.....	44
Table 1.7: Staff relation	44
Table 1.8: Course unit relation.....	44
Table 1.9: Staff unit relation	45
Table 1.10: Result relation.....	45
Table 1.11: User relation.....	46

ABSTRACT

This study showed how efficiency and security can be enhanced in the management of examination result of students in the school of computer studies

The researchers went to the case study and used interview, observation and dissemination of questionnaires, to collect data at the school with a bias towards the examination office.

This data was then analyzed and a using Software Development Life Cycle (SDLC) developed a secured network application. (Secured Online Examination Result Management System)

CHAPTER ONE

INTRODUCTION

1.0 Introduction

In the last few decades, the world has seen a lot happen in the field of network applications. Many online applications have been developed. These include online businesses, asset management systems, and examination results systems. E-commerce is one the biggest fields that have utilized networks and specifically the Internet. The biggest challenge in e-commerce has been to ensure a solution provider has earned the customers' trust before they conduct business online even at a time when identity theft and fraud is on the rise.

With this development, security is becoming a paramount aspect that cannot be overlooked. When mentioning about security of a web application, it is difficult not to consider the security of the platform upon which the web application sits. That is network security. Research indicates there are various methods that have been established to secure networks. This research focuses on the establishment of a web application and the related security thereof. Kampala International University (KIU)'s School of Computer Studies has been used as a case study

1.1 Background

Kampala International University is a higher learning institution located in Kansanga 3km away from Kampala city in Uganda. It has a student population of approximately 7000. A huge cross section of these students is of foreign origin. That means the sponsors are based in other countries other than Uganda. This implies for them to know the

progress on the performance of their dependants, they have to only rely on the dependants to furnish them with the information.

Majority of the work in faculties and schools is done of paper-based on computer-based systems. A key aspect is student-result processing. A huge chunk of it is done on papers that are then transferred onto Microsoft Excel spreadsheet. It is from the latter that each student's result is printed and pinned for viewing. Once the student view his/her result, if there are mistakes, the latter thereafter lodges a complaint with the head of department in respective faculty/school. This marks begins the start of a lengthy, cumbersome and redundant process of fixing the problem. This is the motivation of this study.

1.2 Statement of the Problem

At KIU, currently, results are slowly processed such that by the time they are availed, the proceeding semester is almost in the middle of the next semester. This a huge problem to both the student and the sponsor because neither can make a reliable decision about the proceeding new semester on time.

There is need for an application that can help the students and hopefully the sponsors to access their information online on time for timely decision making about the proceeding semester.

However, to have an effective web application, one should be aware of the potential threats that web applications face. This research has a strong bias towards the security aspect of web applications. This is demonstrated on the application developed for Student Result Management System.

1.3 Objectives

Objectives of this study have been divided into:

1.3.1 Main Objective

To study current system used to manage student results at the School of Computer Studies and hence develop and implement a secure online examination result system

1.3.2 Specific Objectives

- Study the challenges experienced at the School of Computer Studies in relation to Student Result Management.
- Identify the possibilities of developing an online Student Result Management System for the School of Computer Studies.
- To Identify the vulnerabilities / challenges / attacks in network security (attacks in algorithms used in PKI) related to web-based applications.

1.4 Research Questions

The following are some of the questions that will be answered by the project.

1. What are the challenges experienced at the School of Computer Studies related to Student Result Management System?
2. What are the possibilities of developing an online Student Result Management System for the School of Computer Studies of KIU?
3. What are the vulnerabilities or challenges and their related solutions that would affect the network security of the web based application that would be developed for the School of Computer Studies of KIU?

1.5 Scope

The School of Computer Studies of Kampala International University serves as the scope of this study. At this school, mainly the focus will be the office of the examination office as well as that of the administrator that will be key focal points.

This study will examine the current examination result system used and the proposed development. It will also identify the users who access results online, their authorization, authentication and the extent to which they can manipulate the information.

1.6 Justification

Majority of the work in faculties and schools is done of paper-based on computer-based systems. A key aspect is student-result processing. A huge chunk of it is done on papers that are then transferred onto Microsoft Excel spreadsheet. It is from the latter that each student's result is printed and pinned for viewing. Once the student view his/her result, if there are mistakes, the latter thereafter lodges a complaint with the head of department in respective faculty/school. This marks begins the start of a lengthy, cumbersome and redundant process of fixing the problem. This is the motivation of this study.

There is need for an application that can help the students and hopefully the sponsors to access their information online on time for timely decision making about the proceeding semester.

The school of computer studies has personnel that is well skilled with current technology therefore they will be able to feed the results into the system directly without having to do any paper work. This will cut down costs incurred in paper work and the data fed into the

system if the first hand information. The school also has computers that are well networked and hence each and every one will be able to access the services provided by the system with ease. The students will be able to view their results early in the semester and in case of problems raise complaints before it is late and hence avoid inconveniences.

1.7 Limitations of The Study

1. Time-The time frame within which the new system is supposed to be delivered was too short. This was even aggravated by gathering the requirement of the new system as some staff members whom we targeted for the interview were busy and some didn't know how the current system operates.
2. The implementation part longer time compared to the time frame which was rather a short time given that we had five other academic units to take during the same period
3. More than 50% of the staff and students have little or no skills or knowledge in using Linux based operating systems. So there is need of training them.

1.8 Conclusion

Despite the fact that the management of exam results is paper-based computer-based result tracking and handling has been cumbersome and the process takes a long time and becomes more costly.

The new system will be able to provide a better way of handling exam results in a secured connection eliminating issues of hacking or eavesdropping.

The system will also provide security of data stored that is, exam marks from being viewed by people with access to the database and in transit from modification and tampering.

The company will benefit in this research as the data is combined into an automated system resulting in cost saving, this is due to reduction in manpower needed to transfer exam results from paper-based to computer-based system. Data can be shared, redundancy reduced, inconsistency can be avoided and security enforced to a large extent.

CHAPTER TWO

LITERATURE REVIEW

2.1 Introduction

This chapter looks into the security aspects of network systems and applications. Much attention is given to the various methods employed to provide security over networks as well as detailed discussion about information systems.

2.2. Information System

O'Brien (2000), describes information systems as the system that can be any organized combination of people, hardware, software, communication network and data resources that collects, transforms, and disseminates information in an organization.

Kiema (2003), describes an information system as a set of interrelated components working together to collect, process, store and disseminate information to support decision making, coordination, control, analysis and visualization in an organization.

2.2.1 Types Of Information Systems

Businesses tend to have several "information systems" operating at the same time. There are several kinds of information systems in business as described below:

- Executive Support Systems – These are systems designed to help senior management make strategic decisions. It gathers analyses and summarizes the key internal and external information used in the business.
- Management Information Systems (MIS) - Systems mainly concerned with internal sources of information. MIS usually take data from the transaction

processing systems. MIS reports tend to be used by middle management and operational supervisors.

- Decision Support Systems (DSS) - Systems specifically designed to help management make decisions in situations where there is uncertainty about the possible outcomes of those decisions. They comprise tools and techniques to help gather relevant information and analyze the options and alternatives. DSS often involves use of complex spreadsheet and databases to create "what-if" models.
- Knowledge Management Systems (KMS) - Exist to help businesses create and share information. These are typically used in a business where employees create new knowledge and expertise - which can then be shared by other people in the organization to create further commercial opportunities. Good examples include firms of lawyers, accountants and management consultants.

KMS are built around systems which allow efficient categorization and distribution of knowledge. For example, the knowledge itself might be contained in word processing documents, spreadsheets, PowerPoint presentations, internet pages etc. To share the knowledge, a KMS would use group collaboration systems such as an intranet.

- Transaction Processing Systems - As the name implies, Transaction Processing Systems ("TPS") are designed to process routine transactions efficiently and accurately. A business will have several TPS; for example:
 - i) Billing systems to send invoices to customers
 - ii) Systems to calculate the weekly and monthly payroll and tax payments
 - iii) Production and purchasing systems to calculate raw material requirements

- iv) Stock control systems to process all movements into, within and out of the business
- v) Exam results management systems
- Office Automation Systems - Office Automation Systems are systems that try to improve the productivity of employees who need to process data and information. Perhaps the best example is the wide range of software systems that exist to improve the productivity of employees working in an office (e.g. Microsoft Office XP) or systems that allow employees to work from home or whilst on the move.

2.2.2 Benefits Of An Information System

O'Brien (2000) says successful management of information systems and technologies presents major challenges to managers and professionals such as:

1. Information systems are a major source of information and support needed to promote effective decision making by managers and business professionals.
2. They provide a dynamic, rewarding, and challenging career opportunity for millions of men and women.
3. An information system is a key component of the resources, infrastructure, and capabilities of today's e-business enterprises.
4. It is also an important contributor to operational efficiency, employee productivity and morale, and customer-service and satisfaction.

2.2.3 Designing A Management Information System

An MIS can be generally described as any system that provides people with either data or information relating to an organization's operations. It involves activities which include:

- Planning – information about situations and goals.

- Organizing – information to help set objectives to attain these goals.
- Staffing – information about human resources.
- Directing – information to workers concerning implementation of plans
- Controlling – feedback to monitor progress.

Such activities and business processes involve complex information flows within the organization.

Characteristics of MIS are:

- Support structured decisions at the operational and management control levels.
However, they are also useful for planning purposes of senior management staff.
- MIS are generally reporting and control oriented, are designed to report on existing operations and therefore to help provide day-to-day control of operations.
- MIS rely on existing corporate data and data flows.
- They have little analytical capability.
- MIS generally aid in decision making using past and present data.
- They are relatively inflexible.
- MIS have an internal rather than an external orientation.

Architecture of MIS:

- Input: Transaction Processing system + Internal and External data (High volume data)
- Processing: Management software or a program bearing simple models.
- Output: Management reports: Scheduled reports, Exception reports, Demand reports and other reports.

The internal and external information needs of management as inputs to the MIS can be classified as follows:

Internal Information needs:

- Activity Information – information techniques that summarize, analyze, and evaluate the activities taking place in the business operation.
- Status Information – information in the performance status of various aspects such as customer accounts, work in process, project completion reports and so forth.
- Resource Information – information about resources of the business system: personnel / material / facilities.
- Planning and control Information – information and techniques required for producing plans, budgets, schedules, project specifications, forecasts and standards.
- Resource Allocation Information – information and techniques for cost-benefit analysis.

External Information needs:

- Politics and government – political / legal / legislative / laws and regulations / Fiscal policies and so forth.
- Society – demographic / cultural / social trends.
- The economy – Gross Domestic Product (GDP) and other economic indicators.

- Competition – information about competitors in the industry.
- Technology – the technology on new products and processes
- Resources – information on past and present status and expected trends in the supplies of information.

2.3 Software Development

This is a systematic and orderly approach to solving system problems. While this approach comes in different formats, it usually incorporates the following steps:

1. Planning – Identifying the scope and boundary of the problem, planning the development strategy and goals, conducting a feasibility study and establishing the project plan.

Deliverables:

- Identification and prioritization of information system needs.
- Problem is identified and articulated.
- Business case or system justification.
- Project scope.
- Project feasibility.
- Selection of system development participants.
- Project (work) plan.

2. Systems Analysis – Studying and analyzing the problems, causes and effects, and the requirements that must be fulfilled by any successful solution.

Deliverables:

- Description of the current system/environment.
- Determine and structure functional requirements.

- Identification of alternatives.
- Initial system models are built.

3. Systems Design – Designing how the requirements are to be met by the new system, defining technical specifications.

Deliverables:

- Technical detailed specifications of all systems elements (programs, files, network, system software, etc.).
- Interface design.
- Database and file design.

4. System Construction – Building or selecting software

5. System Implementation – Testing the system and training users. Getting the system running and beginning to use it.

Deliverables:

- Software code.
- Documentation
- Installation plan.
- Testing plan.
- Training procedures.
- Initial support capabilities outlined.
- Maintenance plan.
- Evaluation plan.

6. Evaluation – Evaluating the implemented solution, refining the design and implementing improvements.

2.4 Security

2.4.1 Classification of Encryption Algorithms

The new exam result management system will use encryption algorithms to convert plain text(exam results) in a format that can not be understood by the hacker or intruder(cipher text).

Günter (2003) classifies encryption algorithms in dimensions; the type of operations used for transforming plaintext to cipher text, the number of keys used, and the way in which the plaintext is processed.

Type of operations used in transforming plaintext to cipher text:

- **Substitution**, which maps each element in the plaintext (bit, letter, group of bits or letters) into another element
- **Transposition**, which re-arranges elements in the plaintext

The number of keys used:

- **Symmetric ciphers**, which use the same key for en / decryption
- **Asymmetric ciphers**, which use different keys for en / decryption

The way in which the plaintext is processed:

- **Stream ciphers** work on bit streams and encrypt one bit after another. Many stream ciphers are based on the idea of linear feedback shift registers, and there have been detected vulnerabilities of a lot of algorithms of this class, as there exists a profound mathematical theory on this subject. Most stream ciphers do not propagate errors but are sensible to loss of synchronization.
- **Block ciphers** work on blocks of width b with b depending on the specific algorithm.

2.4.2 Security Threats & Requirements

The new exam result management system needs to be secure against threats to data stored in the database and data in transit.

According to Kauffman, Perlman, Spenser (2002), Network Security A threat in a communication network is any possible event or sequence of actions that might lead to a violation of one or more security goals. The actual realization of a threat is called an attack. Examples of Threats:

- A hacker breaking into a corporate computer
- Disclosure of emails in transit
- Someone changing financial accounting data
- A hacker temporarily shutting down a website
- Someone using services or ordering goods in the name of others

Security Goals Technically Defined:

- **Confidentiality:** Data transmitted or stored should only be revealed to an intended audience. Confidentiality of entities is also referred to as anonymity
- **Data Integrity:** It should be possible to detect any modification of data. This requires to be able to identify the creator of some data
- **Accountability:** It should be possible to identify the entity responsible for any communication event.
- **Availability:** Services should be available and function correctly.
- **Controlled Access:** Only authorized entities should be able to access certain services or information

Threats Technically Defined:

- Masquerade: An entity claims to be another entity

- Eavesdropping: An entity reads information it is not intended to read
- Authorization Violation: An entity uses a service or resources it is not intended to use
- Loss or Modification of (transmitted) Information: Data is being altered or destroyed
- Denial of Communication Acts (Repudiation): An entity falsely denies its' participation in a communication act
- Forgery of Information: An entity creates new information in the name of another entity
- Sabotage: Any action that aims to reduce the availability and / or correct functioning of services or systems (Wikipedia, 2008).

2.4.3 Security Services & Mechanisms

The new system utilizes the security services and mechanisms that make sure that connections and data is secure.

Security Service is an abstract service that seeks to ensure a specific security property. It can be realized with the help of cryptographic algorithms and protocols as well as with conventional means:

- One can keep an electronic document on a floppy disk confidential by storing it on the disk in an encrypted format as well as locking away the disk in a safe
- Usually a combination of cryptographic and other means is most effective

- Authentication: The most fundamental security service which ensures, that an entity has in fact the identity it claims to have
- Integrity: In some kind, the “small brother” of the authentication service, as it ensures, that data created by specific entities may not be modified without detection
- Confidentiality: The most popular security service, ensuring the secrecy of protected data
- Access Control: Controls that each identity accesses only those services and information it is entitled to
- Non repudiation: Protects against that entities participating in a communication exchange can later falsely deny that the exchange occurred

2.4.4 Network Security Protocols

The system aims at protecting data in transit. Hence security at transport layer has to be considered and also the protocols in that layer

Network can be secured at different layers in the OSI model. Network security protocols in the layer 2 (link layer) include; IEEE 802.1x and PPP & PPTP.

The main security protocol in layer 3 is the IP Security Architecture (IPSec). The security protocols in layer 4 (Transport layer) are the Secure Socket Layer (SSL) and Secure Shell.

In our research, we will only concentrate on the Transport Layer Security, dwelling on the

SSL and SSH.

2.4.5 Secure Socket Layer & Transport Layer Security (SSL/TLS)

Transport Layer Security (TLS) Protocol (Wikipedia, 2008) and its predecessor, Secure Sockets Layer (SSL), are cryptographic protocols that provide security and data integrity for communications over TCP/IP networks such as the Internet. Several versions of the protocols are in wide-spread use in applications like web browsing, electronic mail, Internet faxing, instant messaging and voice-over-IP (VoIP).

TLS involves three basic phases:

- Peer negotiation for algorithm support
- Key exchange and authentication
- Symmetric cipher encryption and message authentication

Typical algorithms are:

- For *key exchange*: RSA, Diffie-Hellman, ECDH, SRP, PSK
- For *authentication*: RSA, DSA, ECDSA
- *Symmetric ciphers*: RC4, Triple DES, AES, IDEA, DES, or Camellia. In older versions of SSL, RC2 was also used.
- For *cryptographic hash function*: HMAC-MD5 or HMAC-SHA are used for TLS, MD5 and SHA for SSL, while older versions of SSL also used MD2 and MD4.

TLS runs on layers beneath application protocols such as HTTP, FTP, SMTP, NNTP, and XMPP and above a reliable transport protocol.

Security

TLS/SSL has a variety of security measures:

The client may use the certificate authority's (CA's) *public* key to validate the CA's *digital signature* on the server certificate. If the digital signature can be verified, the client accepts the server certificate as a valid certificate issued by a trusted CA.

- The client verifies that the issuing CA is on its list of trusted CAs.
- The client checks the server's certificate validity period. The authentication process stops if the current date and time fall outside of the validity period.
- Protection against a downgrade of the protocol to a previous (less secure) version or a weaker cipher suite.
- Numbering all the Application records with a sequence number, and using this sequence number in the *message authentication codes* (MACs).
- Using a message digest enhanced with a key (so only a key-holder can check the MAC). This is specified in RFC 2104. *TLS* only.
- The message that ends the handshake ("Finished") sends a hash of all the exchanged handshake messages seen by both parties.
- The pseudorandom function splits the input data in half and processes each one with a different hashing algorithm (MD5 and SHA-1), then XORs them together to create the MAC. This provides protection even if one of these algorithms is found to be vulnerable. *TLS* only.

- For confidentiality, A can send a private message to B by encrypting the message with B's public key (readily available) because only B holds the private key to decrypt it.
- For authenticity, A can send B a message encrypted with A's private key. B can be certain it came from A because it can be decrypted only by using A's public key. The identity of the sender is verifiable because only A has access to A's private key. This is the principle behind the digital signature.

In addition, each community needs a trusted third party to investigate individuals and to verify their realworld identity—binding that identity to the public key and verifying that the individual has the private key. These trusted third parties are called **certification authorities** Wikimedia Foundation, Inc.(2008), Certificate Authority and the digitally signed files by which they certify the association of subjects with their public keys are called **digital certificates**. Because such PKC systems require considerable computer power, new types of key management did not prove commercially useful in the mass market until the 1990s, at which time the implementation of **PKI** became feasible.

2.5.1 Emergence Of Public Key Cryptography (PKC)

A public key infrastructure (PKI) is the management model that controls the keys in PKC—making digital signatures possible. The term PKI was first used the 1980s, when a team at Bell Northern Research in Canada (a predecessor of Nortel Secure Networks) was engaged in the use of PKC in packet data switching. A PKI employs PKC in an enterprise wide security infrastructure that is virtually transparent to the end user. The networked system of certification authorities, registration authorities (RAs), certificate management systems (CMSs), and directories:

- Stores digital certificates.
- Allows certificates to be moved securely within the infrastructure.
- Enables certificates to be revoked or updated.

2.5.2 Public Key Cryptography (Asymmetric Key Cryptography)

Public-key cryptography is a method for secret communication between two parties without requiring an initial exchange of secret keys. It can also be used to create digital signatures.

It is also known as **asymmetric cryptography** because the key used to encrypt a message differs from the key used to decrypt it

2.6 Application: Secure Electronic Transaction (SET)

2.6.1 Description

According to Wikimedia Foundation, Inc.(2008), Secure Electronic Transaction (SET) is a system for ensuring the security of financial transactions on the Internet. It was supported initially by Mastercard, Visa, Microsoft, Netscape, and others. With SET, a user is given an electronic wallet (digital certificate) and a transaction is conducted and verified using a combination of digital certificates and digital signatures among the purchaser, a merchant, and the purchaser's bank in a way that ensures privacy and confidentiality.

2.7 Certificate Authority

According to Wikimedia Foundation, Inc.(2008), Certificate Authority or certification authority (CA) is an entity which issues digital certificates for use by other parties. It is

an example of a trusted third party. CAs are characteristic of many public key infrastructure (PKI) schemes. There are many commercial CAs that charge for their services. There are also several providers issuing digital certificates to the public at no cost. Institutions and governments may have their own CAs.

2.8 The Digital Certificate (Public Key Certificate)

2.8.1 Description

According to Wikimedia Foundation, Inc.(2008), Public key certificate , The digital certificate is used to verify the connection between the public key and the owner of that key. (This kind of digital certificate is also called a public key certificate.) When the certification authority issues the digital certificate—digitally signed with that certification authority's private key—it authenticates that the public key belongs to that person.

2.8.2 Certificates And Web based application security

The most common use of certificates is for HTTPS-based web sites. A web browser validates that an SSL (Transport Layer Security) web server is authentic; so that the user can feel secure that their interaction with the web site has no eavesdroppers and that the web site is who it claims to be. This security is important for electronic commerce. In practice, a web site operator obtains a certificate by applying to a certificate provider with a certificate signing request. The certificate request is an electronic document that contains the web site name, contact email address, and company information

CHAPTER THREE

METHODOLOGY

3.1 Introduction

System Analysis is the phase in which the requirements of the new system are identified.

It is a process of gathering and interpreting facts, finding problems and using the information to either recommend change or develop a solution immediately.

The purpose of the study was to evaluate the current system. It involved describing the current system by the use of extensive diagrams and other descriptive model.

The study also evaluates the security offered by the current system and recommend new security measures to the new system

3.2 Procedure Of The Study

To perform the study, the researchers spent several weeks at the school of computer studies observing how exam result are processed and how the security measures are offered by the system. In addition, several interviews and questionnaire were organized with various users of the same system.

3.3 Population of The Area Of Study

The study extended coverage from the registration of new student, staff, course and course unit at the school of computer studies to managing the processing of the student's results, units taught by a particular staff and the display of student results and various reports.

3.4 Data collection methods.

The following methods applied in the collection of the data namely: Interview, questionnaire, Observation, document examination and analysis.

3.4.1 Primary Methods

Face-to-face interviews

This involved physical contact with direct questions posed to the people being interviewed. It was useful in obtaining first-hand information on the topic being investigated.

Questionnaires

This method involved written questions sent to the targeted group to acquire information that may not be obtained from the above research methods. Check sample of the questionnaire at appendix A

3.5 Analysis Of The Current System

3.5.1 Strengths of the current system

The current examination system/server is a standalone application and is able to provide the following functionalities

- Processing of examination results.
- Security even though at a lower level because anybody with access to the standalone server can manipulate the data stored.
- Updating of data stored.

3.5.2 Weaknesses Of The Current System

- A lot of paper work hence higher cost and errors.
- Waste of time as students move to various departments to view their results.

- Waste of time as staff members consults about the units assigned to them for a given course and handing over of results to administrator.
- Possibility of data loss if the standalone server fails or crashes.
- Inconsistency in data as it is moved from one department to another.

3.6 The Proposed System

The proposed system will run database management system (DBMS) to furnish a generic solution to the problems of persistent data storage, concurrent database access, data integrity, security, backups and the overall speed of operations. It will provide back up facility to facilitate recovery.

3.7 System Requirements

Here the requirements for the development of the system were analyzed and are defined consequently in the sub sections below.

3.7.1 Hardware Requirements

This phase determined the hardware that was required in developing the proposed system.

1. Personal Computer

A personal computer which will host the database must be available. Minimal specifications for this computer should be;

- 2.4 GHz Pentium processor or equivalent.
- Hard Disk with storage capacity of at least 40GB. The bigger the free disk space, faster the queries will be processed.
- Backup media – The system needs either a CD Writer or Tape drive for backup mechanism, to sustain data integrity and consistency in case of system failure.

- Memory – For faster transactions of queries, at least 256 MB of RAM is sufficient.

2. Printer

A printer for outputting information such as reports for managerial purposes is a mandatory requirement. A non-impact (Laser or ink-jet) printer is good because it is not noisy and it produces high quality print and it is relatively faster, compared to dot-matrix printer.

3.7.2 Software Requirements

1. Operating System

Linux based operating system since it has a lot of resources that can be used to secure data and provide a secured connection between the server and the hosts.

It also offers Stability, ease of use, ease of train and its GUI makes it competitive in comparison to other operating systems.

2. Apache server

This is compatible with all PHP versions and is also compatible with all types of browsers. The server provides services requested by the host

3. Developing Software

i) MYSQL

MySQL(My Structured Query Language) database management system (DMS) and the SQL database query language were to be used for defining and manipulating databases. MySQL command integer is usually used to create databases and tables in web database application and to test queries. All these statements was directly entered into the command interpreter and executed. The statement could also be included in server-side

PHP scripts. Hugh Williams and David Lane, (2002). SQL is a query language that interacts with a DBMS. SQL is a set of statements to manage databases, tables, and data. The data definition language (DDL) is a set of SQL statements used to manage a database. The MySQL command interpreter was to be used to create database and tables. A SQL statement was used to delete, alter, and drop database and tables, as well as managing indexes. The data manipulation language (DML) encompasses all SQL statements used for manipulating data. There are four statements, which form the DML statements set: SELECT, INSERT, DELETE AND UPDATE.

ii) *PHP*

According to Williams and Lane (2002), describe PHP as a scripting language that provides fast, customized access to DBMSs. PHP is an ideal tool for developing application logic in the middle tier of a three-tier application.

Scripts can manage the http authentication challenge directly. Scripts will be written to test the variable and send a response containing the WWW- authentication header to challenge the browser. When a request contains a username and password, the script can authenticate and authorize the request using any logic that is required. The user credentials set in the variable are then passed onto the function authenticated. This function uses the supplicated authentication scheme of checking that the password is the same as the username. It is critical to implement a secure scheme that stores passwords in a database.

HTTP (Hyper Text transfer protocol) is a stateless protocol that allows applications to distribute resources across more than one web servers. This allows an application to distribute requests across many web servers, thus dividing the load and permitting scaling

of the application. HTTP is a special server protocol, which encrypts confidential ordering data for customer protection.

HTML (hyper text mark up language) is a document-layout and hyper link-specification language. It defines the syntax and placement of special, embedded directions that are not displayed by the browser, but tell it how to display the contents of the document, including text, images, and other support media. The language was to also tells you know how to make a document interactive through special hypertext links, which connect your document with other documents on either your computer or someone else's, as well as with other internet resources, like (FTP) file transfer protocol. Developers rely upon the html standard to program the software that formats and displays common html documents.

3.7.3 Security Requirement

The system is aimed to achieve the highest security level of both data in transit (or during transmission) and stored in the database Other data items that need to be secured during transmission include password, etc. The password needs to be protected in the stored state to avoid people with access to the database from viewing it. The following security measures will be implemented to the system.

- The system will secure data on transmission using SSL (The server will have a public key certificate that will contain it's public key and identity of the company)
Passwords will be encrypted using MD5 hash function

- The system will notify the user when form data is being transmitted over http (unsecured protocol).
- Validation of data on both the client side and server side
- Disabling of http protocol (unsecured protocol) on the system to ensure that all data transmitted will be secure.

This will be done using commands on the server

- *sudo a2dissite default*

- And then *sudo /etc/init.d/apache2 reload*

Encryption during transmission will require the use of Public Key Certificate

3.8 Feasibility Study

3.8.1 Introduction

J. G. Gichuru (2003) defines feasibility study is a process that aims at analyzing the current system in terms of its social, technical and economical and operational compatibility. At this stage the current system in use by an organization is understood fully in order to establish the requirements of the new system. This was carried out in the following aspects:

3.8.2 Technical Feasibility.

Riga (2004) divides technical area into two sections: hardware, software and personnel to develop (or purchase), install and operate the system. To decide technical feasibility, the analyst simply determines if the preliminary design can be developed and implemented using existing technology.

In view of the study that was carried out, the project is technically feasible because the researchers were in a position to develop the system. In addition, the school is in a position to acquire the expected facilities to complete the project. This includes computers and other peripheral items.

3.8.3 Operational Feasibility.

Operational feasibility according to Riga (2004) is the determination that the system will be able to perform the designated functions within the existing organizational environment with its current personnel and existing procedures. The system will be used once it has been developed and implemented.

In view of this project, operational feasibility is 100% since all the staff and the top management wholly accept the new system to be developed.

3.8.4 Economic Feasibility.

This aimed at finding out whether the benefits of the proposed system would outweigh the cost of developing, running and maintaining the proposed system. The Implementation of the proposed system will bring the organization a lot of benefits and at

the same time will incur some cost. The cost benefit analysis carried out showed the benefits of the proposed system Outweighed the cost of the existing system.

3.9 Feasibility Report

- ✓ The organization could afford the hardware, software and technical resources and were easily affordable in the local market
- ✓ The benefits that would be accrued from the new system outweighed the cost of developing, running and maintaining it. The costs to be incurred include:
 - Equipment cost
 - Configuration and installation of hardware and software.
 - Personnel costs i.e. training users

This was summarized as below:

ITEM	QUANTITY	COST PER UNIT	TOTAL
Photocopying	500	50	25,000.00
Printing	300	50	15,000.00
Flash Disk (1 GB)	1	25000	25,000.00
CDs	5	500	2500.00
Training	1	50000	50,000.00
Miscellaneous	1	25000	25,000.00
TOTAL COST			142,500.00

Table 1.0: Research Budget

3.10 Recommendation

- Secured online result management system was necessary
- High skilled personnel required.

3.11 Benefits Of The Feasibility Study

- The study assisted the researchers with coming up with a tentative problem statement and objective.
- After successfully completing the feasibility study we had no doubts that all that we had gathered was enough to declare the new system worth developing.

3.12 Conclusion

After the feasibility study was conducted, it was concluded that a new system was feasible. This system would capture data efficiently, store data effectively and give out quality output as desired. It would also enable the institution to deal with securely and reliably deal with the exam results.

CHAPTER FOUR

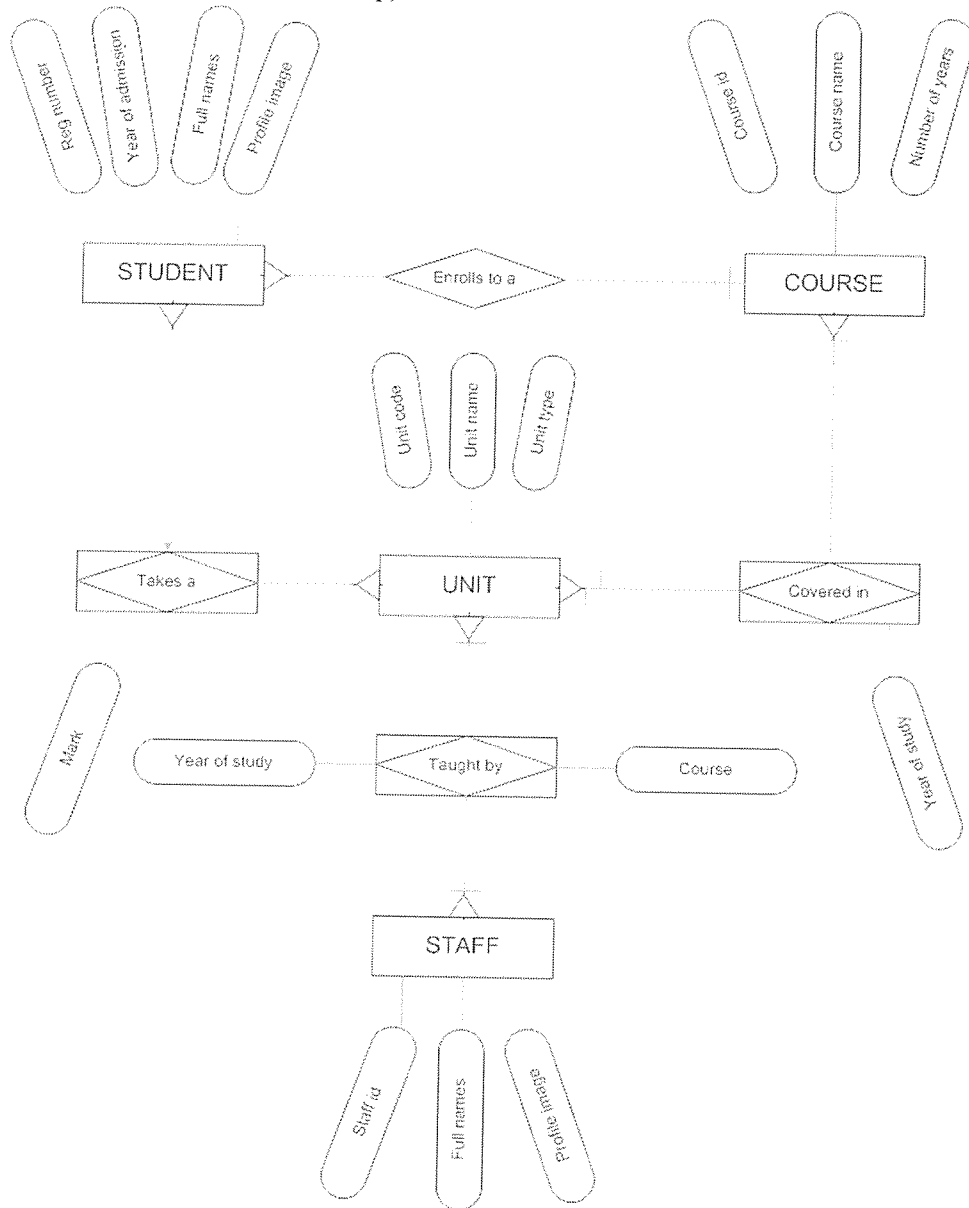
SYSTEM DESIGN

4.1 Introduction

Having clearly understood the problem, collected and analyzed data and hence identified the system requirements, the next important phase is system design. In this phase, all the key issues identified previously are carefully considered. This is very important because most of the errors originate from this area. More than 60% of the total time is spent at this stage.

Tools used in this phase include:

4.2 E-R (Entity Relationship) Model



KEY:

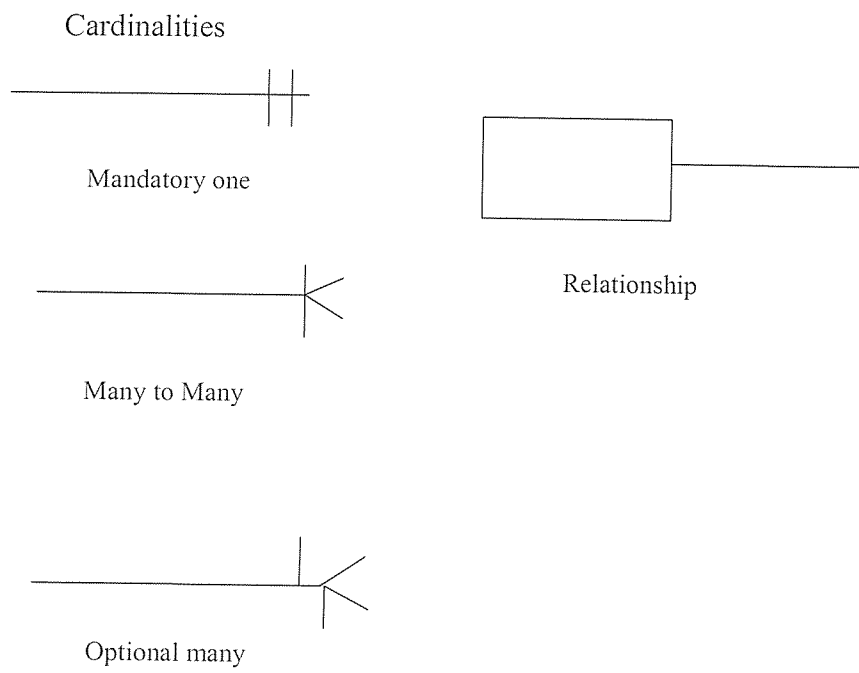


Figure 1.0: Conceptual Database (E-R) Model

It represents the relationships between entities or elements in the system. Also it reflect a static view of the relationship between different entities

4.3 DFD For The New System

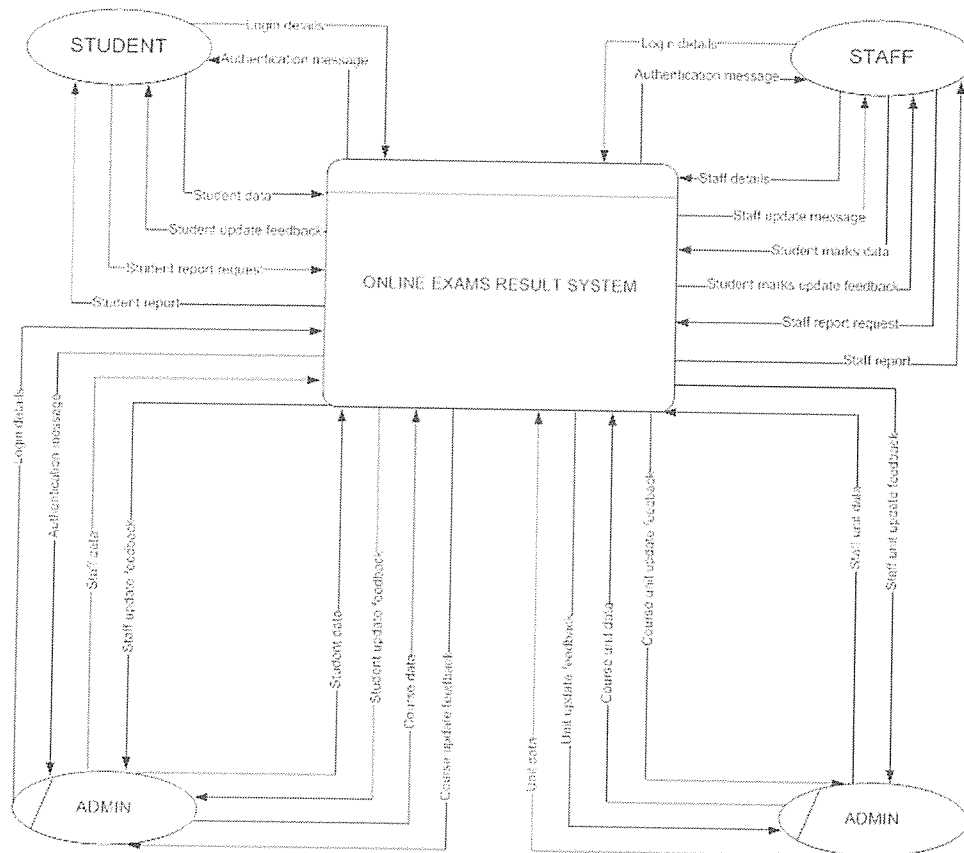


Figure 1.1: Data Flow Diagram - Context Diagram

4.4 Data Dictionary

The system data dictionary consists of four categories namely:

- Data Descriptions
- Data structures

- Data elements
- Data stores

4.5 Data Description

Name	Details
Login Details	Username and password from the student
Login details	Username and password of the staff
Login details	Username and password of the administrator
Authentication message	A message given on login (successful or invalid login)
Student data	Student profile information for update
Student Report Request	Examinations report request (includes year, semester)
Student Report	Includes the semester/year marks
Student Update feedback	Message on updating profile (failed or successful update)
Staff data	Includes the staff personal profile data (password, names, etc)
Staff Report request	Includes the class details for which the report is to be generated
Student marks data	Mark scored by a student in a certain unit
Staff update message	Includes a message on update (successful or failed update)
Staff Report	Includes the class list and the performance on a unit
Student marks update feedback	Includes a message on update (successful or failed update)
Course data	Details of a course which includes name, number of years, abbreviation, etc
Unit data	Unit name, type of unit (graded, pass/fail)
Student data	Student profile information for creation/update
Staff data	Staff profile information for creation/update
Course unit data	Assigning a unit to a course in a certain year and semester
Staff unit data	Assigning a certain staff to a certain class (course and academic year)
Course update feedback	Includes a message on update (successful or failed update)
Unit update feedback	Includes a message on update (successful or failed update)
Student update feedback	Includes a message on update (successful or failed update)
Staff update feedback	Includes a message on update (successful or failed update)
Course unit update feedback	Includes a message on update (successful or failed update)
Staff unit update feedback	Includes a message on update (successful or failed update)
Student Report Request	Includes data like student number
Staff Report Request	Includes the course, unit and the academic year
Student report data	The student details and exams result for a given year
Staff report data	The class results data (a given course and year)

Student data request	Includes the student number for retrieving the student data
Student data	Student personal data
Staff unit data request	Includes the staff number, unit number and the class (course and year)
Staff unit data	Includes the staff unit data
Staff data Request	Includes the staff number
Staff data	Includes the student data
Course data	Course name, abbreviation, years
Course data request	Course id
Unit data request	Unit code
Unit data	Unit name, code and type

Table 1.1: Data Descriptions

4.6 Data Structures

The following is the description of the data structures that are used in the above data flows:

Login data = username + password

Student details = Student registration number + Student name + Student profile image + Admission year + Course

Student name = first name + middle name + last name

Staff details = Staff number + Staff name + Staff profile image

Staff name = surname + middle name + last name

Course details = Course name + Abbreviation + Number of levels + Course id

Unit details = Unit code + Unit name + Type of unit

Type of unit = [graded | not graded]

Student report data = Student details + Academic year

Staff report data = Staff number + Course id + Unit code + Year of study

Student report = Student name + {unit marks} + Year of Study + Level

Staff report = Course name + Unit name + Year of Study + {student unit marks}

Student mark = Student registration number + Unit code + Year of Study + Level + Mark

Course unit details = Course id + Unit code + Level

Staff unit details = Staff number + Course id + Unit code + Year of Study

User details = Username + Password + User level + Last login

4.7 Data Elements

Name	Details	Description	Type
Username	Login name, User name	A string of characters	Base
Password	Secret key	A string of characters	Base
Reg_no	Student registration number	Characters e.g. BCS/14564/71/DF	Base
Student profile image	profile picture	An image of the student	Base
Fname	Student first name	First name	Base
Middle_name	Student middle name	middle name	Base
L_name	Surname	surname	Base
Staff id	Staff number	A unique address for each staff	Base
Staff profile image	profile picture	Representative image of the staff	Base
C_name	The course the student is registered	course the student is offering e.g. Computer Science	Base
Abbreviation	Course abbreviation	characters representing the course name e.g. BCS	Base
Years of Study	Academic year	Characters in the format 2008/2009	Base
Course_id	e.g 1 for computer science, 2 for information technology	A number auto generated by the system	Base
Unit_code	Code assigned to that unit	code that uniquely identifies a unit	Base
Unit_name	Name of that particular unit	Name of the unit e.g. System Analysis And Design	Base
Type of unit	Graded(A B+,C,...) not graded (Pass or Fail)	Number representing graded or not graded	Base
Academic year	Year of registration or	Characters in the format	Base

	entry	2008/2009	
Year of study	Current year of Study	Characters in the format 2009/2010	Base
Unit mark	Student mark, mark	Number representing the student score in a subject (Mark ranges from 0 to 100)	Base
Level	Year in which the student is	A number the year of study expressed an integer e.g. 1 for first year, 2 for second year, etc	Base
User level	Identifies the user as a student or staff	A number that represents the user level of operation (staff, and student)	Base
Last login	Shows the last time the user was logged onto the system	Represents the last time the user was logged onto the system	Base

Table 1.2: Data Elements

4.8 Data Stores

Table Name	Details	Data structure
Student File	Contains the student personal details	Student details
Staff File	Contains the staff personal details	Staff details
Course File	Contains the course details	Course details
Unit File	Contains the details of a particular unit	Unit details
Course Unit File	Contains the listing of the units in a course at various levels or years	Course unit details
Staff Unit File	This file contains all the units assigned to various lecturers	Staff unit details
User File	This is the file that contains the authorized users of the system with their level of operations and passwords	User data

Table 1.3: Data stores

4.9 Relational Model

COURSE (Course_id, name, abbreviation, no_of_years)

UNIT (Unit_code, name, type)

STUDENT (Reg_num, surname, first_name, middle_name, image, year_of_admission, Course_id)

STAFF (Staff_id, surname, other_names, image)

COURSE_UNIT (Course_id, Unit_code, level_of_study)

STAFF_UNIT (Staff_id, Course_id, Unit_code, Year_of_study)

RESULT (Reg_num, Unit_code, Year_of_study, Mark)

USER (Username, Password, User_level, User_id, Last_login)

NB: The above relations are normalized.

4.10 Physical Model

COURSE RELATION

ATTRIBUTE	DATA TYPE	DESCRPTION
Course_id	int(5)	To store course id, auto generated by the system (primary key)
Name	Varchar(50)	Name of the course
Abbreviation	Varchar(10)	Course abbreviation
No_of_years	Int(1)	Number of years a course takes e.g. 3 years for Computer Science

Table 1.4: Course relation

UNIT RELATION

ATTRIBUTE	DATA TYPE	DESCRPTION
Unit_code	Varchar(10)	Primary key and stores the unit code e.g. CS2206
Name	Varchar(50)	Name of the unit
Type	Int(1)	Whether graded or not graded

Table 1.5: Unit relation

STUDENT RELATION

ATTRIBUTE	DATA TYPE	DESCRIPTION
Reg_num	Varchar(20)	Primary key and stores the student registration number
Surname	Varchar(30)	The student surname
First_name	Varchar(30)	The student first name
Middle_name	Varchar(30)	The student middle name
Image	Varchar(20)	The url to the student profile picture
Course_id	Int(5)	Foreign key to the course relation. It indicates the course the student is enrolled to.

Table 1.6: Student relation

STAFF RELATION

ATTRIBUTE	DATA TYPE	DESCRIPTION
Staff_id	Int(11)	Primary key and contains a unique auto generated staff id that identifies a staff
Surname	Varchar(30)	Staff surname
Other_names	Varchar(50)	The staff other names; may include an initial and one name or two names
Image	Varchar(11)	This contains the url of the profile image of the staff

Table 1.7: Staff relation

COURSE UNIT RELATION

ATTRIBUTE	DATA TYPE	DESCRIPTION
Course_id	Int(11)	Part of the composite foreign key and indicates the course
Unit_code	Varchar(10)	This identifies the unit and its part of the composite primary key
Level_of_study	Int(1)	This is a number that indicates the level of the

		course at which the unit is covered e.g. 1 for first year, 2 for second year, etc
--	--	---

Table 1.8: Course unit relation

STAFF UNIT RELATION

ATTRIBUTE	DATA TYPE	DESCRIPTION
Staff_id	Int(11)	Part of composite primary key and foreign key to the staff relation
Course_id	int(5)	Part of composite primary key and a foreign key to the course relation
Unit_code	Varchar(10)	Part of composite primary key and a foreign key to the unit relation
Year_of_study	Varchar(10)	This represents the academic year when the specified staff was teaching the specified unit

Table 1.9: Staff unit relation

RESULT RELATION

ATTRIBUTE	DATA TYPE	DESCRIPTION
Staff_id	Int(11)	Part of composite primary key and foreign key to the staff relation
Course_id	int(5)	Part of composite primary key and a foreign key to the course relation
Unit_code	Varchar(10)	Part of composite primary key and a foreign key to the unit relation
Year_of_study	Varchar(10)	This represents the academic year when the specified staff was teaching the specified unit

Table 1.10: Result relation

USER RELATION

ATTRIBUTE	DATA TYPE	DESCRIPTION
Username	Varchar (30)	Unique user name that identifies a user of the system
Password	Varchar(50)	The user password
User_level	Int(1)	The user level; admin, student, or staff.
User_id	Varchar(20)	Foreign key to the student or staff relation in the database

Table 1.11: User relation

4.11 Database Design

Exam results management of the proposed system will implement database as its core

Driving force. All files will be managed in a single database. This will eliminate

Inconsistency as Well as redundancy control. Tables will form the basic database

Structure. The following files will be found in the database.

- Student file
- Course file
- Unit file
- Staff file
- User file
- Staff unit file
- Course unit file

4.12 Interface Design

This involves designing of objects that would create interface between the user and the system. An interface provides the link between the user, program codes and the data files

4.13 Website Sitemap

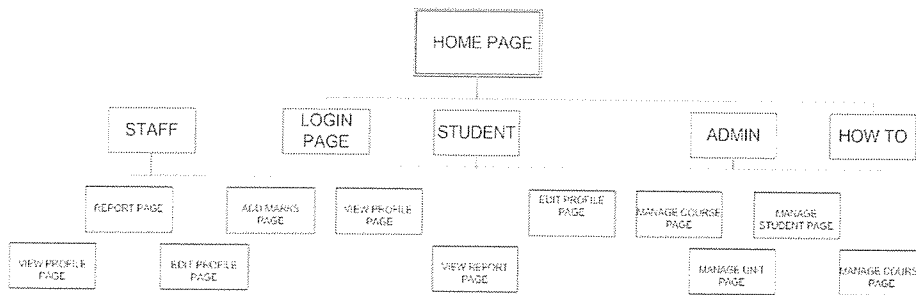


Figure1.2: Website sitemap

4.14 Conclusion

System design and development were very interesting phases. Design included identifying entities, attributes and their relationships. This included liaising with the direct users of the system. This was intended to reduce potential problems in future as possible.

Once the design phase was complete, a further confirmation from direct and indirect users of the system was done until they were satisfied that all the intended purpose was to considered. This phase was complete by converting the design into a working application.

- View his/her graphical results

Once the staff has received his/her login details, he/she can log in to the system. They can change their login password if they wish. If a staff logs in, he/she can:

- Change his/her profile information and upload a picture
- Add/edit student marks for the units he/she is teaching
- View the class performance list
- View graphical reports of the class performance

5.2 Main System Components

The system has 5 major components:

- User registration
- User Authentication
- Changing profile
- Recording examination marks / results
- Viewing reports

5.2.1 User Registration

This step involves the 3 steps highlighted in section 5.1, user verification, accounts creation, account activation. If a user provides the correct details provided at the registration time, the system allows him/her to create an account by choosing a unique username and a password. The following two screen captures show student registration process.

Student Registration : Step 1

Please provide the following information:

Registration number:

Surname:

Year of Admission:

National ID/Passport No :

Submit

Figure 1.3: student registration details

SECURE EXAM RESULTS SYSTEM

Secure
Reliable

HOMESTUDENTSTAFFHELPLOG IN

Student Registration : Step 2

Your details verified in stage 1.

Please provide the following information to complete your registration.

Registration failed. Try another username or the student already registered.

Surname:#####

Reg No: DCS14584/T1/OF

Password:***

Confirm Password:***

Register

Are you a Student?

Students need to register on the system to enjoy the following services:

- Create and update your profile
- View your academic results
- View graphical results

Register

Are you a Staff?

You can enjoy the following secure services on this interactive examination online portal:

- Create and update your profile
- Add/edit student marks

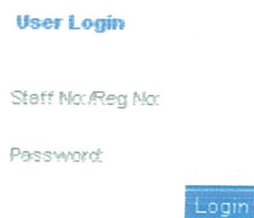
Figure 1.4: User verification

The final stage is account activation, which is done automatically on validation of the account details provided.

5.2.2 User Authentication

Every user visiting the system with no prior authentication or whose session had previously expired has to present his/her credentials (username and password) in the Login form.

The user is presented with a Login form that prompts for the two credentials i.e. the password and the username.



A screenshot of a web form titled "User Login". It contains two input fields: "Staff No./Reg No:" and "Password:". Below the password field is a blue "Login" button.

Figure1.5 User authentication

5.2.3 Changing Profile

The system allows the users to modify their profiles. User profile is a collection of user full names, short description about themselves for other viewers, username and password, and the profile picture.

SECURE EXAM RESULTS SYSTEM

Secure
Reliable

HOME STUDENT STAFF HELP LOG OUT STFO01

Home Profile Page Profile Page Profile Section Report

Njoroge Kimani Edit Profile »

Staff No.: STFO01
Email address: kimani@stfooc.com

About Me

Mr. Njoroge Kimani

Njoroge Kimani
Staff no: STFO01
Logout

Copyright 2010 Developed by Kimani

(a)

HOME STUDENT STAFF HELP LOG OUT STFO01

Home Profile Page Profile Page Profile Section Report

Edit's Profile Edit Profile »

Personal Data

Email address: kimani@stfooc.com
Res password: *****
Confirm password: *****

About Me

First Name: [text input]
Last Name: [text input]
Address: [text input]
City: [text input]
Country: [text input]
Phone: [text input]
Email: [text input]
Website: [text input]
Bio: [text input]

Profile Picture

[text input] Browse...

Njoroge Kimani
Staff no: STFO01
Logout

(b)

Figure 1.6: User profile

5.2.4 Recording Examination Marks

Members of staff registered onto the system can view all the classes assigned to them in a particular academic year. The screen capture below shows the classes assigned to Mr. Kimani Njoroge in the year 2007/2008

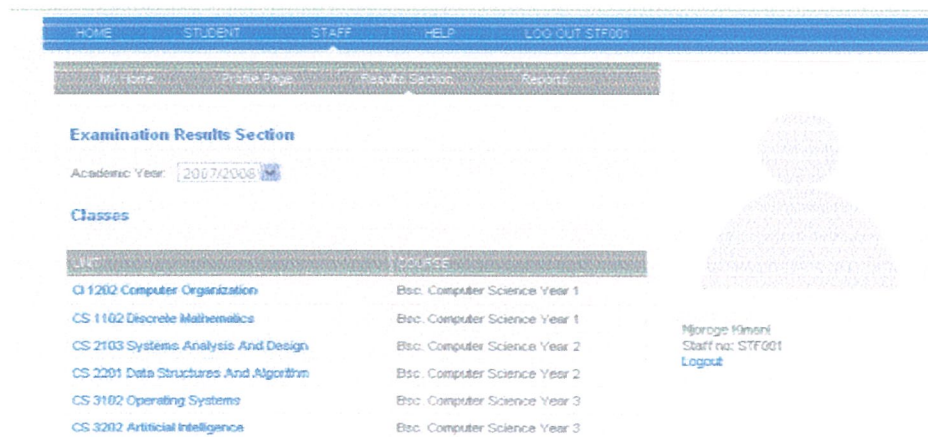


Figure1.7 Staff units

On selecting a particular class, the class list appears as shown in the following screen capture.

[HOME](#)
[STUDENT](#)
[STAFF](#)
[HELP](#)
[LOG OUT STF001](#)

[My Home](#)
[Profile Page](#)
[Result Section](#)
[Feedback](#)

Examination Results Section

[← Back to Listing](#)

Class: **CI 1202 Computer Organization**

Academic Year: **2007/2008**

Courses: **Bsc. Computer Science**

Year of study: **1**

Class Marks

REG NO.	STUDENT NAME	MARKS
BCS/14564/71.DF	KIMANI WILSON	70
BCS/14565/71.DF	YUSSUF ABDULLAH	57

[Save](#)

Njoroge Kimani
Staff no: STF001
[Logout](#)

Figure1.8 Class list

5.2.5 Reports

This module deals with the generation of student and staff reports both textual and graphical reports.

Example of a report is a class report generated by the staff. This is shown in the screen capture below.

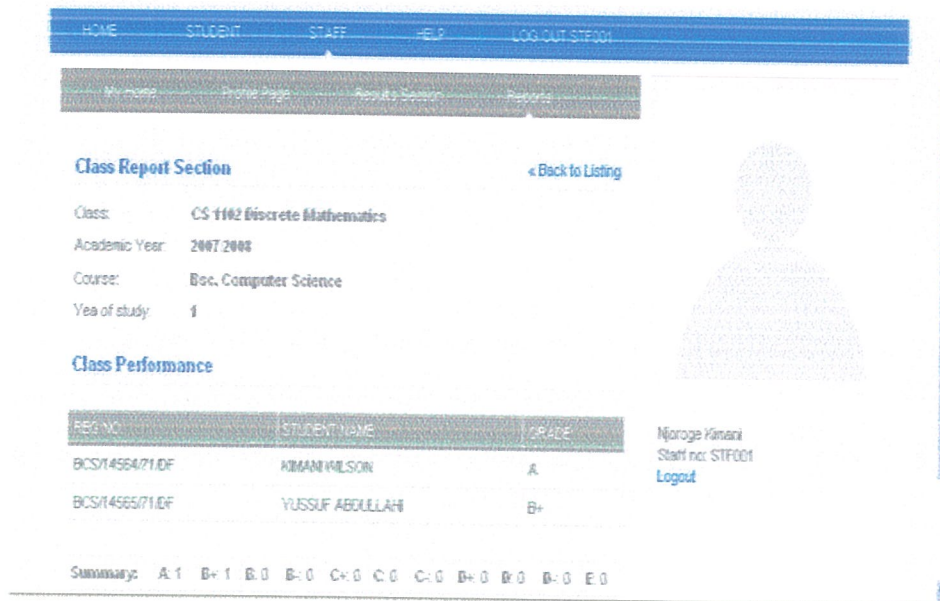


Figure1.9 Class report

The system also generates graphical reports. This is shown in the screen capture below.



Figure1.10 Graphical report

5.3 Security Implementation

The system is aimed to achieve the highest security level of both data in transit (or during transmission) and stored in the database. The student marks keyed in by the staff or the administrator need to be secured during transmission. Other data items that need to be secured during transmission include password, etc. The password needs to be protected in the stored state to avoid people with access to the database from viewing it. The following security measures have been implemented to the system.

- The system secures data on transmission using SSL (The server has a public key certificate that contains it's public key and identity of the company)
- Passwords are encrypted using MD5 hash function
- The system notifies the user when form data is being transmitted over http (unsecured protocol).
- Validation of data on both the client side and server side
- Disabling of http protocol (unsecured protocol) on the system to ensure that all data transmitted is secure.

This is done using commands on the server

- *sudo a2dissite default*

- And then *sudo /etc/init.d/apache2 reload*

Encryption during transmission requires the use of Public Key Certificate

5.4 System Implementation Summary

The front end is accessed by visiting <http://localhost/examportal> while the administration section accessed by visiting <http://localhost/examportal/admin>.

The system can run on any Apache Server installation with MySQL database support.

The GD2 module/extension for apache must be loaded to facilitate the dynamic resizing of profile pictures.

5.5 Conclusion

When the system is implemented it must be maintained whereby files are updated and unnecessary information is deleted. It should show the workings of the new system and how the user should navigate through the system from login to the generation of reports.

CHAPTER SIX

RECOMMENDATIONS AND CONCLUSIONS

6.1 Introduction

Finally after hardwork of designing, developing and implementing the application, the last bit is to monitor performance of the system as well as recommend on the changes that can be done in the near future as well as pointing out areas of further research.

6.2 Recommendation

The researchers recommend that the administration take full advantage of this information system to computerize other departments. This will make the operations concerning the exam results faster, cost effective, secure and more reliable.

6.3 Conclusion

One major achievement was identification of the major security threats to network applications. These threats are both threats to encryption algorithms like RSA and MD5, and security threats which are application dependent like use of http in place of https.

Public Key Certificate was used as the major tool of ensuring security. This research enabled us to have a clear understanding of how public key cryptography works, the encryption and digital signing. The researchers were in a position to generate a self-signed Public Key Certificate, installed it to be used by Apache, and configured the Apache SSL Virtual Host.

The researchers developed a secure examination results system that counters major security threats identified.

The researchers conclude therefore that the paper-based or computer-based system in place is not adequate and the use of this secure exam result management system is more

efficient, reliable, secure and satisfactory. It improves processing of exam result as well as providing an easier access to all services.

Courses, course units and staff will also be effectively managed because the secure result system provides an easier and a faster way of dealing with the listed functions.

Though the Information system will not provide 100% satisfaction, however much it may be customized; it guarantees significant user satisfaction and boost up efficiency, security and reliability.

Security- The secured result management system provides the following as a way of enhancing security

- Authentication - each user of the system will be authenticated. You need to login before carrying out any activity on the system
- Authorization – a user will be required to carry out only the authorized tasks on the system e.g. a student although authenticated, will not modify any marks in the examination results system.
- Data security- the data or information will be protected in stored state and during transmission
- Accountability – the system will provide a log of all the users who have accessed the system, the time of access, the machine used, etc.

Back up

The system will have easy means of backing up data. This is to foster system reliability by enabling recovery of data in case of any disaster.

Interoperability

The system will be able to work with other existing systems. The data that may be needed by other systems in the institution will be readily availed by the system in the right format

Response time

The system will do the tasks requested by the users in the minimum time possible and will provide feedback to show what is happening on the background.

Concurrency Control

The system will handle concurrent access and issues surrounding concurrency.

6.4 Future Work

Network security is a wide field and a lot has to be done. Future activities in this research area would be coming up with a stable Cryptographic Hash Function, which is currently ongoing from 2008 – 2012. Another important issue to research on is the RSA algorithm. Development of quantum computers is seen as a major threat to Public Key Cryptosystems like RSA. One can research on how to improve the algorithms to overcome the threat.

About the application developed, more work can be done on it to make a reality. The system developed was used as a demo on how security can be implemented and never captured all the requirements. A thorough fact finding process can be carried out to ensure that all the requirements are captured and a complete system implemented

APPENDIX A:
SAMPLE QUESTIONNAIRE

Name: _____

Position: _____

Date: _____

We, Kimani Wilson Mburu (BCS/14564/71/DF) and Fatuma Ng'aari (BCS/14558/71/DF) - Third year Computer Science students, as part of our three years course, we are undertaking a project in Network Security (Public Key Infrastructure).

We kindly request you to help us with the necessary information / data by filling this questionnaire.

Any information offered will be highly appreciated and confidentially kept.

Thanks.

Kimani Wilson Mburu.

BCS/14564/71/DF

And

Fatuma Ng'aari

BCS/14558/71/DF

REFERENCES

Krastins J., Strautmanis I. Riga. The Complete Guide to Architecture. - 2004, *Riga: ADD Projects*

Connolly.M (1996), Database Systems. Addison-Wesley publishers Ltd

Diezel. K et al (1999), Macromedia Dream weaver 3 using Dream weaver (1st ed). san Francisco: Macromedia Inc.

Elmasri. R (2000), Fundamentals of database systems, (3rd ed).Singapore: Addison Wesley Longman publisher

Gupta.G (1996),Management Information Systems .New york: West Publishing Company

Kenneth.C (2002) Management Information Systems (6th edition). New Jersey: Penticc-hall.

C.Kauffman, R.Perlman, M.Spenser(2002), *Network Security (Second Edition)*
[Electronic version],
Englewood Cliffs, Prentice Hall

John Leyden (2007, September), *Quantum computing spectre looms over ecommerce, Factor 15 protection*, Retrieved on Januray 2, 2010, from
http://findarticles.com/p/articles/mi_m1200/is_/ai_17935112

John Viega, Matt Messier & Pravir Chandra (2003), Cryptography for Secure Communications, *Network Security with OpenSSL*, 1-30

Kristen Noakes-Fry (2001), *Public Key Infrastructure (PKI): Overview* Gartner Research, 3-20

Paul C. Kocher (1995), *Timing Attacks on Implementations of Diffe-Hellman, RSA, DSS, and Other Systems*, San Francisco, CA 94105, USA , Cryptography Research, Inc., 1-2

Wikimedia Foundation, Inc.(2008), *Secure Shell*, Retrieved January 22, 2010, from http://en.wikipedia.org/wiki/Secure_Shell

WikiMedia Foundation, Inc.(2008), *Cryptographic hash function*, Retrieved January 2, 2010, from http://en.wikipedia.org/wiki/Cryptographic_hash_function

Wikimedia Foundation, Inc.(2008), *Certificate Authority*, Retrieved January 2, 2010, from <http://en.wikipedia.org/wiki/CA>

Wikimedia Foundation, Inc.(2008), *Digital signature*, Retrieved January 2, 2010, from http://en.wikipedia.org/wiki/Digital_signature

Wikimedia Foundation, Inc.(2008), *Digital signature*, Retrieved January 2, 2010, from http://en.wikipedia.org/wiki/Digital_signature

Wikimedia Foundation, Inc.(2008), *Secure Electronic Transaction (SET)* , Retrieved January 2, 2010, from http://en.wikipedia.org/wiki/Secure_electronic_transaction