ENCRYPTION OF BIOMETRIC FINGERPRINT TEMPLATES USING ENCRYPTION KEYS OBTAINED FROM OTHER BIOMETRIC FINGERPRINT TEMPLATES

JOSEPH MUITHI MWEMA

MASTER OF SCIENCE

(Computer Systems)

JOMO KENYATTA UNIVERSITY OF AGRICULTURE AND TECHNOLOGY

2015

Encryption of Biometric Fingerprint Templates using Encryption Keys obtained from other Biometric Fingerprint Templates

Joseph Muithi Mwema

A thesis submitted in partial fulfillment for the degree of Master of Science in Computer Systems in the Jomo Kenyatta University of Agriculture & Technology

2015

DECLARATION

This thesis is my original work and has not been presented for a degree in any other University.

Signature: …… Date: ……..

Joseph Muithi Mwema

This thesis has been submitted for examination with our approval as the University supervisors:

Signature: …… Date: ……..

Dr. Stephen Kimani

JKUAT, Kenya

Signature: …… Date: ……..

Dr. Michael Kimwele

JKUAT, Kenya

DEDICATION

First and foremost, I thank God, the almighty for granting me good health and strength to proceed prosperously. I dedicate this work to my parents, sisters and friends whose support and encouragement ensured that this project was a success.

ACKNOWLEDGEMENTS

I would like to show my gratitude to all who supported me in various diverse ways. First, my sincere thanks go to my research supervisors Dr. Stephen Kimani and Dr. Michael Kimwele for their guidance, advice and the time they spared to offer me their extraordinary support throughout this research work. Special thanks go to my parents and sisters for their encouragement and motivation when I was enrolling for postgraduate studies and particularly my sister Victoria Mwema who offered to proof read this work for me. Lastly, I would like to pay my regards to Sam and Anthony my fellow course mates for their friendship and keeping tabs on me all along to make sure I kept working towards finishing this research work. Hats off to you comrades.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF APPENDICES

ACRONYMS AND ABBREVIATIONS

AES	Advanced Standard Encryption
CRUD	Create, Read, Update and Delete
ECC	Elliptical Curve Cryptography
GUI	Graphical User Interface
IDE	Integrated Development Environment
IEC	International Electrotechnical Commission
ISO	International Organization for Standardization
MD5	Message-Digest 5 Algorithm
PIN	Password Identification Number
RSA	Rivest, Shamir and Adleman
SDK	Software Development Kit
SHA	Secure Hash Algorithm
SPSS	Statistical Package for Social Sciences
SQL	Structured Query Language
USB	Universal Serial Bus

ABSTRACT

The need for fool proof authentication procedures away from traditional authentication mechanisms like passwords, security PINS has led to the advent of biometric authentication in information systems. Biometric data extracted from physiological features of a person including but not limited to fingerprints, palm prints, face or retina for purpose of verification & identification is saved as biometric templates. The inception of biometrics in access control systems has not been without its own hitches & like other systems it has had its fair share of security challenges. Biometric fingerprints are the most mature of all biometric spheres. Biometric systems are further subdivided into multimodal biometric systems and unimodal biometric systems. Effectiveness of biometric systems lies on how secure they are at averting inadvertent disclosure of biometric templates in an information system's archive. This however has not been the case as biometric templates have been fraudulently accessed to gain unauthorized access to information systems. In order to achieve strong and secure biometric systems, systems designers and developers need to build biometric systems that properly secure biometric templates. Several approaches and biometric template protection schemes have been used to safeguard stored biometric templates. Even though there are various biometric template protection schemes and approaches in existence, few of them have been concretely tailored for unimodal biometric systems. This research's intent was to establish an approach for securing biometric fingerprint templates in a relational database. To come up with this approach, precedent biometric template protection schemes and approaches were studied to determine their shortcomings after which an encryption scheme for securing biometric templates stored in a database by encrypting fingerprint templates with encryption keys derived from other fingerprints was designed, developed and tested to ascertain its efficacy. Evaluation of the results showed that a combination of security measures and not just one particular technique aids in optimizing security of archived biometric fingerprint templates.

CHAPTER ONE

INTRODUCTION

1.1 Background Information

The advent of increased security threats in information systems and need to guarantee unbeatable systems security enticed system designers and developers to incorporate use of passwords, PINs and access codes for system users' authorization. On the contrary, these security measures did not provide optimal security as is required of a secure system vault and have been known to be prone to hacks or easy to illegally obtain as is emphasized in (Das, 2011). To stem these challenges, system designers and developers began integrating use of biometrics in design of systems' verification and identification procedures. Tan (2013) considered use of biometric authentication schemes to be more efficient over traditional password based access control methods. Statistics however show that biometric systems have not been known to be impervious to hacks and that there are several known possible attacks on biometric systems which have rendered use of biometrics insufficient in providing water tight security as is evidenced by Rathgeb and Busch (2012).

Biometrics is simply the automatic identification of a person's physiological or behavioral patterns or traits. Biometric patterns captured from a person are saved as biometric templates. Biometric fingerprint templates are physiological patterns extracted by a feature extractor in a biometric fingerprint sensor and saved in a biometric system's database, smartcard or archived in a system folder for purpose of future use in verification or identification of a person. A biometric system can be categorized as either a verification or identification system. El-Sisi (2011) defined a verification system as one which conducts one to one comparison of biometric templates to confirm if identity claimed by an individual is true and defined an identification system as one that searches an entire database for a biometric template match. In the process of verification or identification, a user's fingerprints are extracted for purpose of matching them with previously captured biometric fingerprint templates.

Logistics of safeguarding and preventing captured biometric fingerprint templates from spoofing has proved to be a hard nut to crack for system administrators. Biometric templates stored in a database in their raw format can be illegally retrieved and replayed to the biometric system's matcher by system hackers to grant unauthorized access to a biometric system especially for instances where adversaries disguise themselves as the genuine bearers of the presented biometric traits. Several approaches aimed at protecting archived biometric templates have been proposed and studied. Ahmad et al., (2012) particularized that 'security of biometric data in a biometric system' as one of the key technical issues and challenges regarding use of biometric systems. Schemes used to protect biometric feature sets and biometric templates in biometric systems were reviewed then an encryption technique for encrypting biometric fingerprint templates with encryption keys derived from other fingerprint templates in a unimodal biometric fingerprint system was designed and developed. A unimodal biometric system is a system which is built to authenticate biometric physiological traits from only one part of a human's body (Das, 2012) and in this study, this research proposed a new technique for securing biometric templates in a fingerprint only biometric system.

1.2 Statement of the Problem

Biometric systems save physical traits extracted from the face, iris, voice and fingerprints as biometric templates. During authentication of system users, existing biometric templates are compared by the biometric system's matcher against the presented biometric features. In order to realize optimal and secure use of biometrics as access control features, there is need to guarantee safety of biometric templates stored in authentication systems. Biometric fingerprints of an individual do not vary or change over time (Balakumar & Venkatesan, 2011) which is the permanence characteristic of fingerprints. Passwords, PINS and access codes can be replaced with new ones if they get compromised unlike the case of biometric fingerprint templates which have permanent physical features. It is this distinctive nature of biometrics that can also be exploited to render use of biometrics insecure when biometric templates in a biometric system are illegitimately retrieved from the biometric system database and

replayed to the biometric system's matcher by adversaries to gain unauthorized access to information systems.

The fact that biometrics of a person cannot be changed or replaced like passwords and pins when leaked, brings about the need to securely protect stored biometric templates to prevent counterfeit biometric templates being used to circumvent a biometric matcher (Arjunwadkar et al., 2012). Several approaches of securing biometric templates have been proposed and researched on but most of them seek to address security of biometric templates in multimodal systems which are expensive and a preserve of affluent regimes and security agencies. Unimodal biometric systems on the other hand like 'biometric fingerprints only systems' are frugal and easy to implement but without a distinctively secure way of securing the safety of their biometric fingerprint templates in databases. This research sought to establish an approach for securing biometric templates in unimodal biometric fingerprint systems' databases by proposing to encrypt biometric fingerprint templates with encryption keys generated from other biometric fingerprints using a two-step fingerprint enrolment and authentication process.

1.3 Justification of the Study

Biometric systems require secure and reliable protection of biometric templates. Use of poorly protected or unprotected biometric templates creates loopholes for an attacker to compromise a biometric authentication system and recover original biometric data (Imamverdiyev et al., 2013). Although various biometric template protection schemes and approaches exist including encryption of templates with information prevalent to an individual e.g. year of birth, ID number or security codes as seen in (Kaur et al, 2010) which can be easily guessed and estimated by attackers, there is need for a biometric fingerprint template protection approach that provides security of archived biometric templates in unimodal biometric fingerprint systems. The existing template protection schemes are not fool proof and do not guarantee water tight security as is evidenced by Jadhav (2014). This research sought to establish a robust approach aimed at securing biometric fingerprint templates in the frugal and easy to implement unimodal biometric fingerprint systems because the schemes in

existing literature are more emphatic on addressing biometric template protection in multimodal biometric systems which unlike unimodal biometric systems are very complex, expensive and only affordable to large corporations and are a preserve for rich governments (Das, 2012).

The research sought to establish a more effective technique for securing biometric templates in unimodal biometric fingerprint systems by encrypting them with encryption keys generated from other biometric fingerprint templates before storing them in a database. In a recent research study, researchers pressed that cryptographic template protection renders more secure image protection (Maniroja & Sawarkar, 2013). This study culminated to a more effective technique for securing biometric fingerprint templates that guaranteed safety of not only biometric fingerprint templates in unimodal biometric fingerprint systems but also provided a replicable approach for securing biometric templates in a non-retrievable manner to hackers in other biometric systems.

1.4 Objectives

1.4.1 Broad Objective

To develop a more secure and effective technique for securing biometric fingerprint templates archived in a database based on encryption keys obtained from other biometric fingerprint templates.

1.4.2 Specific Objectives

1. To determine and examine the biometric template protection schemes used to secure biometric templates.
2. Identify the shortcomings of the biometric templates protection schemes and approaches currently in existence.
3. To design and develop a two-step encryption and decryption technique that optimizes ideal features of a biometric template protection scheme.
4. To evaluate the quality of the developed biometric fingerprint encryption and decryption technique.

1.5 Research Questions

The research seeks to address the following questions:

1. What are the existing biometric templates protection schemes and approaches used to secure biometric fingerprint templates?
2. What are the shortcomings of the current biometric fingerprint templates protection schemes and approaches?
3. What are the features of an ideal biometric fingerprint template protection technique?
4. How will the quality of the developed biometric fingerprint encryption and decryption tool be assessed to determine if it meets the required specifications of an ideal biometric fingerprint template protection scheme?

1.6 Scope of study

This study's focus was on security of biometric fingerprint templates in unimodal biometric fingerprint systems. A survey is additionally conducted to explore existing biometric template protection schemes and approaches used by biometric software developers in securing biometric fingerprint templates and determine their shortcomings, as well as find out biometric template security challenges experienced. This information is significant in ascertaining and augmenting validity of existing theoretical literature that this study is predicated on.

1.7 Assumptions and Limitations

Respondents were apprehensive of divulging security practices they had in place to safeguard against attacks on biometric systems they developed. Company policies and non-disclosure agreements signed by respondents prevented them from answering all questions fielded in questionnaires.

Fingerprint images used in this study were captured using only one type of a fingerprint reader and were not representative of other biometric fingerprint readers that exist.

1.8 Definition of Terms

Authentication This is verification or identification of users fingerprints.

Enrolment This is the capturing of a fingerprint image and extracting minutiae for the purpose of archiving, verification or identification of users.

Identification This is comparing a fingerprint against a database of enrolled fingerprints and confirming that the fingerprint is enrolled. It is also the 1: N matching of fingerprints.

Minutiae These are the quantifiable biometric fingerprint features from which comparisons of one print with another can be made.

Verification This is comparing a fingerprint against a specific user's enrolled fingerprint to ascertain a specific person's identity. It is also the 1:1 matching of fingerprints.

1.9 Thesis Organization

In chapter two, the biometric template protection schemes in existing literature are discussed. Their strengths and drawbacks are determined while the types of biometric systems' attacks are explored in detail. The proposed technique that demonstrates the two-step encryption and decryption approach to be used to derive encryption and decryption keys from biometric fingerprint templates' data is described. Chapter three analyzes the research methodology used in this study. The methodologies used for data collection, analysis and interpretation are described. In chapter four, interpretation and analysis of results from the research survey conducted is presented. The fifth chapter discussed system design and development of the proposed biometric encryption and decryption technique. Thereafter, the tools and technologies used are described and justification for their utilization is given. Tests were performed on the new technique and comparisons with existing biometric template protection techniques is done. The final chapter summarized empirical research findings, discussed theoretical implications of research findings and provided recommendations and directions for future work.

CHAPTER TWO

LITERATURE REVIEW

2.1 Introduction

In this chapter, existing schemes and approaches in literature that have been proposed and used by researchers and biometric system developers to protect biometric templates are reviewed. Types of biometric templates attacks that have been documented in existing literature are identified and discussed. To understand these attacks, biometrics were defined, their major components and types identified then biometric properties, functions, capabilities and classifications were discussed.

2.1.1 Biometrics Definition

Biometrics refers to the automatic authentication of a person's physiological or behavioral characteristics (Jain et al., 2005).

2.1.2 Biometric System Definition

A biometric system is a pattern recognition system that retrieves biometric patterns from an individual, extracts biometric feature sets then saves them as biometric templates in databases after which it compares captured feature sets with those saved in database (Morwal et al., 2012). Jain et al., (2005) described a biometric template as a set of salient features that summarizes the biometric data of an individual.

2.1.3 Biometric System Components

A biometric system consists of 5 major components. According to Menariya and Ojha (2012), these five (5) major components are;

i) **Sensor module**: The interface between the user and the biometric system. It is at the sensor where the biometric traits e.g. fingerprint patterns of a user are scanned.
ii) **Feature extractor module**: This is the biometric system module that retrieves feature sets from biometric traits presented at the biometric sensor.

iii) **Templates Database Server**: In the templates database, the extracted feature sets are saved for future use in verification and identification purposes at the templates database or server.

iv) **Matcher module**: This is the biometric system module that performs comparison of feature sets saved in a biometric system database with the feature sets of a person presented at a sensor. A successful match implies the feature sets belong to an identified or verified user while a failed match signifies a mismatch of biometric feature sets in database and those being presented at sensor of a biometric system.

v) **Decision module**: This is the logic module of the biometric system that determines the next point of action after either a successful or a failed match.

2.2 Type of Biometrics

Biometric characteristics used in biometrics are of two (2) types. These characteristics were grouped into two types by Kannan and Thilaka (2013) as either Physical or Behavioral biometrics.

1. Physical Biometrics

The intrinsic characteristics of a human body where physical biometric traits can be extracted & measured for purposes of comparison are Fingerprint, Facial Recognition, Iris, Retina, Voice, Palm Vein and DNA. The physical biometric aspects of a person do not change over time. They are distinct in nature.

2. Behavioral Biometrics

The non-physical unique characteristics that are related to behavior of an individual are called behavioral biometrics. They are; Voice recognition (differences in tonal and pitch variation), handwriting pattern recognition, keystroke spacing. This research study does not dwell on these types of biometrics save for comparison purposes. In contrast to physical biometrics, the behavioral biometric characteristics of a person do change with time.

2.3 Properties of Biometrics

According to Jaiswal et al., (2011), for biometric physical traits or biometric behavioral traits to be considered suitable for use in biometrics, they must meet some very important specifications to facilitate easy identification and verification of individuals. These fingerprints properties are;

i) Universality

This property of biometric fingerprints implies that every person bears biometric fingerprint traits that can be retrieved and used for measuring biometric features from a person (Jaiswal et al., 2011).

ii) Uniqueness / Distinctiveness

It has empirically been observed over time that no two fingerprints on any two persons have been found to bear resemblance to each other for the over 140 years fingerprints have been used for comparison. Fingerprint patterns are so unique such that not even two identical twins have similar fingerprint traits on any of their fingers (Jaiswal et al., 2011).

iii) Permanence

Fingerprint patterns of an individual do not change during their entire lifetime. This is the permanence property of fingerprints. The ridges and bifurcations or rather patterns on a person's fingerprint expand proportionately as the person grows from child to adult thus maintaining their proportional scale in their entire existence (Jaiswal et al., 2011).

iv) Collectability

Biometric features of a fingerprint have to be quantifiable to necessitate easy comparison with other fingerprint samples solely gathered before for purposes of verification and identification (Jaiswal et al., 2011).

v) Accuracy / Performance

Fingerprints have lower False Rejection Rate (FRR) and False Acceptance Rate (FAR) making them more reliable than other modes of authentication (Jaiswal et al., 2011).

vi) Acceptability

An authentication system must meet the required standards for verification and identification for it to be formally accepted and the same applies for fingerprints. Fingerprints have been used since the beginning of the twentieth (20th) century and have become endorsed for standard routines in forensics.

From properties of biometric fingerprints it is evident that the permanence nature of fingerprint is also its own undoing if proper precautions and care are not put into consideration when saving fingerprint patterns in a biometric system's database. Fingerprint patterns of a person do not change in their entire lifetime. If fingerprint patterns of an individual are acquired by adversaries, they cannot be changed unlike the case of passwords where a new password can be used. According to Jaiswal et al., (2011), it is this permanence property of fingerprints that prompts for secure ways of storing biometric templates retrieved from an individual's fingerprint.

2.4 Biometrics Functions

The three major functions of biometrics are Enrollment, Archiving and Biometric Template Matching (Malhotra & Kant, 2013).

i) Enrollment

Biometric systems acquire an individual's biometric data via biometric sensor during Enrollment process (Raju et.al, 2014). A good example is the extracting of biometric fingerprint patterns from a finger for purpose of storing them in a biometric system.

ii) Archiving / Storage

Biometric systems have to save biometric data captured from users to a database or server of the system for subsequent use in biometric template matching (Malhotra & Kant, 2013).

iii) Biometric Template Matching

In biometric template matching, comparison between saved biometric templates and captured biometric data is carried out (Venkatesh, Balaji, & Chakravarthy, 2012). A certain threshold has to be met for a successful template match to be registered i.e. a positive identification or verification. A failed match is when the biometric features of a user do not match with those saved in a biometric system's database.

2.5 Biometrics Capabilities

Biometric template matching of a biometric system takes these two forms of authentication; verification and identification (Venkatesh, Balaji, & Chakravarthy, 2012).

i) Identification

A biometric system has *identification* capabilities if it is able to uniquely retrieve and match an individual's biometric features from a database of other individuals e.g. match fingerprint patterns of a user from several other fingerprints in a database. Identification is a 1: *n* search where *n* is all individuals in a biometric database (Venkatesh, Balaji, & Chakravarthy, 2012).

ii) Verification

In *verification* a known distinctive attribute about a user is used to retrieve biometric features of an individual then perform a match comparison against it from biometric feature sets presented at a biometric sensor e.g. using ID NO, VAT NO, NSSF NO, NHIF NO or Employee NO to retrieve biometric fingerprint features saved with the distinguishing attribute against the fingerprint features presented at a biometric sensor

(Venkatesh, Balaji, & Chakravarthy, 2012). It is in simple terms, to ascertain that the person is who they purport to be or rather a 1:1 matching.

2.6 Biometrics Classification

2.6.1 Unimodal Biometric Systems

A unimodal biometric system is one whose one sensor extracts biometric features from only one physical or behavioral biometric source e.g. fingerprint. Existing literature has shown that unimodal biometric systems are prone to spoof attacks and experience problems like noisy sensor data. This downside to unimodal biometric attacks as seen in (Aly et al., 2012) motivates this study as is later shown in section 2.7 to narrow down to "Type 6 attack" in biometric systems also known as spoof attacks on biometric templates in a biometric system's database.

2.6.2 Bimodal Biometric Systems

A bimodal biometric system has 2 sensors which extract biometric features from only 2 physical or behavioral patterns e.g. fingerprint and face (Malhotra & Verma, 2013).

2.6.3 Multimodal Biometric Systems

(Sanjekar & Patil, 2013) describes a multimodal biometric system as one that uses a combination of two or more biometric modalities in a verification or identification system while Eshwarappa and Mrityunjaya (2010) defined a multimodal biometric system as a multi-biometric system that utilizes more than one physiological or behavioral biometrics for enrollment and identification.

2.7 Biometric System Attacks

Biometric attacks are the adversarial threats that a biometric system is susceptible to at the channels between its components or on its components. This study found out from (Ratha et al, 2001) that biometric system attacks are categorized into eight types. The study designed a diagrammatic representation of these attacks shown in figure 2.1 and discussed these eight types of biometric system attacks.

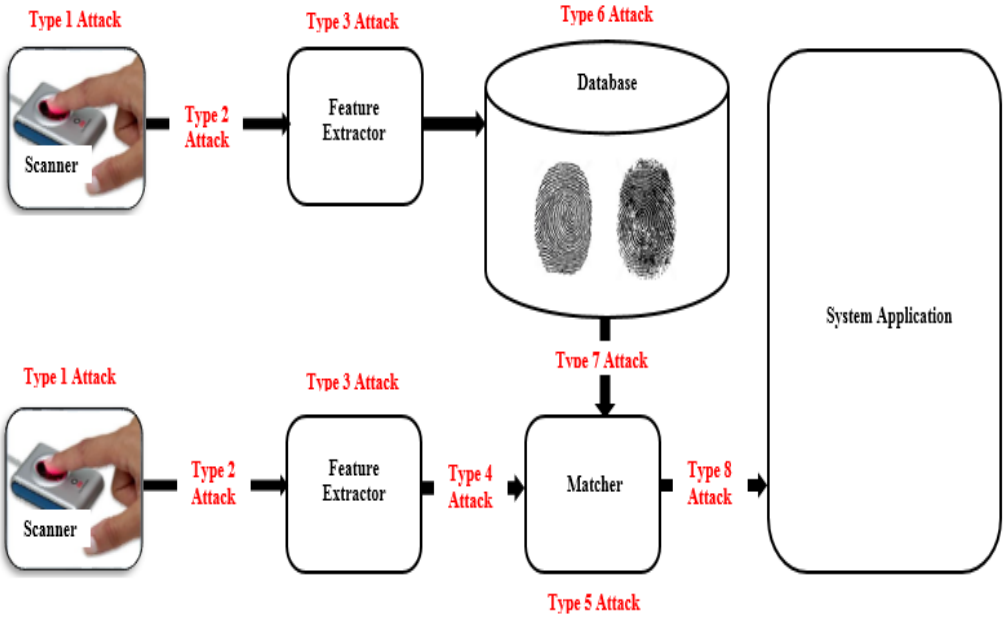

Figure 2.1. Biometric System's Attacks

1. Attack at the scanner

In this attack also known as "Type 1 attack", the attacker can physically destroy the recognition scanner and cause a denial of service. The attacker can also create a fake biometric trait such as an artificial finger to bypass fingerprint recognition systems, or inject an image between the sensing element and the rest of the scanner electronics to bypass recognition systems.

2. Attack on the channel between the scanner and the feature extractor

This attack is also known as "Type 2 attack" or "Replay attack". When the scanner module in a biometric system acquires a biometric trait, the scanner module sends it to the feature extractor module for processing. Type 2 attack happens between scanner and extractor.

3. **Attack on the feature extractor module**

In this attack, the attacker can replace the feature extractor module with a Trojan horse. This attack is known as “Type 3 attack”.

4. **Attack on the channel between the feature extractor and matcher**

This attack also known as “Type 4 Attack” is where the attacker intercepts the communication channel between the feature extractor and the matcher to steal feature values of a legitimate user and replay them to the matcher at a later time.

5. **Attack on the matcher**

This point of attack is known as “Type 5 Attack”. The difference is that the attacker replaces the matcher with a Trojan horse. The attacker can send commands to the Trojan horse to produce high matching scores and send a “yes” to the application to bypass the biometric authentication mechanism.

6. **Attack on the system database**

This attack also known as “Type 6 Attack”, the attacker compromises the security of the database where all the templates are stored. Compromising the database can be done by exploiting vulnerability in the database software or cracking an account on the database. In either way, the attacker can add new templates, modify existing templates or delete templates.

7. **Attack on the channel between the system database and matcher**

In this attack, the attacker intercepts the communication channel between the database and matcher to either steal and replay data or alter the data. This point of attack is known as “Type 7 Attack”.

8. **Attack on the channel between the matcher and the application**

In this attack also "Type 8 Attack", the attacker intercepts the communication channel between the matcher and the application to replay previously submitted data or alter the data.

2.8 Biometric Fingerprint Template Security

In this section, the study explored the vulnerabilities posed by biometric template attacks then reviewed the 'Type 6 attack' which is the prevalent attack on biometric templates in a biometric system database.

2.8.1 Biometric Template Vulnerabilities

This study established from a more recent research by Raju et al., (2014) that attacks on biometric templates can lead to the following vulnerabilities;

i. A biometric template can be replaced by an impostor's biometric template to gain unauthorized access.
ii. A physical spoof of a Biometric Template can be created from the biometric template to gain unwarranted access to the system including other systems that use the same biometric fingerprint trait.
iii. Stolen biometric Templates can be replayed to the matcher to gain unauthorized access past authentication vaults.
iv. Biometric Templates if not properly secured can be used by adversaries for cross-matching across other databases to covertly track a person without their consent.

2.8.2 Biometric Template Attack in the Database

This study established from review of biometric system threats and attacks that "Type 6 attack" is where an adversary attacks biometric templates in a database. As is seen in this type of attack, the hacker can add new templates, modify existing templates or delete templates.

In a previous publication, Brindha (2012) mentioned that, one of the most vital harmful attacks on a biometric system happens when it is against the biometric templates. She further explained how attacks on the templates can lead to grave vulnerabilities where a template can be replaced by an impostor's templates to achieve unlawful access to a system. She further cautioned against biometric templates being stored in plaintext form and insisted that fool-proof methodologies are essential in securing storage of biometric templates to safeguard both safety of the biometric system and that of the users.

2.9 Biometric Template Protection Techniques

Biometric Template Protection Schemes are classified into Feature Transformation and Biometric Encryption. Jain et al., (2008) categorized the various biometric template protection techniques as (i) Feature Transformation and (ii) Biometric Encryption with the most common Feature Transformation technique being Cancellable Biometrics. This is the basis on which biometric template techniques have been classified. Figure 2.2 shows a diagrammatic representation of these techniques that this study came up with to represent these techniques according to whether they stem from feature transformation or biometric encryption.

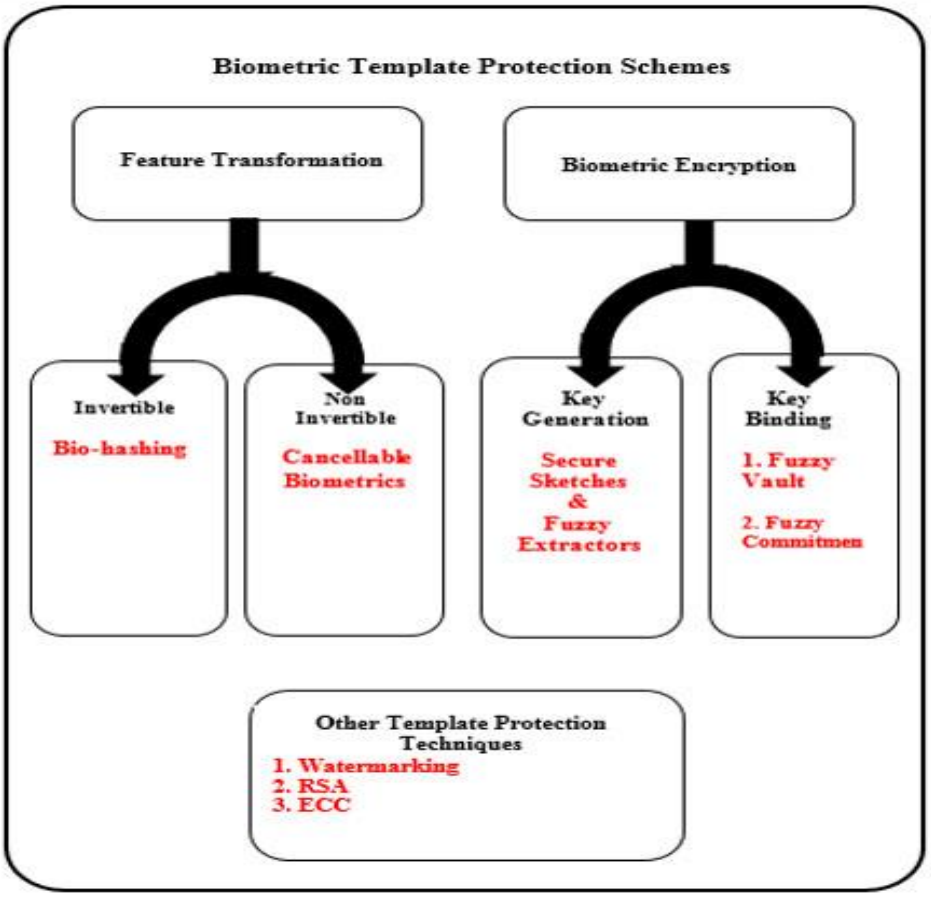

Figure 2.2. Biometric Template Protection Schemes

2.9.1 Feature Transformation

In Feature Transformation, a biometric template (BT) is transformed to F (BT, X) after a function F with a randomly generated key X is applied to it. Feature Transformation is further categorized into either invertible or non-invertible transform. In invertible transform, the key X can be used to recover the original biometric template (BT) while in non-invertible transform the key X is a one-way key that makes it hard to recover the original biometric template (BT) even if the key X is known as pointed out by Arjunwadkar and Kulkarni (2010). Existing literature identify bio-hashing and cancellable biometrics as invertible and non-invertible transformation respectively (Gaddam & Lal, 2011).

i) Cancellable Biometrics

Unlike passwords, PINs and access codes, biometric templates can never be replaced with newer ones if compromised. To circumvent this challenge cancellable biometrics was introduced where biometric templates can be cancelled and replaced (Radha & Karthikeyan, 2011).

Cancellable biometrics scheme is an intentional and systematic repeatable distortion of biometric template data with the purpose of protecting it under transformational-based biometric template protection. In the concept of cancellable transformation, a transformed template can be cancelled and re-issued by changing transformation parameters if misplaced (Ratha et al., 2007).

Cancellable biometric is not without its fair share of challenges, Rathgeb and Uhl (2011) raised concerns that if transformed biometric data is compromised, transformation parameters should be changed to deter adversaries from tracing and cross-matching users' biometric templates.

From studying cancellable biometrics, the study found out that if transformational parameters are known to hackers, cancellable biometrics will not be secure. The other downside of cancellable biometrics as is evidenced by Du et al., (2011) is that it reduces recognition accuracy of the biometric-based system due to the high variance brought about by the distorted data when transformation is applied on users' biometric data.

ii) Bio-hashing

Biohashing is a biometric template protection approach in which features from a biometric template are transformed using a transformation function defined by a password or a key known only to the user (Kannan & Thilaka, 2013). This key or password needs to be securely stored and remembered by the user for subsequent authentication.

The key or password used by user in biohashing increases entropy of biometric templates which further deters adversary attacks. Direct mixing of a pseudo-random

number (which is kept secret) and biometric data is used to compute a binarized key of 80-bits key with a 0.93% false rejection rate of the system (Radha & Karthikeyan, 2010).This generated physical token can be used in smartcard or USB tokens as shown by Kannan and Thilaka (2013).

The major drawback of biohashing is the reduced performance when the legitimate token is retrieved and presented by an adversary purporting to be a legitimate user (Gaddam & Lal, 2011). Das et al., (2012) however are of the opinion that bio-hash must be linkable to the original template to permit authentication and at the same time be non-invertible to thwart incidences of theft but then the need to have some elasticity to make the biohashing robust introduces possibilities of some unavoidable information leakage in the process of computing the bio-hash.

2.9.2 Biometric Cryptosystems

Traditional identity authentication based on simple passwords have always been easy to break using e.g. simple dictionary attacks (Li & Hwang, 2010). To circumvent these caveats, cryptographic secret keys and passwords have been proposed. Jain et al., (2008) subdivided these biometric cryptosystems into the two following categories; Key Generation and Key Binding.

i) Key Generation

Study of existing literature revealed that, in Key Generation, a biometric key is derived directly from biometric data as is evidenced in (Dodis et al., 2008). This study then proceeded to explore Secure Sketches and Fuzzy Extractors which fall under Key Generation Cryptography Schemes.

a) **Secure Sketches and Fuzzy Extractors**

Dodis et al (2008) originated with secure sketches and fuzzy extractors in a preliminary version of their research work in year 2004 which was entirely published in a later work in (Dodis et al., 2008). Their biometric fingerprint scheme of using secure sketches and fuzzy extractors was significant in the biometric cryptosystems as it allowed for correcting of error codes in biometric data and generating almost linear

encryption keys for use in encryption and decryption. In their later published research work they alleged that they were formaly defining efficient and secure techniques for;

- Retrieving keys for any cryptography application from noisy data including biometric data.
- Then reliably and securely perform authentication of biometric data.

They defined Fuzzy Extractor and Secure Sketch they proposed as follows;

a) **Fuzzy Extractor:** A Fuzzy Extractor reliably extracts almost uniform randomness **R** from its input: The significance of fuzzy extraction is that it is error-tolerant in the sense that **R** will not change even if the input changes e.g. if another biometric template from the same finger is used, as long as it is almost similar to the original **R** implying **R** can be used in a cryptographic application as a key.

b) **Secure Sketch:** Dodis et al., (2008) held that their Secure Sketch produced public information about its input **w** that did not reveal **w**, and yet allowed exact recovery of **w** given another value that is close to **w** an advantage that made it possible to be reliably used to reproduce error-prone biometric inputs without incurring security risks intrinsic in storing them.

In a recent publication on analysis of reusability of fuzzy extractors and secure sketches by Blanton and Aliasgari (2013), they inferred that a number of the original constructions could not be safely applied severally to the same biometric, thus significantly limiting and reducing their usability in practice.

ii) Key Binding

In Biometric Cryptosystems, this study established that Key Binding is where a secret key and the biometric template are monolithically bound within a cryptographic framework where it is computationally infeasible to decode the key or biometric template without prior knowledge of the user's biometric data (Kannan & Thilaka, 2013). The study continued to explore Fuzzy vault and Fuzzy commitment

cryptographic schemes which use key binding in this research to determine how key binding works.

a) Fuzzy Vault

Fuzzy vault is a cryptographic construct that was first proposed by Juels and Sudan (2002) where secret infromation is encrypted and decrypted securely using a fuzzy unordered set of genuine points and haff points. Geetika and Kaur (2013) described a biometric fuzzy vault as a biometric cryptosystem used for protecting private keys and releasing them only when the legitimate users enter their biometric data while Deshpande and Joshi (2013) defined a fuzzy vault as a scheme utilized for secure binding of randomly generated keys with extracted biometric features.

While studying significance of biometric vault scheme, this study determined from (Prakash & Bharathan, 2012) that the motivation to protect secret keys in biometric cryptographic modules using fuzzy vault scheme came from the analogy that the current cryptographic algorithms have a very high proven security but have problems in guaranteeing absolute secret key security management. This assertion is further affirmed by Meenakshi and Padmavathi (2010) who confirmed that fuzzy vault eliminates key management problems found in other practical cryptosystems. The following are the limitations of a fuzzy vault scheme as shown in (Hooda & Gupta, 2013);

i. Difficulty in revoking a compromised vault which is also prone to cross-matching of biometric templates across databases.
ii. Easy for an attacker to stage attacks after statistically analysing points in vault.
iii. It is possible for an attacker to substitute their biometric features with that of the targeted biometric features thus beating vault authentication.
iv. The other threat is that, if the original template of the genuine user is temporarily exposed, the attacker can glean the template during this exposure.

b) Fuzzy Commitment

Fuzzy Commitment is a biometric cryptosystem which is used to secure biometrics traits represented in binary vector (Jeny & Jangid, 2013). Fuzzy commitment scheme is further described as one where a uniformly random key of length 1 bits is generated and used to exclusively index an n-bit codeword of suitable error correcting code where the sketch extracted from the biometric template is stored in a database.

The difference between fuzzy vault and fuzzy commitment as contrasted by Geethanjali et al., (2012) is that, biometric traits secured by fuzzy commitment are represented in the form of binary vectors which are divided into a number of segments and each segment is separately secured while biometric traits in fuzzy vault are represented in the form of point set which are secured by hiding them with chaff points.

Al-Saggaf and Acharya (2013) argued that the ordinary fuzzy commitment scheme cannot satisfy hiding and binding properties of biometric traits and considered it insecure. They pointed out that the cryptographic hash function **h (c)** where the secret message **c** is hidden in the hash value **h (c)** as not secure enough because the cryptographic hash functions such as **MD5** and **SHA** families have already been proven theoretically and practically to be vulnerable to collision and second preimage attacks. Their argument that **MD5** and **SHA** are vulnerable is undeniably supported in (Schmitt & Jordaan, 2013).

Advantages of Biometric Keys

This study found out that the advantages of using biometric keys as compared to traditional passwords as shown by Das (2011) to be as follows;

1) Biometric Keys cannot be misplaced or forgotten.
2) It is difficult to copy and distribute them.
3) They are extremely hard to reverse engineer, forge or distribute
4) They are not easy to guess at unlike passwords.

2.9.3 Other Biometric Template Protection Schemes

i) Watermarking Scheme

The aim of watermarking is to use biometric fingerprint templates as a message to be integrated in a robust watermarking application like copyright protection in order to enable biometric recognition after the extraction of the watermark. In a biometric watermarking scheme, if an attacker tries to replace or forge the biometric template then he must have the knowledge of pixel values where watermark information is hidden as evidenced in (Malhotra & Kant, 2013).

While exploring existing biometric template protection techniques, Poongodi and Betty (2014) explained the advantage of watermarking approach as follows; they said it was difficult to forge stored biometric templates and that watermarking provided high security of biometric templates. Fazli and Zolfaghari-Nejad (2012) backed the same views that biometric watermarking is one of the template protection techniques that significantly prevents attacks on biometric templates but added that it was best used when biometric data is to be transmitted via network or by a person e.g. in a smart card.

This study then explored the downsides of watermarking as compared to other biometric template techniques and established that there is a greater amount of time taken in inserting a watermark in biometric templates as was pointed out by Poongodi and Betty (2014) and that most of the algorithms used for watermarking require original image to be present to extract the watermark unlike biometric cryptosystems techniques which do not need to keep the original image after encryption is done as was shown by Naik and Holambe (2010). This made the study to conclude that, keeping the original image in a watermarking scheme requires more storage space which presents an opportunity for adversaries to spoof the original image.

ii) Rivest, Shamir and Adleman (RSA) Technique

RSA is an encryption algorithm for public key cryptography based on the practical difficulty problem of factorization of large integers as was described by Nasir and Kuppuswamy (2013). RSA algorithm's debut was in 1978 when it was first introduced by Rivest, Shamir and Adleman and was named after the brains behind it as Rivest, Shamir and Adleman algorithm. The implementation of RSA algorithm involves a public key and a private key where the public key can be known to everyone and used for encrypting messages. This is such that the message encrypted with public key will only be decrypted using the private key (Chandra et al, 2013).

RSA is implemented in three (3) phases where in the 1st phase key generation happens and in the 2nd and 3rd phase encryption and decryption takes place. RSA is secure if long keys are used and is significant in that it protects files from hackers and also ensures safe transmission of files between two (2) points as argued in (Zhou & Tang, 2011). Based on this observation this study concluded that an RSA encrypted message is likely to be decrypted if brute force is used where public key is known and the private key used is short.

iii) Elliptic Crypto Curve (ECC) Technique

Muthukuru and Sathyanarayana (2013) described an Elliptic Curve Cryptography also known as ECC as a public key cryptography that makes use of algebraic forms of elliptic curves over elements restricted to finite fields. They added that ECC algrorithm uses smaller keys leading to lower memory usage and reduced computational requirements than traditional encryption and decryption algorithms.

While comparing RSA and ECC encryption algorithms, this study established from a research experiment comparing the two algorithms done by Maniroja and Sawarkar (2013) that, RSA scheme takes 10 seconds to encrypt an image of size 256 by 256 whilst ECC scheme takes 30 seconds. The study also noted that an equivalent amount of time was required in decryption of images during verification and identification of persons on a biometric authentication system using these biometric template protection schemes and due to this bottleneck, there was need for alternative biometric encryption

schemes or rather the need for RSA and ECC schemes to be optimized for short turnaround times since biometric systems' performance is critical if they are to be considered efficient for use in verification and identification processes.

2.10 Features of an Ideal Unimodal Biometric Template Protection Scheme

According to Maltoni et al., (2003), an ideal biometric template protection scheme should consist of the following four attributes.

i) **Diversity** : A secure biometric template must not allow crossmatching across databases, thus ensuring their bearer's privacy.
ii) **Revocability** : It should be straightforward to revoke a compromised biometric template and reissue a new one based on the same biometric physical traits of the initial bearer.
iii) **Security** : It should not be possible to reverse engineer the secure biometric template to obtain the original biometric template. This property discourages adversaries from recreating original biometric traits and using them as a physical spoof in stolen templates.
iv) **Performance** : The biometric template protection scheme should not reduce the matching speeds of templates or trigger an upward surge in False Acceptance Rates and False Rejection Rates.

2.11 Biometric Encryption Key Derivation

2.11.1 Introduction

First, the study reviewed biometric template protection schemes in existing literature and established that there isn't a reliable, effective and foolproof technique that guarantees diversity, revocability, security and performance as is required of an ideal biometric template protection scheme. This current status of affairs then motivated this research study to device an approach that derives biometric encryption keys from biometric fingerprint templates. It involves a two-step enrollment and authentication of fingerprints while encrypting fingerprints before saving them to a database with encryption keys derived from other biometric fingerprint templates.

This section demonstrates how this approach derives biometric encryption keys from biometric fingerprint templates. First, when a fingerprint is captured using a fingerprint sensor, a fingerprint template is extracted from it for purposes of enrollment, verification and identification. The remainder of section 2.11 proceeds to show what constitutes a biometric fingerprint template $\mathbf{B_T}$, a minutia point $\mathbf{m_i}$, a ridge type $\mathbf{r_i}$ and illustrates how this study arrived at a biometric encryption key $\mathbf{Enc_k}$ from these properties of a biometric fingerprint template $\mathbf{B_T}$.

2.11.2 Description of Biometric Encryption Key Components

$\mathbf{B_T}$ will denote a biometric fingerprint template.

A biometric fingerprint template $\mathbf{B_T}$ consists of minutiae **m** points as shown in (Bansal et al., 2011). Where $\mathbf{m_1}, \mathbf{m_2}, \mathbf{m_3}\ldots\ldots \mathbf{m_n}$ minutiae points make up a fingerprint template $\mathbf{B_T}$.

The encryption algorithm requires the summation of minutiae **x** coordinate values in biometric fingerprint template $\mathbf{B_T}$ which is calculated as follows;

$$\sum_{n=1}^{n} x_n = x_1 + x_2 + x_3 + \ldots + x_n$$

Where **n** is the number of minutiae points in a biometric fingerprint template $\mathbf{B_T}$.

The encryption algorithm requires the summation of minutiae **y** coordinate values in Biometric Fingerprint Template $\mathbf{B_T}$ which is calculated as follows;

$$\sum_{n=1}^{n} y_n = y_1 + y_2 + y_3 + \ldots + y_n$$

Where **n** is the number of minutiae points in a biometric fingerprint template $\mathbf{B_T}$.

The encryption algorithm requires the summation of minutiae **θ** angle of orientation values in Biometric Fingerprint Template $\mathbf{B_T}$ which is calculated as follows;

$$\sum_{n=1}^{n} \boldsymbol{\theta_n} = \boldsymbol{\theta_1} + \boldsymbol{\theta_2} + \boldsymbol{\theta_3} + \ldots + \boldsymbol{\theta_n}$$

Where **n** is the number of minutiae points in a biometric fingerprint template $\mathbf{B_T}$

The encryption algorithm requires the count of all ridge bifurcations **b** in a given biometric fingerprint template $\mathbf{B_T}$ which is denoted as **b.**

The encryption algorithm requires the count of all ridge endings **e** in a given biometric fingerprint template $\mathbf{B_T}$ which is denoted as **e.**

All ridges $\mathbf{R_T}$ in a biometric template is a sum of all bifurcations **b** and endings **e** in a biometric template $\mathbf{B_T}$ as shown below;

$\mathbf{R_T} = \mathbf{b} + \mathbf{e}$

A minutia point $\mathbf{m_i}$ is uniquely identified by

$\mathbf{m_i} = \{\mathbf{x_i}, \mathbf{y_i}, \boldsymbol{\theta_i}, \mathbf{r_i}\}$ **where i = 1...n** as is expounded in (Bansal et al., 2011).

2.11.3 Deriving Biometric Encryption Key

The study then derived a biometric encryption key $\mathbf{Enc_k}$ from a biometric fingerprint template's $\mathbf{B_T}$ total number of **x** values $\sum_{n=1}^{n} \boldsymbol{x_n}$, total number of **y** values $\sum_{n=1}^{n} \boldsymbol{y_n}$, summation of angles of orientation $\sum_{n=1}^{n} \boldsymbol{\theta_n}$, total number of ridge bifurcations **b** and total number of ridge endings **e** appended with alphanumeric literals in between them to increase the strength of the derived biometric encryption key as follows;

$\sum_{n=1}^{n} \boldsymbol{x_n}$ is appended with alphabet **'X'** and

$\sum_{n=1}^{n} \boldsymbol{y_n}$ is appended with alphabet **'Y'** and

$\sum_{n=1}^{n} \boldsymbol{\theta_n}$ is appended with alphabets **'AO'** and

b is appended with alphanumeric **'BFN1'** and

e is appended with alphanumeric **'END0'**

Such that if $\sum_{n=1}^{n} x_n$ is **1122**, $\sum_{n=1}^{n} y_n$ is **3344**, $\sum_{n=1}^{n} \theta_n$ is **5566**, **b** is **77** and **e** is **88** then the derived encryption key **Enc$_k$** will be as shown below

Enc$_k$ = {1122X3344Y5566AO77BFN188END0}

Encryption Key **Enc$_k$** derived from a Biometric Fingerprint Template **B$_T$** will be arrived at using this novel approach as shown below;

Enc$_k$= $\sum_{n=1}^{n} x_n$ & 'X' & $\sum_{n=1}^{n} y_n$ & 'Y' & $\sum_{n=1}^{n} \theta_n$ & 'AO' & b & 'BFN1' & e & 'END0'

In a similar study done by Kaur et al., (2010), it was demonstrated that increasing the length of the password for encrypting biometric fingerprint templates increased security of the encryption system they were testing. In this study's encryption key, alphanumeric literals were added to the derived encryption key components to make the encryption key stronger.

2.11.4 Example of Retrieving Key for Encryption from Fingerprint Template

To demonstrate how **Enc$_k$** is retrieved from a fingerprint template, this study captured a biometric fingerprint image shown in figure 2.3 using the proposed biometric encryption and decryption tool.

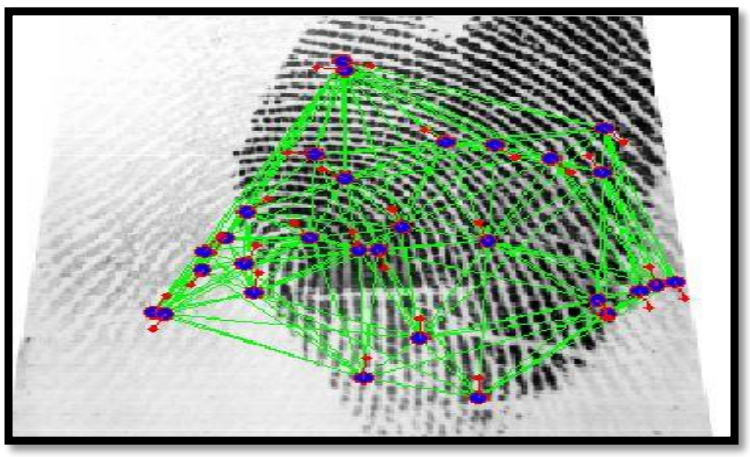

Figure 2.3. Fingerprint image showing minutiae points

The fingerprint image in figure 2.3 is then processed to extract its minutiae data and the fingerprint feature sets. In an X and Y axis plane the data for minutiae points would resemble data presented in tabular format. The minutiae points shown in figure 2.3 are presented as biometric template data in figure 2.4 which shows 30 minutiae points extracted with their X, Y, Direction and Ridge Type values.

MINUTIAE	X	Y	DIRECTION θ	RIDGE TYPE
1	204	272	228	Ending
2	249	261	92	Bifurcation
3	225	270	96	Ending
4	222	207	208	Ending
5	271	252	216	Ending
6	272	281	92	Ending
7	148	264	252	Ending
8	161	319	248	Ending
9	161	248	236	Ending
10	160	325	116	Bifurcation
11	185	216	208	Ending
12	193	143	192	Ending
13	167	201	204	Bifurcation
14	175	201	72	Bifurcation
15	169	117	188	Ending
16	110	209	40	Ending
17	101	200	168	Bifurcation
18	79	160	172	Ending
19	84	159	44	Bifurcation
20	273	159	204	Ending
21	269	168	76	Ending
22	287	174	76	Ending
23	119	226	160	Bifurcation
24	146	209	220	Bifurcation
25	218	104	192	Ending
26	294	178	204	Ending
27	118	192	176	Ending
28	302	180	76	Bifurcation
29	122	173	184	Ending
30	100	188	44	Bifurcation

Figure 2.4. Biometric Fingerprint Template showing Minutiae Data

Using the technique this study proposes for encrypting biometric fingerprints from fingerprint templates, the following values that make up the cipher key (**Enc_k**) are obtained from biometric fingerprint template in figure 2.4.

From section 2.11.3 this study proposes the below biometric encryption cipher key for encrypting biometric fingerprint templates.

Enc_k= $\sum_{n=1}^{n} x_n$ & 'X' & $\sum_{n=1}^{n} y_n$ & 'Y' & $\sum_{n=1}^{n} \theta_n$ & 'AO' & b & 'BFN1' & e & 'END0'

To determine Σx_n this study summed all the X values of the 30 minutiae points in this fingerprint template as follows;

From $\sum_{n=1}^{n} x_n = x_1 + x_2 + x_3 + ... + x_n$ in section 2.11.3 this translates to

$\sum_{n=1}^{n} x_{30} = x_1 + x_2 + x_3 + ... + x_{30}$ which results to $\sum_{n=1}^{n} x_{30} = \mathbf{5584}$

To determine Σy_n this study summed all the Y values of the 30 minutiae points in this fingerprint template as follows;

From $\sum_{n=1}^{n} y_n = y_1 + y_2 + y_3 + ... + y_n$ in section 2.11.3 this translates to

$\sum_{n=1}^{n} y_{30} = y_1 + y_2 + y_3 + ... + y_{30}$ which results to $\sum_{n=1}^{n} y_{30} = \mathbf{6256}$

To determine $\Sigma \theta_n$ this study summed all the θ values of the 30 minutiae points in this fingerprint template as follows;

From $\sum_{n=1}^{n} \theta_n = \theta_1 + \theta_2 + \theta_3 + ... + \theta_n$ in section 2.11.3 this translates to

$\sum_{n=1}^{n} \theta_{30} = \theta_1 + \theta_2 + \theta_3 + ... + \theta_{30}$ which results to $\sum_{n=1}^{n} \theta_{30} = \mathbf{4684}$

To determine **e**, this study counted all the values of ridge endings **e** in this fingerprint template which are 20 hence **e=20.**

To determine **b**, this study counted all the values of ridge endings **b** in this fingerprint template which are 10 hence **b=10.**

The end encryption key $\mathbf{Enc_k}$ after appending subsequent alphanumeric literals as proposed in section 2.11.2 the following key is derived from the fingerprint image in figure 2.3.

Enc_k= 5584X6256Y4684AO10BFN120END0

This is so after appending 'X' literal to $\sum_{n=1}^{n} x_n$, appending 'Y' literal to $\sum_{n=1}^{n} y_n$, appending 'AO' literal to $\sum_{n=1}^{n} \theta_n$, appending 'BFN1' alphanumeric literals to **b** and appending 'END0' alphanumeric literals to **e.**

2.12 Advanced Encryption Standard (AES) Cipher Algorithm

This study adopted AES algorithm to encrypt and decrypt biometric fingerprint templates. AES is a symmetrical encryption algorithm implying that the same key used for encryption is the same key that is required for decryption (Ramchander & Deepika, 2013).

i) Description of AES Encryption

AES is based on substitution and permutation design and has a fixed block size of 128 bits and a key size of 128, 192 or 256 bits. This study uses AES 256 because a 256 bit key is longer and is in the foreseeable future, more difficult to crack by a malware or hacker thus making it desirable for this research. The fact that AES can allow for 256 bit keys is a significant strength that it has the potential of protecting against future attacks e.g. collision attacks and possible quantum computing algorithms (Alanazi, et al., 2010). AES operates on a 4x4 order matrix of bytes called the state. AES encryption has two states namely; plaintext and ciphertext. Plaintext is the text, string, file or data that is to be encrypted while ciphertext is plaintext that has been encrypted. In this study, biometric fingerprint templates extracted from fingerprint templates are the plaintext to be ciphered into ciphertext i.e. encrypted biometric fingerprint templates. A key size in AES determines number of repetitions of transformation round that cipher a plaintext into a ciphertext. A 128 bit key has 10 rounds, 192 bit key has 12 rounds and 256 bit key has 14 rounds (Stallings, 2011).

ii) Stages of AES algorithm

AES has four stages which are required for every round (Nawaz, Hossain, & Grihan, 2013). The cypher begins with add round stage while the last round excludes the mix column. The four stages of AES algorithm are:

i. Substitute bytes: This function uses an S-box to perform a byte-by-byte substitution of the block.
ii. Shiftrows: This is a simple permutation for encryption and decryption.

iii. Mix Columns: This is a substitution that makes use of arithmetic with the irreducible polynomial "m(x) = x8 + x4 + x3 + x +1".

iv. Add round key: This function does a bitwise XOR operation of the current block with a portion of the expanded key.

v. General Structure of AES Encryption Process

This research sought to study AES cypher and established from (Stallings, 2011) that the structure of an AES encryption process to be as follows; First, The cipher takes a plaintext block size of 128 bits (16 bytes). The input to the encryption and decryption algorithms is a single 128-bit block. In (NIST, 2001) this block is depicted as a square matrix of bytes. This block is copied into the State array, which is modified at each stage of encryption or decryption. After the final stage, State is copied to an output matrix.

The ordering of bytes within a matrix is by column. So, for example, the first four bytes of a 128-bit plaintext input to the encryption cipher occupy the first column of the in matrix, the second four bytes occupy the second column, and so on. Similarly, the first four bytes of the expanded key, which form a word, occupy the first column of the matrix.

The cipher consists of rounds, where the number of rounds depends on the key length: 10 rounds for a 16-byte key, 12 rounds for a 24-byte key, and 14 rounds for a 32-byte key. This study uses AES 256 encryption and thus has a 32-byte key. The first rounds consist of four distinct transformation functions: SubBytes, ShiftRows, MixColumns, and AddRoundKey, which are described subsequently. The final round contains only three transformations, and has an initial single transformation (AddRoundKey) before the first round, which can be considered Round 0. Each transformation takes one or more matrices as input and produces a matrix as output. Figure 5.1 shows that the output of each round is a matrix, with the output of the final round being the ciphertext. Also, the key expansion function generates round keys, each of which is a distinct matrix. Each round key serves as one of the inputs to the AddRoundKey transformation in each round (Stallings, 2011). The structure of this AES encryption process is presented in the diagram in figure 2.5.

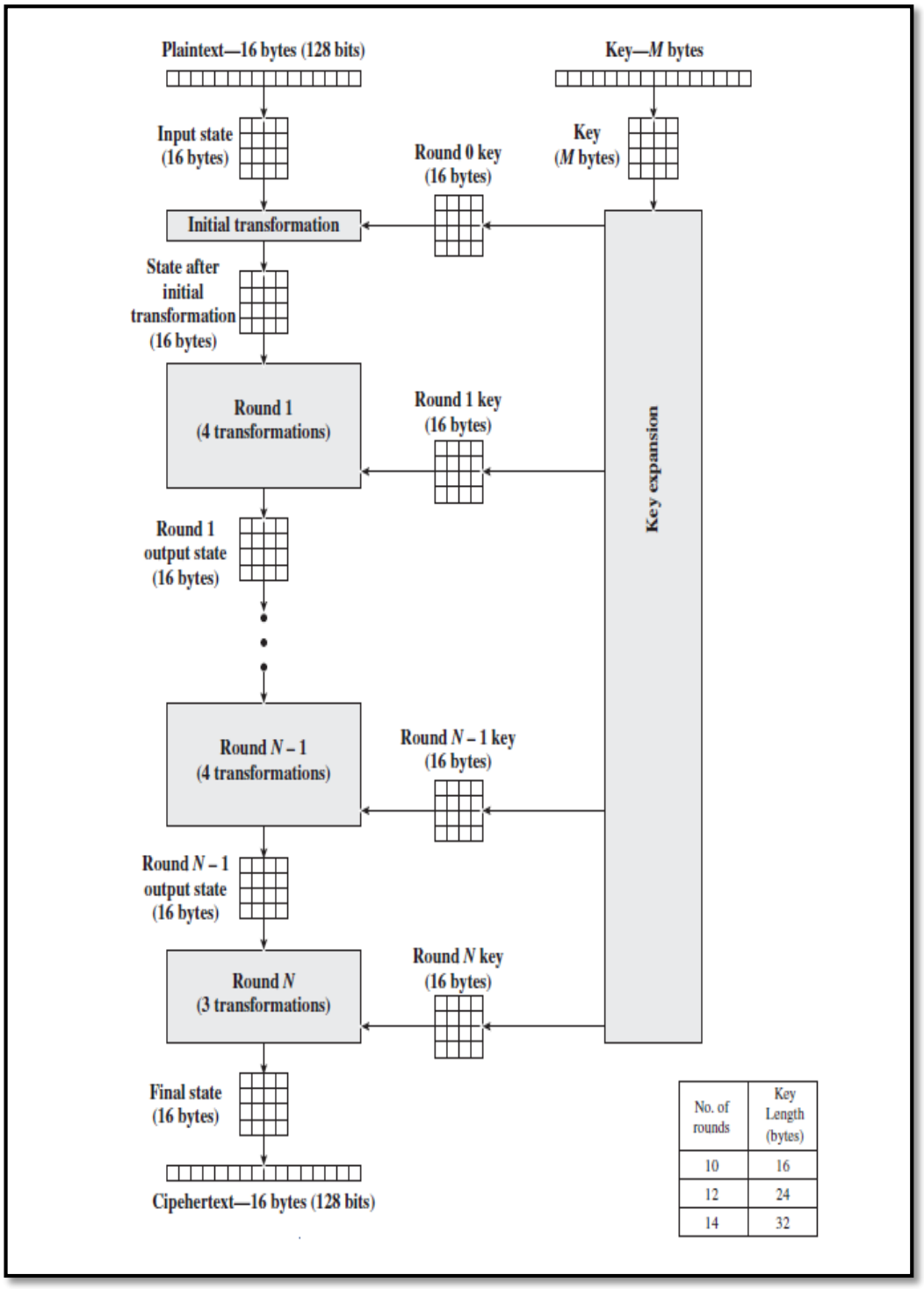

Figure 2.5. Structure of AES Encryption (Stallings, 2011)

iii) AES 256 Encryption and Decryption through 4 stages of AES algorithm

In AES algorithm, before encryption or decryption starts, AES takes the Cipher Key and performs a Key Expansion routine to generate a key schedule.

a) Encryption

AES 256 Encryption follows these steps to encrypt plaintext to ciphertext (Ramchander & Deepika, 2013). Encryption is described by individual transformations such a SubBytes, ShiftRows, MixColumn and AddRound Key.

1. SubBytes:
   Sub byte transformation is a nonlinear byte substitution that operates independently on each byte of the state using a substitution table called S-box.
2. ShiftRows:
   In shift rows transformation the bytes in the last three rows of the state are cyclically shifted over different numbers of bytes. The first row is not shifted.
3. MixColumn:
   Mix column transformation operates on the state column by column treating each column as a four-term polynomial.
4. AddRoundKey:
   In the Add round key transformation a round key is added to the state by a simple bitwise XOR operation. Each round key consists of byte words from the key schedule. These byte words are each added into the columns of the state.

b) Decryption

AES 256 Decryption follows these steps to decrypt ciphertext to plaintext. Decryption is described by individual inverse transformations of Encryption. The individual transformations used in Decryption process are Inv ShiftRows, Inv Subbytes, Inv Mixcolumn and Add Round Key (Ramchander & Deepika, 2013).

1. InvSubBytes:

   This is the inverse of the Sub Byte transformation in which inverse S-box is applied to each byte of the state.
2. InvShiftRows:

   Inv Shift Rows is the inverse of the shift rows transformation. The bytes in the last three rows of the state are cyclically shifted over different numbers of bytes. The first row is not shifted.
3. InvMixColumn:

   This is the inverse of the Mix column transformation. Inverse mix column operates on the state column by column treating each column as a four term polynomial.
4. AddRoundKey:

   The Add Round Key is same as at encryption stage but only that the keys in this stage are in the reverse order.

   The diagram in figure 2.6 shows the steps followed in AES 256 encryption and decryption in this study.

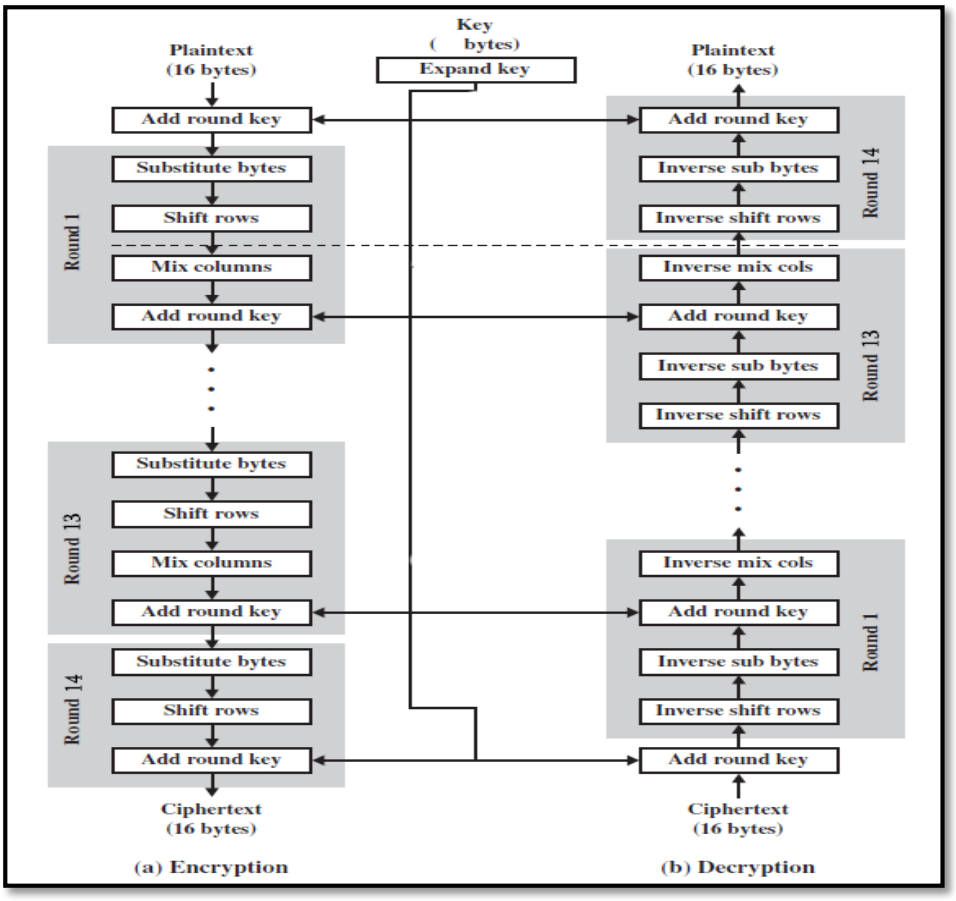

Figure 2.6. AES 256 Encryption and Decryption (Stallings, 2011)

iv) AES Encryption Modes of Operation

The study's quest to provide optimal security on biometric fingerprint templates, prompted this research to choose Cipher Block Chaining mode (CBC). CBC provides more security than Electronic Code Block implying that same block of plaintext which in this study is the biometric fingerprint data, yields different ciphertext results each time CBC encryption is run. In CBC mode, an XOR is performed on the input plaintext and the previously encrypted (or decrypted) ciphertext. Previously encrypted or decrypted data is not available during the first operation, hence an initialization vector must first be provided. CBC works on complete 128 bit blocks of plaintext, such that if the availed plaintext presented for ciphering is less than 128 bit long, the data is first padded (Stallings, 2011).

v) AES Fingerprint Encryption and Decryption Example

When a fingerprint is presented onto a fingerprint reader, a fingerprint image is captured. Feature sets or minutiae which are biometric traits of the fingerprint are extracted and saved as a biometric fingerprint template. Biometric templates are saved using various proprietary, ANSI and ISO standard formats. How fingerprints are saved in a biometric system determines how secure a biometric system is at averting adversarial attacks (Arjunwadkar et al., 2012). This research chose to use ISO 19794-2 format for biometric fingerprint templates which is an ISO standard format accepted widely in the spheres of biometric fingerprints (Alexandru et al., 2012).

a) Fingerprint Encryption using AES

Step1:

Fingerprint images are captured from 2 different fingers of same individual via biometric system's fingerprint reader.

Step 2:

Fingerprint minutiae are extracted from captured fingerprint images.

Step 3:

Fingerprint minutiae are saved into ISO 19792-4 format which are then Base64 encoded so that the fingerprint templates' plaintext is in text string and for easy transfer without data loss between feature extractor and database channel or between matcher and database channel.

Step 4:

Encryption key $\mathbf{Enc_k}$ to be used as cipher key in AES 256 encryption is retrieved from the fingerprint template 1 using proposed technique shown in section 2.11 during Biometric Encryption Key Derivation.

Step 5:

In this step, fingerprint template 2 is the plaintext that is encrypted with the encryption key retrieved from the first fingerprint to a ciphered string.

Step 6:

The fingerprint template 1 is saved to RDBMs database 1 while encrypted fingerprint template 2 is saved into a second RDBMs database 2.

Figure 2.7 shows fingerprint template data in ISO 19794-2 format before and after it is encrypted using AES 256.

PlainText: (ISO 19794-2 format Biometric Fingerprint Template which is encoded to Base64 string)	Rk1SACAyMAAAAAI6AAABSAFkAMUAxQEAAAAzHkDMAFPkAID5AF5cAEDhAFVgAEDeAJTQAEEPAGfY AEEQAEpcAECUAFv8AEChACT4AEChAGvsAICgAB50AEC5AIvQAEDBANTAAICnAJrMAICvAJpIAECp AO68AEBuAJIoAIBlAJuoAEBPAMOsAIBUAMQsAEERAMTMAAENALtMAEEfALVMAIB3AIGgAICSAJLc AEDaAPvAAEEmALHMAEB2AKOwAIEuAK9MAEB6ALz4AIBkAKcsAAFoAAIABgAAEAEBYlNFRwCsABIR BwkNDBUZGRsTFB0QEA8VGw0KHRoaEBoPDxYUFRwzCAYTFQIADBcdDwvKBAEBAhQZHB0TGQQFDRcB BRAWFxYaFxIdGhYcEA4LER0UGw8XExsDChwPEhwKCBcKHRYXCBwXEhARHBgLAQAREBAXFggSGgwI DQMCBRYGBAIIAA0IGgwRGhgOHRccDBwWDBYXBgwDEg8GBwYADA8aDREPCgADARwNCw0UAwoGBgkD AgsMAAcPCAwGCgIDBAMAChYIAgAFAAkEABMDCwMIBxUDDAwDCAsKHAo8SFgYCGQQICQscERYNABsE CgEYEykDEAYLFBUEEhcCBwsTGBQRFw4NFAQODBsDAgkXAAMFCAEOGhMEGQEOFxUBDhlbARYAGBUL FQ4dDhEUDRYHGAMZBRsFAQcYGRgNCgcWCRUFCxIBCQoJDhMYGwsbBQcYHAUDwkDBwsEEAkdCREJ
Encryption Key: Encryption key to be used in AES 256 encryption of plaintext to ciphertext Biometric Encryption Key derived from proposed technique in section 2.11 **Enc_k= 5584X6256Y4684AO10BFN120END0**	5584X6256Y4684AO10BFN120END0
CipherText: PlainText after being encrypted using Encryption Key **Enc_k=5584X6256Y4684AO10BFN120END0** to CipherText. Resulting Biometric Fingerprint Template string after it has been encrypted ready for archiving in RDBMs database	6E555671526434797863653677A6745766649595A337974303834555141705168622F7654416 F4676656B614A6F3159317667F706F304A44703276495436712B6E5A5156506A4532466A326A0D 0A2B687076646F4E4F2B58362F75636F6863617446 6A3649753452517949794F7757346E4E375 96C56614C43686F76687A5952634B304357696C51794A754D504E575332723239396 3364C492F 0D0A755350576C55473568484A776A5430646F466531356168415 77A61462F374D48483330626 76232595834475059776 12F776F506A6B61626B4F6E3944736145451535677554756633 2466C31 590D0A664F6D674653697A79464C6F6C4C4461615466794B3654725877 5A6155542B574D4C596 9645268387641573773767853377137 6B446F5545454626E2F7051483764717870637330326677 50550D0A4965574268 6E636E36424D7A2F484A4661736E447A4D485359522B335539476A57796 E6F5A5653465 36D537468763562714549323675 4D7930714C303352497 84C674E67476A563539 7454430D0A615A50454F466F51497A7665364E314F4366364C7A562B496D342F7842784D47475 A6C765646485271324F6A754139494C7A773958306A636A5038704C3542334448523 6A4E4641 383068370D0A4F6137546F5768346147714D37416D576C625956566E326A67486A4E4A7756335 5525931323750577A4A57554F36354247657A436A5955563246727862314772716914F435949 2B7935643 10D0A42377479565A61627A51546F744B7871594C597965514369484 3546A5073763 44C7A737044343145683 14E436F6646636B663963737233626847554348537 96D2F4957305538 5847664C77770D0A666D5951765A43754C7235677A507A574C424443694 23441304C3871454F7 0445455624754326561785343623236 36A3664357056645 76E535A4B4230467675325 14F2B532F 684F647758534 50D0A337877564E5072787365666357 46E32786369532B7631427047667344 94 444576C7875394 3635A73694C58734F7A6E6343304B52445970784A4474367765 4A4669796C48 4468726643 2F4D730D0A6C722B4941304D6C544E7A6A2F6D536 92F5853664A4C4B634E6157436 F67466F533463755534 4769717669755649565 8626C6835746C775533492F6A7439377144594 3 4B6D6B5677574F64300D0A69477A304C4477346D432F6C45777962595136453136616A49576E6 D6935432F73485432586C5A536C506A69386C316C7666393443 94B4C6E514F66656A6E4B5552 7975756B6479684D66570D0A6B374730616974 6A472F72574C615A437761346464476763 5A763 153757A33634E70714E43384D7752626271637350783051554778444435522F7551472F436F79 5851686F32553165476231 0D0A444C6949664930633368843744C4C51784C69325550534E654 A7131796944E5456547A7468503650794B6635615228766638612F7A316E3167787137367 83536 463043392B6261703379596B0D0A442F6550383769664833755334493 96F2B414448754F6B447 A5376334C62536B766C302F334165444B7361343952367A7255595645695855535374594764 6A 366C474A56434930796F6C466D0D0A345A6E3474735671 2F47454B0D0A

Figure 2.7. AES Fingerprint Template Encryption

b) Fingerprint Decryption using AES

Decryption in AES is usually the inverse of encryption (Stallings, 2011).

Step 1:

Fingerprint template 1 in RDBMs database 1 is retrieved and decoded from Base64 encoding.

The ciphered string of the second fingerprint template 2 in RDBMs database 2 is retrieved.

Step 2:

Decryption Key is retrieved from fingerprint template 1 which was retrieved from RDBMs database 1 using technique proposed in section 2.11. AES algorithm is a symmetrical cipher algorithm implying that the cipher key used as encryption key during encryption is the same cipher key used as decryption key during decryption (NIST, 2001).

Step 3:

Ciphered fingerprint template 2 is deciphered using AES 256 to ISO 19794-2 plaintext using decryption cipher key retrieved from fingerprint template 1 using technique proposed in section 2.11.

Step 4:

Decrypted biometric fingerprint template 2 now in ISO 19794-2 format is then used for matching of fingerprints during fingerprint verification and identification processes.

Figure 2.8 shows encrypted fingerprint template data before and after it is decrypted to ISO 19794-2 fingerprint template that is encoded to Base64 string.

CipherText: CipherText to be decrypted using Encryption Key **Enc_k=5584X6256Y4684AO10BFN120END0** to PlainText Encrypted Biometric Fingerprint Template string	6E555671526434797863 6C53677A6745766649595A337974303843555141705 16B622F7654416 F4676656B614A6F315931766F706F304A44703276495436712B6E5A5156506A4532466A326A0D 0A2B6870766646F4E4F2B58382F75636F6863617466 6A3649753452517949794F7757346E4E375 96C56614C43686F76687A5952634B304357696C51794A754D504E5753327232393963364C492F 0D0A7553505765547356848A776A5430646F4665313561684157 7A61462F374D4848333062 6 76232595834475059776 12F776F506A6B61626B4F6E3944736145415356775547566332466C31 590D0A664F6D6746536 97A79464C6F6C4C4461615466794B36547258775A61555426574D4C596 9645268387641573773767853377137 6B446F5545454262E2F705148376471787063733032 6677 50550D0A49655742686E636E36424D7A2F484A4661736E447A4D4853595228335539476A57796 E6F5A5653465365374687635627145493236754D7930714C3033524978 4C674E67476A563539 7454430D0A615A50454F466F51497A7665364E314F4366364C7A562B496D342F7842784D47475 A6C7656646852713246F6A7541394947A773958306A636A5038704C3542334448523 6A4E4641 383068370D0A4F6137546F5768346147 14D37416D576C625956566E326A67486A4E4A7756335 5525931323750577A4A57554F36354247657A436A5955563246727862314772716941 4F435949 2B793564310D0A42377479565A61627A51546F744B7871594C597965514369484354 6A5073763 44C7A737044343414568314E436F6646636B6639637372336268475543485379 6D2F4957305538 5847664C77770D0A666D5951765A43754C7235677A507A574C424443694234411304C3871454F7 0445455624754326561785343632363 6A3664357056645 76E535A4B42304676753251 4F2B532F 684F647758534500D0A337877564E5072787365666357 46E32786369532B7631427047766734494 444576C78753943635A73694C58734F7A6E6343304B5244597078 4A4474367765 4A4669796C48 44687266432F4D730D0A6C722B4941304D6C544E7A6A2F6D53692F5853664A4C4B634E6157436 F67466F5334637555344769717669755649565862 6C8835746C775533492F6A74393771445943 4B6D6B5677574F64300D0A69477A304C4477346D432F6C45777962595136453136616A49576E6 D6935432F73485432586C5A536C506A69386C316C766639344394B4C6E514F66656A6E4B5552 7975756B6479684D66570D0A6B3747306169746A472F72574C615A43776134646476 7635A763 153757A33634E70714E43384D7752626271637350783051554778444435522F7551472F436F79 5851686F3255316547623 10D0A444C6949664930633368684 3744C4C51784C69325550534E654 A713179694E5456547A7468503650794B663561522B766638612F7A316E3167778713736783536 463043392B6261703379596B0D0A442F6550383769664833755334493 96F2B414448754F6B447 A5376334C62536B766C302F334165444B7361343952367A7255595645695855533745947646A 366C474A56434930796F6C466D0D0A345A6E34747356712F47454B0D0A
Decryption Key: Decryption key (same as encryption key in symmetrical algorithms like AES) to be used in AES 256 decryption of ciphertext to plaintext	5584X6256Y4684AO10BFN120END0
PlainText: CipherText after being decrypted using Cipher Key **Enc_k= 5584X6256Y4684AO10BFN120END0** to PlainText. Resulting Base64 encoded Biometric Fingerprint Template string in ISO 19794-2 format after it has been decrypted.	Rk1SACAyMAAAAAI6AAABSAFkAMUAgQEAAAAzHkDMAFPkAID5AF5cAEDhAFVgAEDeAJTQAEEPAGfY AEEQAEpcAECUAFv8AEChACT4AEChAGvsAICgAB50AEC5AIvQAEDBANTAAICnAJfMAICvAJpIAECp AO68AEBuAJIoAIBlAJuoAEBPAMOsAIBUAMQsAEERAMTMAEENALtMAEEfALVMAIB3AIGgAICSAJLc AEDnAPvAAEEmALHMAEB2AKOwAIEuAK9MAEB6ALa4AIBkAKcsAAFoAAIABgAAEAEBYlNFRwCsABIR BwkNDBUZGRsTFB0QEA8VGw0KHRoaEBoPDxYUFRwaCAYTFQIADBcdDwwKBAEBAhQZHB0TGQQFDRcB BRAWFxYaFxIdGhYcEA4LER0UGw8XExsDChwPEhwKCBcKHRYXCBwXEhARHBgLAQAREBAXFggSGgwI DQMCBRYGBAIIAA0IGgwRGhgOHRccDBwWDBYXBgwDEg8GBwYADA8aDREPCgADARwNCw0UAwoGBgkD AgsMAAcPCAwGCgIDBAMAChYIAgAFAAkEABMDCwMIBxUDDhwDCAsKHAo8FgYCGQQICQscERYNABsE CgEYEykDEAYLFBUEEhccCBwsTGBQRFw4NFAQODBsDAgkXAAMFCAEOGhMEGQEOFxUBDhIbARYAGBUL FQ4dDhEUDRYHGAMZERsFAQcYGRgNCgcWCRUFCxIBCQoJDhMYGwsbBQcYHAUIDwkDBwsEEAkdCREJ

Figure 2.8. AES Fingerprint Template Decryption

2.13 Conclusion

In this chapter, this study introduced biometric systems then progressed to identify biometric attacks and threats in existing literature. It was then establihed from existing literature that most of biometric attacks target the biometric template. Thereafter, the study determined vulnerabilities that biometric templates are exposed to as a result of these attacks and continued to explore the 'Type 6' attack on biometric templates which is the attack of biometric templates in databases. The various biometric template protection techniques falling under feature transformation and cryptosystems were explored to identify their strengths and drawbacks. Finally, features of an ideal biometric template technique as defined in existing literature were discussed. The study then explored AES algorithm in details and explained how Encryption and Decryption works in this algorithm. This study chose to use AES 256 algorithm over AES 128 or AES 192 because of its strength and ability to resist against foreseable future quantum and brute force attacks. The study then illustrated with examples how to encrypt and decrypt biometric fingerprint templates using AES. In the following chapter the study discusses the research methodology used to determine attacks experienced in biometric systems by biometric system developers and establish status of affairs of the current biometric template protection techniques, their usage and how efficient they are by conducting a survey and analyzing data gathered.

CHAPTER THREE

RESEARCH METHODOLOGY

3.1 Introduction

This chapter defined study population, sampling technique, sample size, research instrument and data analysis. Questionnaires used to collect data for analysis and discussion consisted of open ended and closed ended questions. Closed ended questions were comprehensive and equally exclusive to eschew ambiguity of amassed data in scenarios of non-conforming select option questions answered by respondents.

3.2 Research Design

The research adopted the survey research design because it is extensive and it can be used to get an accurate sample from which to gather targeted results. Survey research is flexible for online surveys as well as for collecting data for later analysis and for administration of the questionnaire through an internet page hosted on a web server such that the respondents can visit the website and their responses are captured in real time (Devlin, 2006).

3.3 Study Population

The target population in this research constituted of all biometric software developers who currently are in the roles of developing biometric software systems or integrating biometrics into information systems and persons who work or have worked as biometric systems developers in biometric projects in Kenya. The study targeted a population of 390 biometric software developers who could be reached online and online questionnaires were distributed to them. This population was representative of respondents required for survey conducted by the study.

3.4 Sample Size and Sampling Technique

The study was based on a sample size of seventy-eight (78) biometric systems developers. The response rate was 83 but 5 questionnaires were rejected as they were not correctly filled by respondents leading the research to choose 78 of them. The sample size of 78 is approximately 20% of the representative target population which is reliable for data analysis and testing for levels of significance in correlations carried out (Westland, 2010). This study employed simple random sampling. The study opted to utilize this method over other random sampling methods because it provisioned for an equal likelihood of a biometric software developer from the study population being included. Individuals in a simple random sampling technique have the same probability of being chosen at any stage in a simple random sampling process as is evidenced in (Yates & Moore, 2008).

3.5 Research Instrument and Data Analysis Tools

Questionnaires were selected because they enabled the researcher to collect standardized data from biometric systems developers which was ready for statistical analysis of responses. The researcher administered Questionnaires to collect data from respondents. Questionnaires were tailored to capture data pertinent to the research's objective and research questions. This study utilized Statistical Package for Social Sciences (SPSS) software for data analysis and interpretation. The researcher chose to use SPSS as it offered a wide range of basic, advanced statistical and analytical techniques for processing data gathered from sampled respondents (Coakes & Steed, 2009).

3.6 Conclusion

This chapter discussed the methodology upon which this study was conducted. The Research design, study population, sampling technique, research instruments and data analysis tools used in the study are described and explained. The survey's result findings were used to compare, contrast and augment validity of existing literature assertions and to establish the current status of affairs as pertains to biometric fingerprint template protection techniques in existence and to inform this research

study to develop an ideal biometric fingerprint template protection technique that provides optimized security features for biometric fingerprint templates archived in databases. The following chapter will present, interpret and analyze data collected.

CHAPTER FOUR

DATA ANALYSIS AND DISCUSSIONS

4.1 Introduction

This chapter presents result findings from conducted survey. The analysis of collected data was based on frequency and cross-tabulation statistical analysis methods which made it possible to establish the correlations between different values of variables and their exceeding probabilities (Frink, 2006). Questionnaire used in the study comprised of these (4) sections;

Section A: Comprised of biometric systems developers' background.

This section gathered basic data about biometric systems developers and sought to determine their conceptions about impediments preventing wide scale adoption of biometrics.

Section B: Sought to ascertain biometric systems developers' experience in biometrics security.

This section was used to determine biometric developers' understanding, skills and competence in biometric security and use them for correlation of data variables in the study.

Section C: Targeted to establish efficiency of encryption methods.

This research sought to determine strengths and vulnerabilities of existing biometric encryption methods in this section for comparison with the proposed biometric encryption technique.

Section D: Sought to establish biometric templates security challenges.

In this section the research wanted to determine how the type of attacks experienced in biometric systems inform other known attacks in existing literature while determining the prevalent attacks on biometric systems.

4.2 Biometric Systems Developers' Background

Biometric systems developers' particulars and pertinent data based on their experience with biometrics systems were captured in this section. These details included gender, age, years of experience as biometric systems developers, type of biometric systems developed, if they had undertaken studies in biometric systems development, knowledge in data encryption and what their conceptions were on impediments preventing wide scale adoption of biometrics.

4.2.1 Respondents Age

Data collected had the following statistics for the ages of the respondents. The age 20 years and below had 0(0%) entries, 3(3.8%) of the respondents were between 21-25 years, The age 26-30 years had 27(34.6%) respondents. 21 (26.9%) respondents were in the age bracket 31-35 years and 27 (34.6%) were of age 35 years and above. This data is shown in Table 41 below.

Age of respondents in years	No. of Respondents	No. of Respondents in percentage (%)
21 - 25	3	3.8%
26 - 30	27	34.6%
31 - 35	21	26.9%
35 and above	27	34.6%
Total	**78**	**100.0**%

Table 4.1. Statistics of Respondents Age

4.2.2 Respondents who have studied Biometric Systems Development

Data collected revealed that 46 (59.0%) of respondents had undertaken studies or a course in biometric systems development while 32(41.0%) were active biometric systems developers without any particular training in the field. These statistics are tabulated in Table 4.2.

Studied Biometric Systems Development	No. of Respondents	No of respondents in percentage (%)
Yes	46	59.0%
No	32	41.0%
Total	**78**	**100.0**%

Table 4.2. Statistics of Respondents who have studied Biometric Systems Development

4.2.3 Respondents' Experience as Biometric Systems Developers

From the data collected, 52 (66.7%) of the respondents had 1-5 years of experience as biometric systems developers, 19 (24.4%) had experience of 6-10 years. While only 5 (6.4%) respondents had 11-15 years of experience, only 2 (2.6%) had an experience of 16 years and above. This data is shown in detail in Table 4.3.

Experience in years as a Biometric Systems Developer	No. of Respondents	No of respondents in percentage (%)
1 - 5 years	52	66.7%
6 - 10 years	19	24.4%
11 - 15 years	5	6.4%
16 years and above	2	2.6%
Total	**78**	**100.0%**

Table 4.3. Statistics of Respondents Experience as Biometric Systems Developers

From the above statistics, it is evident that there are fewer respondents with increasing number of years of experience. Most of the respondents 52(66.7%) had an experience of 1-5 years.

4.2.4 Type of Biometric Systems Developed

Data collected indicated 64(82.1%) or respondents had experience developing fingerprint systems, 43(55.1%) had developed face recognition systems while 16 (20.5%) had been developing iris systems. A further 14 (17.9%) had experience developing voice recognition systems and 7 (9.0%) had been developing palm vein recognition systems. 12 (15.4%) of respondents had experience developing other biometric systems which included *online signature, finger vein and score level fusion of face and fingerprints*. This data is shown in Table 4.4. A previous study by Seung-hwan et al., (2013) showed that fingerprints are the most widely developed 'user knowledge-based' authentication because they are easy to implement.

Type of Biometric Systems Developed	No. of Respondents	Total No. of Respondents	No of respondents in percentage (%)
Fingerprint	64	78	82.1%
Face	43	78	55.1%
Iris	16	78	20.5%
Voice	14	78	17.9%
Palm Vein Recognition	7	78	9.0%
Other(s)	12	78	15.4%
Total		**78**	**100.0%**

Table 4.4. Statistics of Type of Biometric Systems Developed

Table 4.5. Shows statistics of respondents who develop one or more than one biometric systems. From the data collected, it is depicted that most of the biometric systems developers could develop two or more biometric systems with 32(41.0%) the majority having experience of developing fingerprints and face systems. In few scenarios were respondents only experienced in developing only one type of biometric system as shown in the Table 4.5 below where 3(3.8%) developed face systems only, 4(5.1%) developed fingerprint systems only, 1(1.3%) developed iris only and 1(1.3%) developed voice only. There was no scenario observed where a respondent‘s expertise was based on developing palm vein recognition systems only.

Biometric Systems Developed by Respondents	No. of Respondents	No. of respondents in percentage (%)
Face	3	3.8%
Face, Iris	4	5.1%
Face, Palm Vein Recognition	1	1.3%
Face, Score level fusion of face and fingerprint	1	1.3%
Face, Voice	1	1.3%
Fingerprints	4	5.1%
Fingerprints, Face	32	41.0%
Fingerprints, Face, Iris, Palm Vein Recognition	1	1.3%
Fingerprints, Finger vein	1	1.3%
Fingerprints, Iris	10	12.8%
Fingerprints, Palm Vein Recognition	6	7.7%
Fingerprints, Voice	10	12.8%
Iris	1	1.3%
Iris, Voice	1	1.3%
Voice	1	1.3%
Voice, online signature	1	1.3%
Total	**78**	**100.0**%

Table 4.5. Statistics of Respondents who Develop One or More Biometric Systems

4.2.5 Biometric Systems are more secure than passwords, PINs or access codes

It was evident from collected data that 66(84.6%) of respondents considered biometrics to be more secure than passwords, PINs or access codes while the remainder 12(15.4%) were of the contrary opinion an indicator that biometrics were considered more secure than conventional methods of identification in information systems. Jain et al., (2004) support these findings as they vouched their support for increased use of biometrics over passwords, secret tokens, PINs or any kind of passwords that can be easily compromised. These findings are shown in Table 4.6 below.

Biometrics Provide more Security than PINs, access codes & passwords	No. of Respondents	No. of Respondents in Percentage (%)
Yes	66	84.6%
No	12	15.4%
Total	**78**	**100.0%**

Table 4.6. Statistics showing results of use of Biometrics over pins, access codes & passwords

4.2.6 Respondents' Experience in Data Encryption

Respondents' knowledge in data encryption was captured in data collection to determine their level of expertise in securing data with encryption to prevent adversary attacks on archived data.

Respondents Knowledge in Data Encryption	Score Level Weights	No. of Respondents	No. of Respondents in Percentage (%)
Excellent	5	14	17.9%
Above Average	4	31	39.7%
Average	3	28	35.9%
Poor	2	5	6.4%
Very Poor	1	0	0.0%
	Mean=3.63	**Total =78**	**Total =100.0%**

Table 4.7. Statistics of Respondents Knowledge in Data Encryption

Respondents' knowledge in data encryption as shown above in Table 4.7 illustrated that 14(17.9%) of respondents considered their knowledge in data encryption as excellent, 31(39.7%) respondents ranked above average while 28(35.9%) respondents data encryption knowledge was ranked as poor. None of the respondents in the data collected thought their data encryption skills fared very poorly. The overall mean for the rankings of respondents' data encryption knowledge was 3.63 which is slightly more than average tending to above average and a good pointer that more than average number of biometric developers lay emphasis on security of data.

4.2.7 Impediments Towards wide scale adoption of Biometric Systems

From data collected, impediments preventing wide scale adoption of biometric systems, *high costs of biometric hardware & software* was the main reason identified by respondents at 53(67.9%) followed by 41(52.6%) of respondents who cited lack of expertise to develop, implement & support biometric systems. 31(39.7%) of respondents were of the opinion that accuracy of biometric identification systems was a contributing factor while sizably voluminous data size of biometric templates and

known security flaws were singled out by 15(19.2%) and 10(12.8%) of respondents respectively. Other impeding factors identified by the remainder of 18 (23.1%) of respondents were *verification & identification time, low bandwidth because of the immensely colossal size of biometric data, users' unwillingness to give out their biometric data alluding security concerns and trust*. This data is presented in Table 4.8 and Table 4.9.

Impediments Towards Wide Scale Adoption of Biometric Systems	No. of Respondents	Total No. of Respondents	No. of Respondents in Percentage (%)
High Costs of Biometric Hardware & Software	53	78	67.9%
Known Security Flaws	10	78	12.8%
Lack of Expertise to Develop, Implement & Support Biometrics Systems	41	78	52.6%
Accuracy (False Acceptance Rate and False Rejection Rate)	31	78	39.7%
Big data size of Biometric Templates in storage space	15	78	19.2%
Other(s)	18	78	23.1%
Total		**78**	**100.0%**

Table 4.8. Statistics of Impediments that delay wide scale adoption of Biometric Systems

In order to show respondents who selected one or more impediments as contributing factors to delayed adoption of biometrics, this key was used to represent data collected in Table 4.9.

Key:

Cost	: High Costs of Biometric Hardware & Software
Security	: Known Security Flaws
Expertise	: Lack of Expertise to Develop, Implement & Support Biometrics Systems
Accuracy	: Accuracy (False Acceptance Rate and False Rejection Rate)
Data	: Big data size of Biometric Templates in storage space
Other	: Other(s)

Impediments Towards Wide Scale Adoption of Biometric Systems	No. of Respondents	No. of Respondents in Percentage (%)
Accuracy	6	7.7%
Accuracy; Data	1	1.3%
Costs	7	9.0%
Costs; Accuracy	10	12.8%
Costs; Data	3	3.8%
Costs; Security	1	1.3%
Costs; Security; Data	1	1.3%
Costs; Security; Expertise	3	3.8%
Costs; Security; Expertise; Data	1	1.3%
Costs; Expertise	18	23.1%
Costs; Expertise; Accuracy	3	3.8%
Costs; Expertise; Accuracy; Data	3	3.8%
Costs; Expertise; Data	3	3.8%
Security; Accuracy	2	2.6%
Security; Expertise	1	1.3%
Security	1	1.3%
Expertise	4	5.1%
Expertise; Accuracy	5	6.4%

Other	5	6.4%
Total	**78**	**100.0%**

Table 4.9. Statistics of One or More Biometric Systems' Implementation Impediments

The data presented in Table 4.9. reveals that the greatest number of respondents 18(23.1%) specified High costs of biometric software & Hardware coupled with Lack of Expertise to Develop, Implement & Support Biometric Systems as being the leading factors impeding wide scale adoption of biometric systems. High costs and expertise required to implement biometric systems have been the leading factors delaying incorporation of biometrics into information security systems as evidenced by Das (2012).

To determine correlation amongst *Age of Respondents*, *Respondents Biometric Experience*, *If Respondent has pursued a Biometric Course*, *if biometric are more secure than PINs*, *Passwords & access codes* and *Respondents Knowledge in Data Encryption*, correlation analysis was done and results shown in Table 4.10. The following correlations were significant in this study. They were as follows;

Correlation between Age of Respondents and Respondent's Experience as Biometrics Developer,

Correlation between Biometric Course and Respondent's Experience as Biometrics Developer,

Correlation between Encryption Knowledge and Respondent's Experience as Biometrics Developer,

Correlation between Biometric Course and Data Encryption Knowledge.

		Age of Respondents	Respondent's Experience as a biometric system's developer	If Respondent has taken any Biometric course or Studies	If biometrics more secure than PINs, access codes & passwords	Respondent's knowledge on Data Encryption
Age of Respondents	Pearson Correlation	1	.417**	-.072	.152	-.209
	Sig. (2-tailed)		.000	.530	.184	.066
	N	78	78	78	78	78
Respondent's Experience as a biometric system's developer	Pearson Correlation	.417**	1	-.264*	.030	-.232*
	Sig. (2-tailed)	.000		.020	.794	.041
	N	78	78	78	78	78
If respondent has taken any Biometric course or Studies	Pearson Correlation	-.072	-.264*	1	-.067	.372**
	Sig. (2-tailed)	.530	.020		.562	.001
	N	78	78	78	78	78
If Biometrics more secure	Pearson Correlation	.152	.030	-.067	1	-.196

than PINs, access codes & passwords	Sig. (2-tailed)	.184	.794	.562		.085
	N	78	78	78	78	78
Respondent's knowledge on Data Encryption	Pearson Correlation	-.209	-.232*	.372**	-.196	1
	Sig. (2-tailed)	.066	.041	.001	.085	
	N	78	78	78	78	78
**. Correlation is significant at the 0.01 level (2-tailed).						
*. Correlation is significant at the 0.05 level (2-tailed).						

Table 4.10. Correlation Matrix

There is a **positive** Correlation of **0.417** with a ***p*** value of **0** between *Age of Respondents* and *Respondent's Experience as Biometric Systems Developer* implying that *Respondent's Experience as Biometric Systems Developer* increases as they get older.

There is a **negative** Correlation of **-0.264** with a ***p*** value of **0.020** between *If respondent has taken Biometric Course* and *Respondent's Experience as Biometric Systems Developer* a partial indicator that with increased respondents experience as biometric developers there is a marginal reduction in respondents who have formal studies in biometrics. Majority of the respondents who have more experience in developing biometric systems have not studied courses in biometrics. This correlation could maybe be attributed to there being fewer institutions training in biometrics or there being fewer or no known biometric courses.

There is a **negative** Correlation of **-0.232** with a ***p*** value of **0.041** between *Data Encryption Knowledge* and *Respondent's Experience as Biometric Systems Developer*. This a slight pointer that *when respondents experience as biometric systems developers increases, there is a small decrease in awareness of data encryption.* This phenomenon

however changes for respondents who have had formal studies in biometrics as shown in the next correlation below.

There is a **positive** Correlation of **0.372** with a ***p*** value of **0.001** between *Respondent's Data Encryption Knowledge* and *if Respondent has taken any Biometric course or Studies* a possible likelihood that, as more respondents study a course in biometrics, respondents become more erudite in data encryption.

4.3 Biometric Templates Security

This section sought to discover preferred area of storage for biometric templates, determine whether there are measures to protect biometric templates, ascertain if there are policies in place that put emphasis on securing of biometric templates in storage, then identify which biometric template protection techniques & methods are used and conclusively ascertain from respondents which biometric encryption schemes they utilized.

4.3.1 Biometric Templates Storage Space

Storage space for biometric templates was of importance to the researcher and this study sought to determine where respondents archive or save biometric templates i.e. storage space in biometric systems. Table 4.11 shows results from study as follows; 55(70.5%) of respondents saved their biometric templates in *databases* while only 1(1.3%) of respondent saved biometric templates in *USB modules*. 7(9.0%) of respondents chose *folders* and 10(12.8%) of respondents preferred *smart cards*. The remainder 5(6.4%) of respondents who identified *other* places listed the following storage places; *encrypted databases* and a coalescence of both *databases and smartcards*. According to (Jain et al, 2008) the potentially damaging attack on a biometric system is against the biometric templates stored in the system database signifying that most developers' save their biometric templates in a database in preference to other storage spaces as this study revealed.

Biometric Templates Storage Space	No. of Respondents	No. of Respondents Percentage (%)
Folders	7	9.0%
Databases	55	70.5%
Smart cards	10	12.8%
USB Modules	1	1.3%
Other(s)	5	6.4%
Total	**78**	**100.0%**

Table 4.11. Statistics of where Respondents save Biometric Templates

4.3.2 Respondents who take measures to Protect Biometric Templates

The researcher sought to determine if there were any measures aimed at protecting biometric templates from the sampled respondents and this study showed that 66(84.6%) of respondents had measures in place while 12(15.4%) of respondents did not. These findings are shown in Table 4. 12 below.

Are there Measures in place to Protect Biometric Templates	No.of Respondents	No. of Respondents Percentage (%)
Yes	66	84.6
No	12	15.4
Total	**78**	**100.0**

Table 4.12. Statistics to show if Respondent has Measures to Protect Biometric Templates

4.3.3 Policies aimed at Protecting Biometric Templates in Storage

To further investigate the magnitude with which security of biometric templates is put into consideration the researcher inquired from the respondents whether there were any policies in their organizations governing security of biometric templates. The results presented in Table 4.13 showed that 61(78.2%) of respondents had policies in place while 17(21.8%) of respondents admitted they did not have any governing policies in place.

Are there Biometric Templates Security Policies	Respondents	No. of Respondents Percentage (%)
Yes	61	78.2%
No	17	21.8%
Total	**78**	**100.0%**

Table 4.13. Statistics showing if there are Biometric Templates Security Policies

Observing that 17(21.8%) of respondents in Table 4.13 did not have policies to mitigate biometric templates attacks, asked what measures they had in place to counter Biometric template attacks in storage the researcher established that the following practices were used; *matching live finger again, file access permissions were established in linux, cryptologic tools, servers without external access were used, databases were password protected and database access permissions were regulated or denied.*

4.3.4 Biometric Templates Protection Techniques

The researcher narrowed further down from determining whether there were measures and policies in place targeted at protecting biometric templates to ascertaining which template protection techniques respondents used. It was established that 39(50%) of respondents used *Biometric Encryption Technique* to secure biometric templates while

16(20.5%) of respondents made use of *Feature Transformation Technique*. 23(29.5%) of respondents did not use any biometric template protection techniques leaving them exposed to experiencing biometric template attacks in their biometric systems. Even though in this study most of the respondents i.e. 39(50%) indicated that they preferred to use Biometric Encryption to 16 (20.5%) of respondents who would use Feature Transformation, a survey done by Rathgeb and Uhl (2011) indicated that there are no competing interests in the two main categories of biometric template protection techniques. These statistics are presented in Table 4.14.

Biometric Template Protection Technique	No. of Respondents	No. of Respondents Percentage (%)
Feature Transformation	16	20.5%
Biometric Encryption	39	50.0%
None	23	29.5%
Total	**78**	**100.0%**

Table 4.14. Statistics for Biometric Templates Protection Techniques Used

4.3.5 Biometric Encryption Techniques and Schemes

From Table 4.14, it was established that the majority of respondents 39(50.0%) had indicated that they used *Biometric Encryption* technique. The researcher determined from the study that of the two methods *Key Binding* and *Key Generation* found in *Biometric Encryption Technique* that 16(20.5%) of respondents used *Key Binding* while 23(29.5%) used *Key Generation*. From these results also presented in Table 4.15 it is evident from this study that *Key Generation* method is the most prevalent *Biometric Encryption* method than *Key Binding*. This is supported in (Maniroja & Sawarkar, 2013) where it is apparent that there is more security with generating

encryption keys than binding encryption keys while securing data from images though another study by Cheol-Joo et al., (2014) opined that key generation algorithms are not popular because biometric features differ every time they are captured even from the same fingerprint.

Biometric Encryption Methods	No. of Respondents	No. of Respondents Percentage (%)
Key Binding	16	20.5%
Key Generation	23	29.5%
Total	**78**	**100.0%**

Table 4.15. Statistics for Biometric Encryption Methods Used

The current biometric encryption schemes used to protect biometric templates were explored. It was required for respondents to identify the schemes they had used to protect biometric templates. From the data collected and tabulated in Table 4.16. it is shown that 10(12.8%) of respondents had used *Fuzzy Vault,* 6(7.7%) of respondents had used *Water Marking*, 40(51.3%) had used *RSA & ECC* and 9(11.5%) indicated they had used *Fuzzy Commitment* and 12(15.4%) specified they had used *Cancellable Biometrics.* 22(28.2%) of respondents indicated that they did not use any *biometric encryption schemes* while 4(5.1%) of respondents indicated that they used other *biometric encryption schemes.* The other schemes specified by respondents included *private encryptions, AES 128* and others were bound by security company policies that prevented them from divulging the encryption schemes they used. The results of the *Biometric Encryption Schemes* used by respondents are shown in Table 4.16.

Biometric Encryption Schemes	No. of Respondents	Total No. of Respondents	No of respondents in percentage (%)
Fuzzy Vault	10	78	12.8%
Water Marking	6	78	7.7%
RSA and ECC	40	78	51.3%
Fuzzy Commitment	9	78	11.5%
Cancellable Biometrics	12	78	15.4%
None	22	78	28.2%
Other(s)	4	78	5.1%

Table 4.16. Statistics of Biometric Encryption Schemes used Under Key Generation Method

4.4 Efficiency of Encryption Methods

This section was significant in reviewing efficiency of biometric encryption methods used to protect biometric fingerprint templates. It consisted of the following subsections; Views of respondents on efficiency of encryption methods they used, Encryption keys and biometric templates storage space, Practices improving biometric encryption, Encrypting data with biometric encryption keys derived from fingerprint templates, Biometric encryption keys' entropy strength, Biometric encryption keys future use in data encryption.

4.4.1 Biometric Systems Developers views on Efficiency of Encryption Methods Used

This section was a basis for determining from respondents if there were risks of hacking biometric encryption methods used to secure biometric templates. This study established that 10(12.8%) of respondents *Strongly Disagreed*, 31(39.7%) of respondents *Disagreed*, 22(28.2%) of respondents *Agreed* while 5(6.4%) *Strongly Agreed* and 10(12.8%) neither agreed nor disagreed to any extent and were categorized as *Neutral*. These findings are presented in Table 4.17.

There is Risk of Hacking Biometric Systems in the Encryption Method Used	No. of Respondents	No of respondents in percentage (%)
Strongly Disagree	10	12.8%
Disagree	31	39.7%
Neutral	10	12.8%
Agree	22	28.2%
Strongly Agree	5	6.4%
Total	**78**	**100.0%**

Table 4.17. Statistics showing if there is Risk of Hacking Biometric Encryption Method Used

This section determined from respondents whether encryption methods used to secure biometric templates were considered fool proof. The study established that 7(9.0%) of respondents *Strongly Disagreed*, 19(24.4%) of respondents *Disagreed*, 19(24.4%) of respondents *Agreed* while 9(11.5%) *Strongly Agreed* and 24(30.8%) neither agreed

nor disagreed to any extent and were categorized as *Neutral*. These findings are presented in Table 4.18.

The Encryption Methods Used by Respondent are Fool Proof	No. of Respondents	No of respondents in percentage (%)
Strongly Disagree	7	9.0%
Disagree	19	24.4%
Neutral	24	30.8%
Agree	19	24.4%
Strongly Agree	9	11.5%
Total	**78**	**100.0**%

Table 4.18. Statistics showing if Encryption Methods used by Respondent are Fool Proof

This study sought to determine from this section if encryption methods used were satisfactory in securing biometric data. The study established that 5(6.4%) of respondents *Strongly Disagreed*, 15(19.2%) of respondents *Disagreed*, 31(39.7%) of respondents *Agreed* while 12(15.4%) *Strongly Agreed* and 15(19.2%) neither agreed nor disagreed to any extent and were categorized as *Neutral*. These findings are presented in Table 4.19.

Biometric Template Encryption Method used is Satisfactory	No. of Respondents	No of respondents in percentage (%)
Strongly Disagree	5	6.4%
Disagree	15	19.2%
Neutral	15	19.2%
Agree	31	39.7%
Strongly Agree	12	15.4%
Total	**78**	**100.0%**

Table 4.19. Statistics of Respondents whose Biometric Encryption Method is satisfactory

Results for Mean, Median and Mode of Efficiency of Encryption Methods used were presented in Table 4.20. The mode for if there is risk of hacking biometric systems in Encryption Method used is **2** whose equivalent is *Disagree*. The greater percentage of respondents *Disagreed* that there is risk of hacking biometric systems based on Encryption Method used implying that they believed their biometric encryption method was not so exposed to the risk of hacking.

	if there is risk of hacking biometric systems in Encryption Method Used	if biometric encryption methods are fool proof	if biometric template security is satisfactory in Encryption Method Used
N	78	78	78
Mean	2.76	3.05	3.38
Median	2.00	3.00	4.00
Mode	2 (Disagree)	3 (Neutral)	4 (Agree)

Table 4.20. Mean, Median and Mode of Efficiency of Encryption Methods

The mode for *if biometric encryption methods are fool proof* is **3** whose equivalent is Neutral. The greater percentage of respondents were not sure whether *biometric encryption methods they used were fool proof* implying that they did not really doubt or consider them to be insecure.

The mode for *if biometric template security is satisfactory in Encryption Method used* is **4** whose equivalent is Agree. The greater percentage of respondents agreed that biometric template security is satisfactory based on the Encryption Method they used implying that they believed the biometric encryption method they used provided satisfactory security on biometric templates of the biometric systems they developed.

			if there is risk of hacking biometric systems in Encryption Method Used	if biometric encryption methods are fool proof	if biometric template security is satisfactory in Encryption Method Used
Spearman's rho	if there is risk of hacking biometric systems in Encryption Method Used	Correlation Coefficient	1.000	-.223	-.376**
		Sig. (2-tailed)	.	.050	.001
		N	78	78	78
	if biometric encryption methods are fool proof	Correlation Coefficient	-.223	1.000	.322**
		Sig. (2-tailed)	.050	.	.004
		N	78	78	78
	if biometric template security is satisfactory in Encryption Method Used	Correlation Coefficient	-.376**	.322**	1.000
		Sig. (2-tailed)	.001	.004	.
		N	78	78	78

**. Correlation is significant at the 0.01 level (2-tailed).

Table 4.21. Correlations of Encryption Methods based on their Efficiencies

Spearman's rho was used to find correlations between encryption methods efficiencies because the rating scale was ordinal. The correlations presented in Table 4.21, are described as follows;

There is a **negative** Correlation of **-0.376** with a **p** value of **0.001** between *if there is risk of hacking biometric systems in Encryption Method used* and *if biometric template security is satisfactory in Encryption Method used* implying that the risk of hacking biometric systems based on biometric encryption method used *increases* when the encryption method's efficiency *reduces* and is not satisfactory.

There is a **positive** Correlation of **0.322** with a **p** value of **0.001** between *if biometric encryption methods are fool proof* and *if biometric template security is satisfactory in Encryption Method used* implying that if biometric encryption method *excels* in being fool proof then the encryption method's efficiency *increases* and is considered satisfactory.

4.4.2 Encryption Keys and Encrypted Biometric Templates Storage Space

The researcher observed that 65(83.3%) of respondents would not want to keep encryption keys in the same storage space with Encrypted Biometric Templates. 13(16.7%) of respondents would on the contrary keep encryption keys together with encrypted biometric templates in the same storage space i.e. folder, database or USB. From the findings of the study it is evident that the respondents are cautious about storing encryption keys in the same storage space with biometric templates an indicator that they are aware about the security concerns of preventing extraction of encryption keys as is cautioned by Das (2012). The tabulated findings are shown in Table 4.22. The objective of a biometric system developer would be to make it hard for an adversary to decode biometric data in a biometric system by keeping biometric encryption keys in a different location away from encrypted biometric data. In the proposed biometric encryption and decryption tool, biometric encryption keys have to be derived from biometric fingerprint templates in order for the decryption tool to advance to the second step of verification or identification.

Would Respondents keep Encryption Keys in same storage space with Encrypted Biometric Templates?	No. of Respondents	No. of Respondents Percentage (%)
Yes	13	16.7%
No	65	83.3%
Total	78	100.0%

Table 4.22. Statistics of Respondents who would keep Encryption Keys in the same archiving space with Encrypted Biometric Templates

4.4.3 Practices improving Biometric Encryption

Practices Improving Biometric Encryption	No. of Respondents	Total No. of Respondents	No of Respondents in percentage (%)
Improving Image Acquisition Process	36	78	46.2%
Making Biometric Encryption Resilient against attacks	31	78	39.7%
Improving Accuracy and Security of Biometric Encryption Algorithms	52	78	66.7%
Use of Multimodal Biometrics	38	78	48.7%
Other(s)	3	78	3.8%

Total	**78**	**100.0%**

Table 4.23. Statistics of Practices Biometric Encryption

Key:

Image Acquisition : Improving Image Acquisition Process

Multimodal : Use of Multimodal Biometrics

Resilient to Attacks : Making Biometric Encryption Resilient against attacks

Encryption Apps : Develop Biometric Encryption Applications

Accuracy & Security : Improving Accuracy and Security of Biometric Encryption Algorithms

Other(s) : Other(s)

Combination of Best Practices Improving Biometric Encryption	No. of Respondents	No of Respondents in percentage (%)
Encryption Apps	2	2.6%
Accuracy & Security	5	6.4%
Accuracy & Security, Encryption Apps	3	3.8%
Accuracy & Security, Multimodal	8	10.3%
Image Acquisition	3	3.8%
Image Acquisition, Encryption Apps	1	1.3%

Image Acquisition, Accuracy & Security	8	10.3%
Image Acquisition, Accuracy & Security, Encryption Apps	1	1.3%
Image Acquisition, Accuracy & Security, Multimodal	2	2.6%
Image Acquisition, Accuracy & Security, Multimodal, Encryption Apps	1	1.3%
Image Acquisition, Resilient to Attacks	2	2.6%
Image Acquisition, Resilient to Attacks, Accuracy & Security	2	2.6%
Image Acquisition, Resilient to Attacks, Accuracy & Security, Encryption Apps	1	1.3%
Image Acquisition, Resilient to Attacks, Accuracy & Security, Multimodal	2	2.6%
Image Acquisition, Resilient to Attacks, Accuracy & Security, Multimodal, Encryption Apps	6	7.7%
Image Acquisition, Resilient to Attacks, Multimodal	1	1.3%
Image Acquisition, Multimodal	5	6.4%
Image Acquisition, Multimodal, Encryption Apps	1	1.3%
Resilient to Attacks	2	2.6%
Resilient to Attacks, Encryption Apps	2	2.6%
Resilient to Attacks, Accuracy & Security	5	6.4%

Resilient to Attacks, Accuracy & Security, Encryption Apps	2	2.6%
Resilient to Attacks, Accuracy & Security, Multimodal	4	5.1%
Resilient to Attacks, Accuracy & Security, Multimodal, Encryption Apps	2	2.6%
Multimodal	4	5.1%
Multimodal, Encryption Apps	2	2.6%
Other(s)	3	3.8%
Total	**78**	**100.0**%

Table 4.24. Statistics of Combination of Practices Improving Biometric Encryption

4.4.4 Encrypting Data with Biometric Encryption Keys Derived From Fingerprint Templates

The study sought to establish whether respondents considered *encryption of data using encryption keys derived from biometric fingerprint templates* a feasible idea. The results shown in Table 4.25 revealed that 48 (61.5%) of respondents believed it would be achievable while 30(38.5%) declined. These results exposed that 48 (61.5%) of respondents would encrypt data with encryption keys derived from biometric fingerprints if they had a way to derive encryption keys from fingerprints however for the 30 (38.5%) who would not derive entropy from biometric fingerprints could have been because they did not think it was possible to derive strong and unvarying encryption keys from fingerprints. Their reservations are not farfetched because the noisy nature of biometrics yields different variations of the same fingerprint even in repeated fingerprint image captures (Cheol-Joo et al., 2014) .

If Respondent would Encrypt Data with Biometric Encryption Keys Derived From Fingerprint Templates	No. of Respondents	No. of Respondents Percentage (%)
Yes	48	61.5%
No	30	38.5%
Total	**78**	**100.0%**

Table 4.25. Statistics of Respondents who believed Encryption Keys Derived from Fingerprint templates could be used to protect data in storage

4.4.5 Biometric Encryption Keys Rich and Strong in Entropy

The study sought to establish whether respondents believed encryption keys derived from biometric templates would be rich in entropy for encrypting data than a combination of passwords and access codes. This study revealed that 72 (92.3%) of respondents thought encryption keys derived from biometrics would provide rich entropy than passwords and access codes. 6 (7.7%) of respondents were not convinced and when asked why, they explained that; *there would be overlaps in combination of keys from biometric templates if there were more people* and *strength of security keys is depended on quality of biometrics implying poor samples would result in lower strength of encryption keys.* These findings are presented in Table 4.26.

If Encryption Keys Derived from Biometrics would be Rich and Strong in Entropy	No. of Respondents	No. of Respondents Percentage (%)
Yes	72	92.3%
No	6	7.7%
Total	**78**	**100.0%**

Table 4.26. Statistics of Respondents who Think Encryption Keys Derived from Biometrics would be Rich and Strong in Entropy

4.4.6 Biometric Encryption Keys Future Use in Data Encryption

The study revealed that 62(79.5%) of respondents agreed that in the foreseeable future encryption of data using biometric encryption keys will become a prevalent practice among systems developers. 16(20.5%) of respondents did not think it would be possible. This research sought to estimate respondents' prospects of future trends of biometric encryption security in this section. These findings are shown in Table 4.27.

Does it seem feasible in the near future for Entropy to be Derived from Biometrics and used in Data Encryption?	No. of Respondents	No. of Respondents Percentage (%)
Yes	62	79.5%
No	16	20.5%
Total	**78**	**100.0%**

Table 4.27. Statistics of Respondents who Foresee Use Of Entropy from Biometrics in Data Encryption

4.5 Biometric Templates Security Challenges

This section sought to establish if respondents faced security challenges with regards to biometric template security then determine biometric attacks encountered and discover if biometric templates storage areas had been compromised. The study additionally sought respondents' opinions on whether they considered databases as the most ideal preference for biometric templates storage and why they would not choose databases for biometric templates storage. Finally, the section investigates options respondents would utilize to ascertain biometric templates are safely stored in databases.

4.5.1 Challenges Pertaining to Biometric Template Security

From the data collected, 15 (19.2%) of respondents agreed to having encountered challenges related to biometric templates security while 63 (80.8%) did not. The respondents who admitted to having faced biometric template security issues were asked to specify in particular which challenges they experienced and they listed the following; *data theft from customer locations, difficulty in guaranteeing high accuracy levels while ensuring security levels are upheld, biometric templates modifications, leaking of biometric template information to unauthorized users, encryption keys being based on combination of passwords possibly known to adversaries, difficulty in generating random chaff surrounding biometric features in mobile devices due to limited processing resources* and *non-secure infrastructure.* Table 4.28 shows these statistics.

Are there challenges encountered in Biometric Template Security?	No. of Respondents	No. of Respondents Percentage (%)
Yes	15	19.2%
No	63	80.8%
Total	**78**	**100.0%**

Table 4.28. Statistic of Challenges Encountered in Biometric Template Security

4.5.2 Types of Biometric Attacks Encountered

The major attacks waged on biometrics templates by adversaries in biometric systems were; *spoofing* which is the fooling of biometric system by using fake finger, face or iris templates. It ranked as the most encountered attack reported by 43(55.1%) of respondents followed by *Tampering* at 20 (25.6%).

Tampering is where biometric attackers modify biometric feature sets to obtain high verification scores. *Trojan* attacks which entail the replacing of the biometric matcher programs with ones that always allow access were identified as the third most recurring attacks on biometric templates being identified by 19 (24.4%) of respondents.

Replay attacks where biometric system sensors are circumvented by running pre-saved biometric templates and *Substitution attacks* which involve replacing of users' biometric templates with those of adversaries each had 17 (21.8%) of respondents identifying them respectively.

A further 12 (15.4%) of respondents did not encounter any biometric attacks as they specified *none* in the *other* select option. These results agree with the assertion in (Brindha, 2012) that the major significant attack in a biometric system is spoofing of biometric templates in a biometric system database. These figures are presented in Table 4.29 and Table 4.30.

Biometric Attacks Encountered	No. of Respondents	Total No. of Respondents	No of Respondents in percentage (%)
Spoofing	43	78	55.1%
Replay Attacks	17	78	21.8%
Substitution Attacks	17	78	21.8%
Tampering	20	78	25.6%

Trojan Attacks	19	78	24.4%
None	12	78	15.4%
Total		**78**	**100.0%**

Table 4.29. Statistics of Biometric Attacks Encountered

Combination of Biometric Attacks Encountered	No. of Respondents	No of Respondents in percentage (%)
Replay attacks	3	3.8%
Replay attacks, Substitution attacks	1	1.3%
Replay attacks, Tampering	1	1.3%
Replay attacks, Trojan attacks	1	1.3%
Spoofing	24	30.8%
Spoofing, Replay attacks	2	2.6%
Spoofing, Replay attacks, Substitution attacks	2	2.6%
Spoofing, Replay attacks, Substitution attacks, Tampering	2	2.6%
Spoofing, Replay attacks, Substitution attacks, Tampering, Trojan attacks	3	3.8%

Spoofing, Replay attacks, Tampering, Trojan attacks	1	1.3%
Spoofing, Replay attacks, Trojan attacks	1	1.3%
Spoofing, Substitution attacks	1	1.3%
Spoofing, Substitution attacks, Tampering	1	1.3%
Spoofing, Substitution attacks, Trojan attacks	1	1.3%
Spoofing, Tampering	3	3.8%
Spoofing, Trojan attacks	2	2.6%
Substitution attacks	2	2.6%
Substitution attacks, Tampering	2	2.6%
Substitution attacks, Tampering, Trojan attacks	2	2.6%
Tampering	3	3.8%
Tampering, Trojan attacks	2	2.6%
Trojan attacks	6	7.7%
Other(s)	12	15.4%
Total	**78**	**100.0**

Table 4.30. Statistics of Biometric Attacks Encountered

4.5.3 Biometric Templates Storage Space Compromised

Other than investigating types of biometric attacks experienced by respondents, the research established that 2 (2.6%) of respondents had their biometric template storage space compromised implying that adversaries not only attacked biometric templates but also attacked biometric storage space as well. 76 (97.4%) of respondents had not experienced any attacks on their biometric templates storage space. The Table 4.31 shows these results below.

Biometric Template Storage Space ever been Compromised?	No. of Respondents	No of Respondents in percentage (%)
Yes	2	2.6%
No	76	97.4%
Total	**78**	**100.0%**

Table 4.31. Statistics showing if Biometric Template Storage has ever been compromised

Information systems archive data in databases and since most biometric systems too store biometric templates in databases as well, the study established that 61 (78.2%) of respondents considered databases as the most ideal storage space for biometric templates while 17 (21.8%) of respondents did not. These figures are shown in Table 4.32. The respondents who would not opt for databases to store biometric templates cited *security concerns, long time taken to find template match* and *risks involved in central storage databases.* They would instead *save biometric templates in dedicated memory sticks, encrypted folders* and *smart cards using MOC technology.* Respondents suggested, *a secure device that the operating system is incapable of accessing* as a viable research area for researchers interested in researching about secure biometric template storage space.

Respondents using Databases as Ideal Template Storage Space	No. of Respondents	No of Respondents in percentage (%)
Yes	61	78.2%
No	17	21.8%
Total	**78**	**100.0%**

Table 4.32. Statistics of Respondents using Databases as Ideal Template Storage Space

4.5.4 Measures used to ensure Safe Storage of Biometric Templates in Database

The study determined that 59(75.6%) of respondents indicated that *Encrypting of Biometric Templates Before Saving Them in Database* would ensure safe storage of biometric templates in database, 50(64.1%) of respondents would rather *Reduce Levels of Access to Database* while 38(48.7%) and 36(46.2%) of respondents would *Use strong passwords* and *change database passwords often* respectively. 7(9.0%) of respondents who had selected *others* specified that they would *implement strong access control to database, use finger scans to access database, use data vaults, deploy database firewalls* and *implement audit software.* These data results are shown in Table 4.33 and Table 4.34.

Measures used to ensure Safe Storage of Biometric Templates in Database	No. of Respondents	Total No. of Respondents	No of Respondents in percentage (%)
Change Database Passwords often	36	78	46.2%
Use Strong Passwords	38	78	48.7%
Reduce Levels of Access to Database	50	78	64.1%
Encrypt Biometric Templates Before Saving them in Database	59	78	75.6%
Other(s)	7	78	9.0%
Total		**78**	**100.0%**

Table 4.33. Statistics of Measures ensuring Safe Biometric Templates in Database

Key:

Change DB passwd : Change Database passwords oftenly

Reduce DB access : Reduce levels of access to database

Strong passwd : Use strong passwords

Encrypt Bio Templates : Encrypt biometric templates before saving them in database

Other(s) : Other(s)

Combination of Measures used to ensure Safe Storage of Biometric Templates in Database	No. of Respondents	No of Respondents in percentage (%)
Change DB passwd	5	6.4%
Change DB passwd, Encrypt Bio Templates	1	1.3%
Change DB passwd, Reduce DB access	2	2.6%
Change DB passwd, Reduce DB access, Encrypt Bio Templates	3	3.8%
Change DB passwd, Strong passwd, Encrypt Bio Templates	2	2.6%
Change DB passwd, Strong passwd, Reduce DB access	3	3.8%
Change DB passwd, Strong passwd, Reduce DB access, Encrypt Bio Templates	20	25.6%
Encrypt Bio Templates	14	17.9%
Reduce DB access	1	1.3%
Reduce DB access, Encrypt Bio Templates	10	12.8%
Strong passwd	1	1.3%

Strong passwd, Encrypt Bio Templates	1	1.3%
Strong passwd, Reduce DB access	3	3.8%
Strong passwd, Reduce DB access, Encrypt Bio Templates	8	10.3%
Other(s)	4	5.1%
Total	**78**	**100.0%**

Table 4.34. Statistics of Combination of Measures ensuring Safe Biometric Templates in Database

4.6 Respondents Views, Comments & Suggestions

In the *Any Other Comments* section of the Questionnaires fielded to respondents. The sampled respondents mentioned that *biometric templates security is key to the advancement of the field of biometrics, passwords for biometric systems' databases should be changed every 90 days and no later than 180 days* and that *clearing i.e. zeroing data of de-allocated memory in biometric systems is of utmost significance as memory is vulnerably susceptible if malicious scripts could potentially read it and retrieve biometric image data before it is emptied.*

4.7 Conclusion

In this chapter, respondents' utilization and view of existing biometric fingerprint template protection schemes and approaches was explored. It was discovered that some biometric encryption schemes were preferred over others. Majority of the respondents which is 40 (51.3%) preferred to use RSA and ECC scheme over other biometric template protection schemes. It was additionally observed from the data collected, that most of the sampled respondents 55(70.5%) saved biometric templates in databases. Spoofing at the database level was the most experienced attack on biometric templates and was identified by 43 (55.1%) of respondents as the most

persistent attack on biometric systems. Results from sampled respondents showed that, a combination of measures and not one form of prevention measure were required to protect biometric templates against adversary attacks. In the following chapter this study discussed the design and development of the biometric template encryption tool which entailed a two-step enrollment and authentication of biometric fingerprints templates using encryption keys derived from other biometric fingerprint templates. This tool optimized security of biometric fingerprint templates archived in a unimodal biometric system's database.

CHAPTER FIVE

SYSTEM ANALYSIS AND DEVELOPMENT

5.1 Introduction

This chapter presents the design and development process of the biometric fingerprint encryption and decryption tool. One of the objectives of this study was to build a software tool to demonstrate a technique of encrypting and decrypting biometric fingerprint templates using encryption and decryption keys derived from other biometric fingerprints then testing it to determine its viability and efficacy.

5.2 Requirements Analysis

5.2.1 Functional Requirements

Significant requirements of the developed system comprised of the following.

i. System captures fingerprint images from presented biometric fingerprint images.
ii. System extracts fingerprint templates into ISO 19794-2 format and raw images.
iii. System has enrolment functionality of saving fingerprint templates into system database.
iv. System has functionality of verifying presented fingerprints from archived fingerprints.
v. System has functionality of identifying presented fingerprints from archived fingerprints.
vi. System saves fingerprints in RDBMs database.
vii. System does encryption and decryption of users' fingerprint templates.
viii. System derives encryption keys from enrolled fingerprints.
ix. System encrypts extracted fingerprint templates before saving to database with encryption keys derived from other fingerprints.
x. System performs decryption of archived encrypted fingerprint templates using decryption keys derived from enrolled users' fingerprint templates during verification and identification of enrolled system users.

xi. System uniquely identifies and verifies users after verification and identification of their presented fingerprints.
xii. System should not allow cross matching of fingerprints across various databases.
xiii. System should prevent reverse engineering of fingerprint templates from adversarial attempts to obtain original fingerprint images.
xiv. System matching speeds during verification and identification should not compromise system's False Acceptance Rate (FAR) and False Rejection Rate (FRR).

5.2.2 Non Functional Requirements

The following are requirements that are not specific to the main functionality of the main system though they enhanced usability, interactivity and presentation of fingerprint images and minutiae data in the developed system. They are;

i. Intuitive and easy to use system user interface.
ii. Tabulated fingerprint minutiae data showing minutiae's angles of orientation and ridge types.
iii. Animated fingerprint image showing fingerprint patterns on presentation of fingerprint to sensor.
iv. System response turnaround time to users' interaction is within 1 minute which is an acceptable and short turnaround time for fingerprint authentication speed.
v. System should be able to manually load fingerprint image files from computer data folders.
vi. System is not resource intensive as it is a light weight application.
vii. System uses various fingerprint readers.
viii. System is capable of running on various operating systems platforms including Microsoft Windows and Linux.
ix. System is able to capture fingerprint images and save them in desired computer folder locations and paths.
x. System should on refresh clear logs, clear fingerprint image and clear minutiae data table.

5.3 System Architecture

The system was implemented using a multi-tier architecture. The system was constructed to use 3-tier architecture to allow for scalability and independent handling of the various components of each tier. The system's structured architecture consisted of presentation, application and data layers.

In the presentation layer, Java's JSwing framework was used to implement form components for capturing system user's particulars, capturing of fingerprints, displaying fingerprint image patterns and viewing of tabulated minutiae data. The application layer implemented the fingerprint enrolment, verification and identification functionalities. The application layer also handled the application's logic while in the data layer, the external data source for archiving and retrieval of application's data which included fingerprint templates and user details to and from the non-embedded MySQL database was built. The Three-Tier architecture implemented by this system is shown in figure 5.1 below.

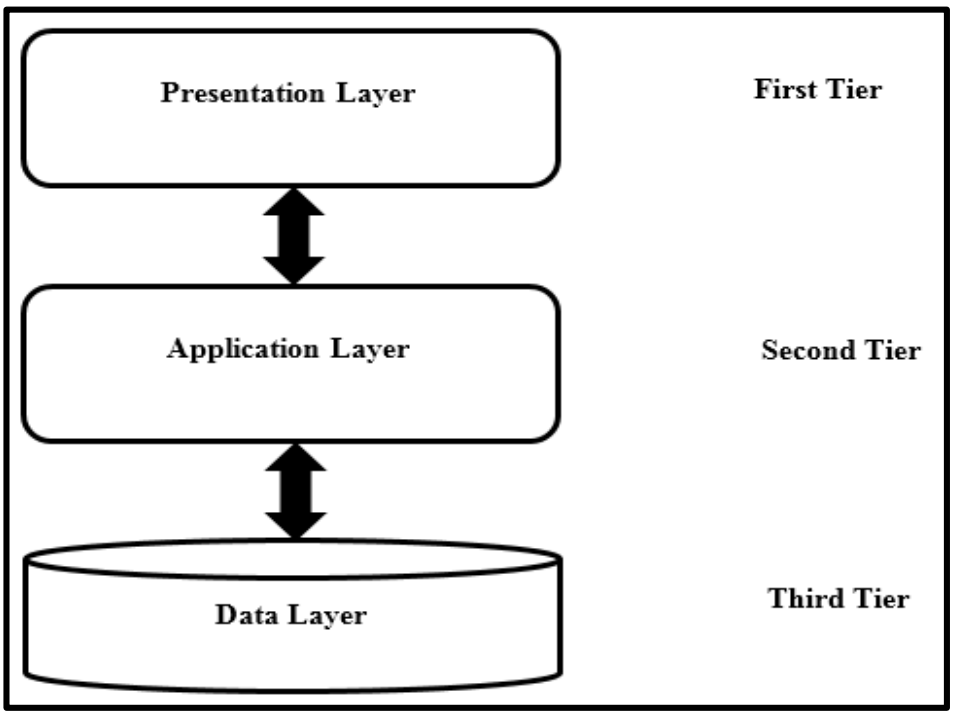

Figure 5.1. Three-Tier System Architecture

5.4 System Flow Design

System flow is divided into two major phases which are the two roles performed by the system. They are;

i) User Registration and Fingerprints Enrolment.
ii) User Authentication and Fingerprint Matching.

5.4.1 User Registration and Fingerprints Enrolment

The following sequence of events take place in this phase. First the system prompts for user details i.e. user names and national identity card no. The system will not advance to the next steps until these details are provided. Once user particulars are supplied, system proceeds to the second step where capturing of fingerprints takes place.

Fingerprints registration process is divided into two other sub processes. The first one is where the user supplies their first fingerprint for enrolment preferably any of their index finger. The finger once captured, the system extracts a fingerprint template **t1** from it and then the biometric fingerprint encryption modules extract a unique biometric key **ek** from it. The system then prompts the user to present the second fingerprint for enrolment after which it extracts a biometric fingerprint template **t2** from it.

Once the user's details have been entered, fingerprints captured for enrolment and biometric encryption key **ek** is derived from the first enrolled fingerprint **t1**, the system then encrypts the second user's fingerprint template **t2** with the encryption key **ek** derived from the first fingerprint template **t1** to encrypted template **et2** which is now secured. This step completes with the system saving the first fingerprint template to database **db1** and saving of the encrypted fingerprint template **et2** together with the supplied user details to database **db2**. Figure 5.2 below shows a diagrammatic flow of fingerprint registration process.

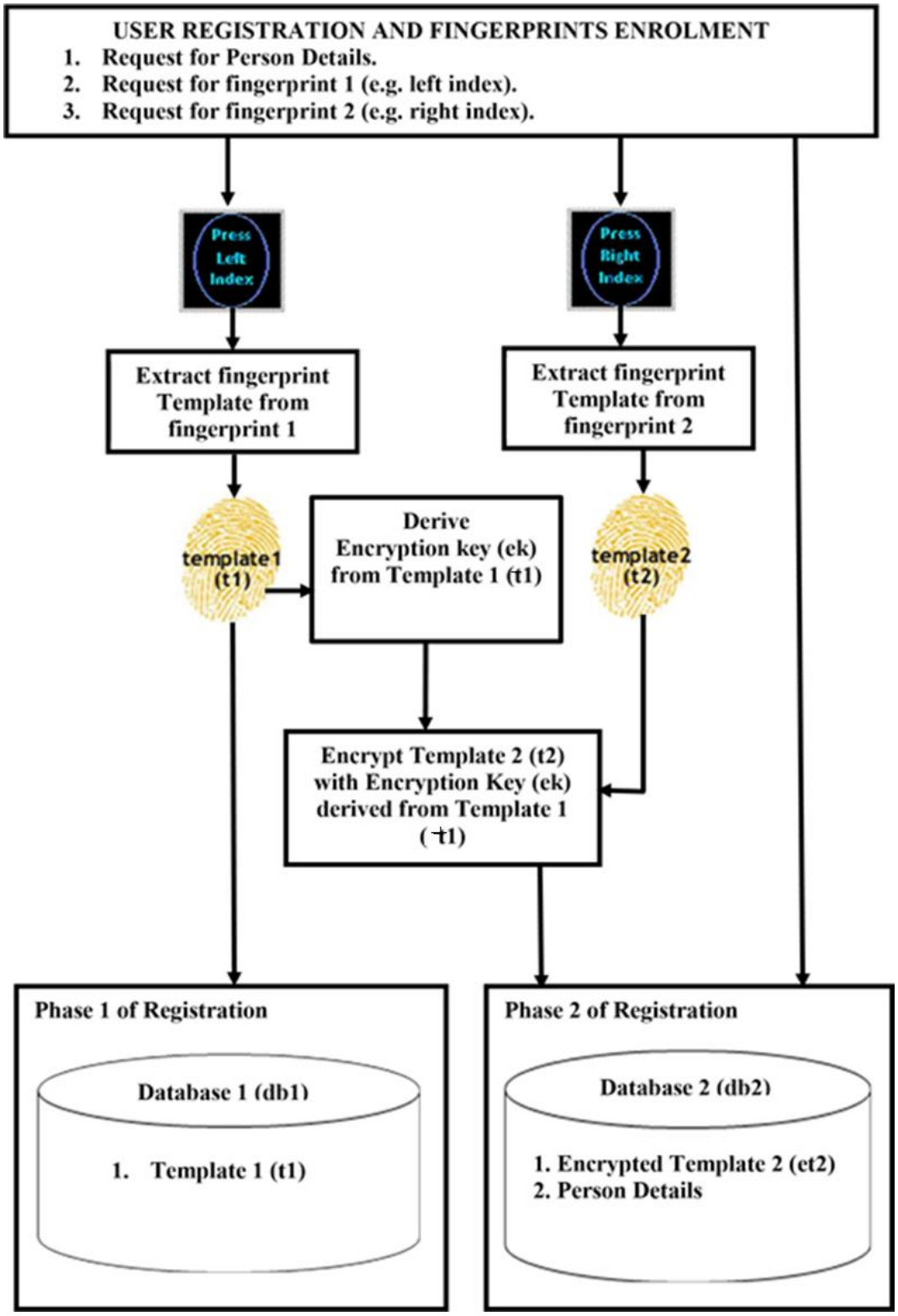

Figure 5.2. User Registration and Fingerprints Enrolment

5.4.2 User Authentication and Fingerprint Matching

This phase verifies and identifies system users. In verification the user is authenticated against user details they provide while in identification the user is authenticated from looping thru the entire fingerprint databases. In either verification or identification if the presented fingerprint is similar to the one saved in database **db1** the system alerts for fraudulent system use because, due to the noisy nature of fingerprint images, no two fingerprint images from the same fingerprint should be similar to each other.

In **verification**, system user is prompted to enter identity number. System then searches database **db1** for fingerprint template **t1** saved against the supplied identity number. If the identity number provided exists, the system retrieves fingerprint template **t1** saved against it in readiness for matching. The system then prompts the user to present their fingerprint for capturing of fingerprint image and extraction of template **vit1** to be matched against template **t1** in the first step of verification. If presented fingerprint does not match the verification process ends but if the presented fingerprint and template **t1** match the system proceeds to the 2^{nd} step of verification.

In the second step of verification, the system prompts the user to present the second fingerprint for capturing and extraction of fingerprint template **vit2** for verification. The system then derives decryption key **dk** from matched template **t1** in first step of verification. The decryption key **dk** attempts to decrypt templates in database **db2** by looping thru all templates in database **db2**. If an encrypted template **et2** is successfully decrypted to **dt2**, the template is matched against template **vit2** extracted from the second fingerprint presented for verification. When the two templates **dt2** and **vit2** match, the system returns and displays the user details i.e. their names and identity number but if the two templates do not match the verification process ends and returns notification that there was no match.

In **identification**, system prompts user to present their fingerprint for capturing of fingerprint image and extraction of template **vit1** to be matched against looping of templates **t1** in database **db1** in the first step of identification. If presented fingerprint does not match with any of the templates in database **db1** the identification process

ends but if the presented fingerprint and and a template **t1** match the system proceeds to the 2nd step of identification.

In the second step of identification, the system prompts the user to present the second fingerprint for capturing and extraction of fingerprint template **vit2** for identification. The system then derives decryption key **dk** from matched template **t1** in first step of identification. The decryption key **dk** attempts to decrypt templates in database **db2** by looping thru all templates in database **db2**. If an encrypted template **et2** is successfully decrypted to **dt2**, the template is matched against template **vit2** extracted from the second fingerprint presented for identification. When the two templates **dt2** and **vit2** match, the system returns and displays the user details i.e. their names and identity number but if the two templates do not match the verification process ends and returns notification that there was no match. Figure 5.3 below shows a diagrammatic flow of both fingerprint verification and identification process.

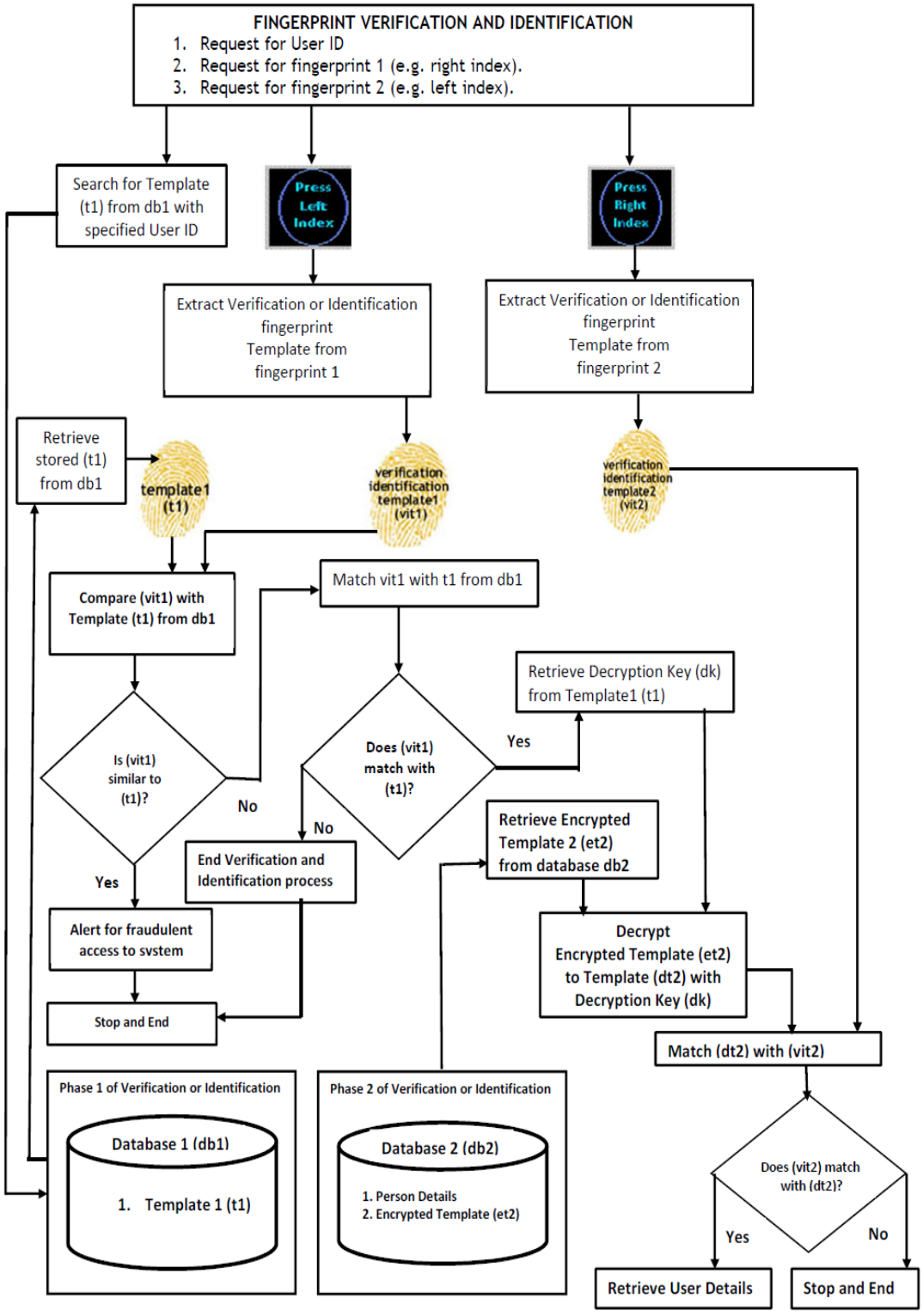

Figure 5.3. Fingerprint Verification and Identification

5.5 Use Case Diagrams

To model the dynamic nature of the two-step biometric fingerprint encryption and decryption tool, this study used use case diagrams to model the subsystems of this technique's tool. Use case diagrams when compared to other UML diagrams are the most appropriate in gathering design functional requirements of a system while also identifying actors and including both internal and external factors.

i). Use Case Diagram for Fingerprint Encryption and Enrolment

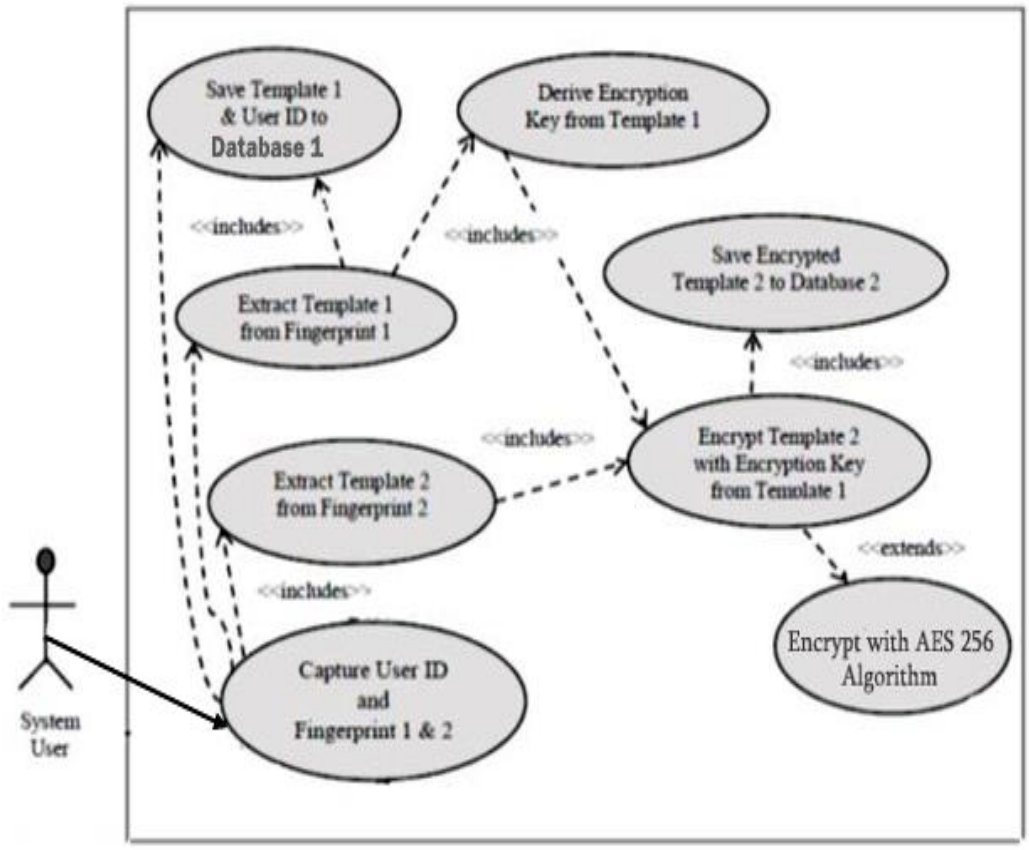

Figure 5.4. Use Case Diagram for Fingerprint Encryption and Enrolment

Use case diagram for fingerprint encryption and enrolment in figure 5.4 guides how user fingerprint enrolment and fingerprint encryption is implemented. The user's two fingerprints and user ID are first captured. Templates are extracted from both two

fingerprints where encryption key is derived from template 1 which is initially extracted from fingerprint 1. Template 1 together with user ID is then saved to database 1 while derived encryption key from template 1 is used to encrypt template 2 via AES 256 encryption algorithm. Template 2 is initially extracted from fingerprint 2. Encrypted template 2 is then saved to database 2.

ii). Use case Diagram for Fingerprint Decryption and Fingerprint Matching

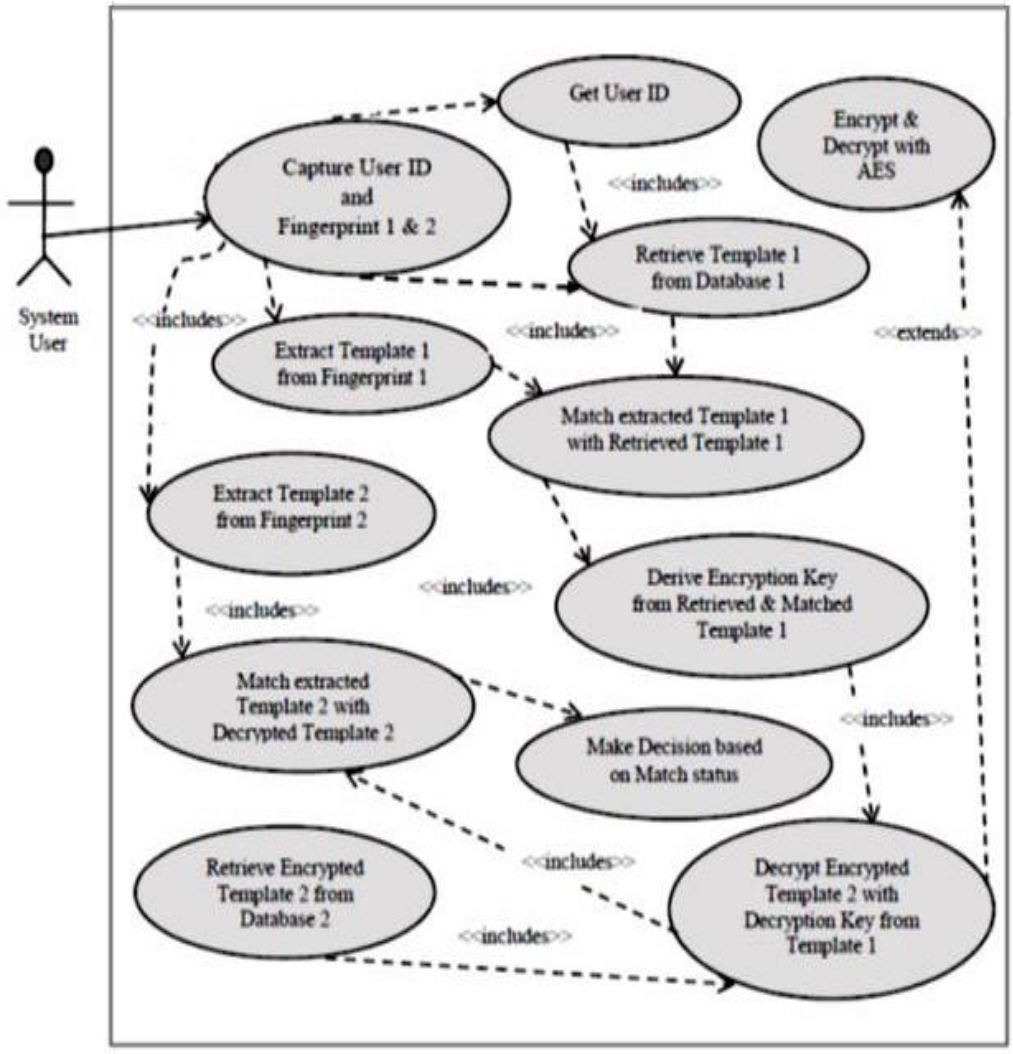

Figure 5.5. Use Case Diagram for Fingerprint Decryption and Matching

Use case diagram for fingerprint encryption and enrolment in figure 5.5 guides how user fingerprint matching and fingerprint decryption is implemented. The user's two fingerprints and user ID are first captured. User ID is only required where verification is to be done where it aids in retrieving template 1 from database 1 else for identification it is not requisite. Templates are extracted from both two fingerprints where decryption key is derived from retrieved template 1 after extracted template 1 is matched to retrieved template 1 from database 1. Retrieved template 2 is then retrieved from database 2 and if successfully decrypted by decryption key using AES 256 decryption algorithm, it is then matched to extracted template 2 from fingerprint 2. Authentication is successful if extracted template 2 matches with retrieved template 2 else it is a failed authentication.

5.6 UML Class Design

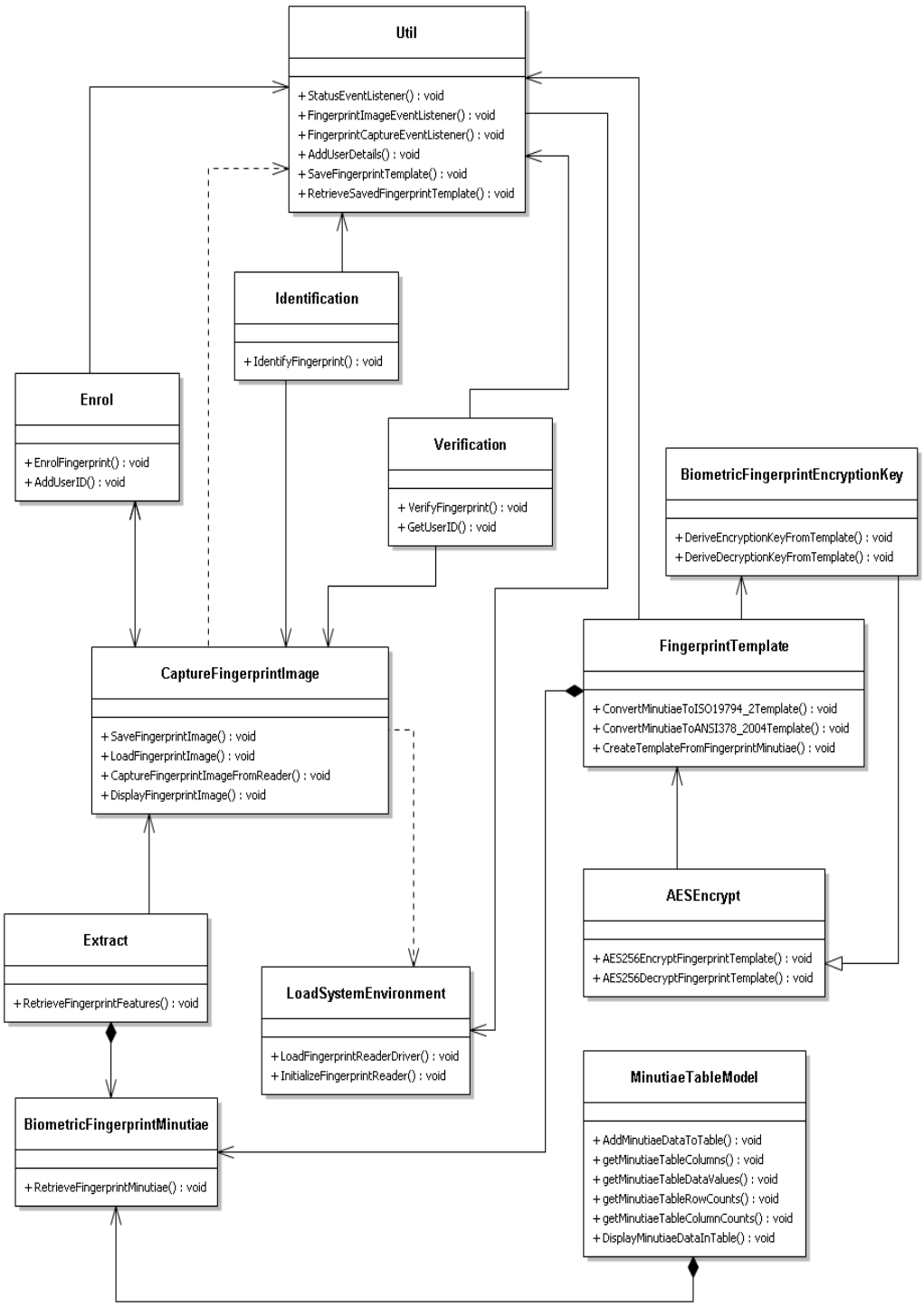

Figure 5.6. UML Class Diagram

This study used UML class diagram in figure 5.6 to present a graphical representation of the static view of the proposed biometric fingerprint encryption and decryption tool and the various aspects of this technique. The following subsections discuss the collections of this UML class diagram.

5.6.1 LoadSystemEnvironment Class

This class loads fingerprint reader drivers and initializes the connected reader in readiness for capturing fingerprint images by the system in capturing fingerprint images. It consists of methods LoadFingerprintReaderDriver and InitializeFingerprintReader.

5.6.2 Enrol Class

This class has methods which perform the functions of enrolling users' fingerprints to system and also captures user id to be saved against captured fingerprints.

5.6.3 CaptureFingerprintImage Class

This class handles the fingerprint image using the following methods; CaptureFingerprintImageFromReader, LoadFingerprintImage, SaveFingerprintImage and DisplayFingerprintImage. It is able to capture fingerprint image from fingerprint reader or load it from file system, save it to file system and also display the presented fingerprint image.

5.6.4 Util Class

This class implements the following event listener classes i.e. status, image and finger. It has methods for adding new user's details and fingerprint templates to database. It also has methods triggered by finger events for selecting fingerprint templates from database for purpose of matching.

5.6.5 Extract Class

This class consists of method RetrieveFingerprintFeatures which retrieves fingerprint features from fingerprint images from which fingerprint minutiae data which makes up fingerprint templates is drawn from.

5.6.6 FingerprintTemplate class

This class has a method whose function is to create biometric fingerprint templates from minutiae data retrieved from fingerprint features of captured fingerprint images. It also has methods for converting minutiae to ISO 19794-2 and ANSI 379-4 fingerprint template formats.

5.6.7 Verification Class

The verifyFingerprint method of this class performs 1 to 1 matching of fingerprint templates based on a specified user id. Its other method is GetUserID.

5.6.8 Identification Class

The identifyFingerprint method of this class performs 1 to many matching of fingerprint templates.

5.6.9 AESEncrypt Class

This is the class whose methods are used for AES 256 encryption and AES 256 decryption of biometric fingerprint templates.

5.6.10 BiometricFingerprintEncryptionKey Class

This class consists of a method which retrieves and returns biometric encryption key and decryption key from fingerprint templates. It has these two methods; DeriveEncryptionKeyFromTemplate and DeriveDecryptionKeyFromTemplate.

5.6.11 BiometricFingerMinutiae Class

This class has a method for retrieving fingerprint minutiae data which is used to create biometric fingerprint templates in FingerprintTemplate class.

5.6.12 MinutiaeTableModel Class

MinutiaeTableModel class is the model class of Java's JTable component which comprises of methods which add fingerprint minutiae data to display table, get column names, get minutiae data values, get row counts and column counts.

5.7 Database Design

MySQL which is a non-embedded database as well as a relational database management system was used to store biometric fingerprint templates and user details in two databases **db1** and **db2** as shown figure 5.7 below. Database **db1** stores fingerprints templates used in first (1st) step of enrollment, verification and identification from which biometric encryption and decryption keys are derived from. Figure 5.8 below shows **registration_fp1** relation where this data goes into while database **db2** stores encrypted fingerprint templates and users particulars used in second (2nd) step of enrollment, verification and identification as shown in **enc_registration_fp2** relation in figure 5.9 below.

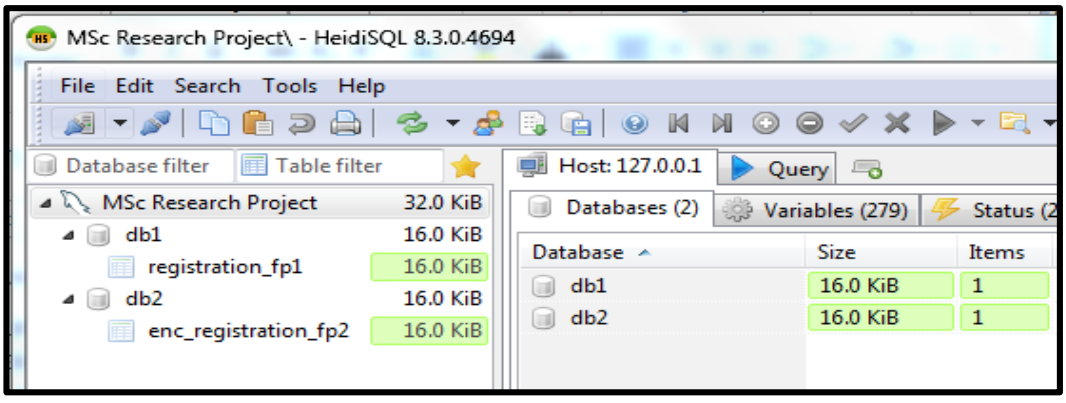

Figure 5.7. System Databases

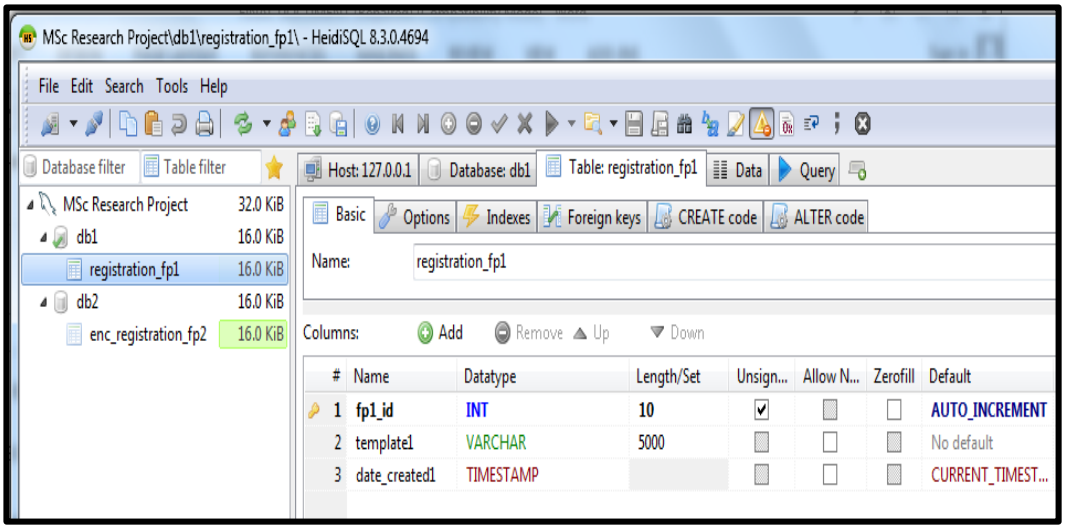

Figure 5.8. Registration_fp1 Table

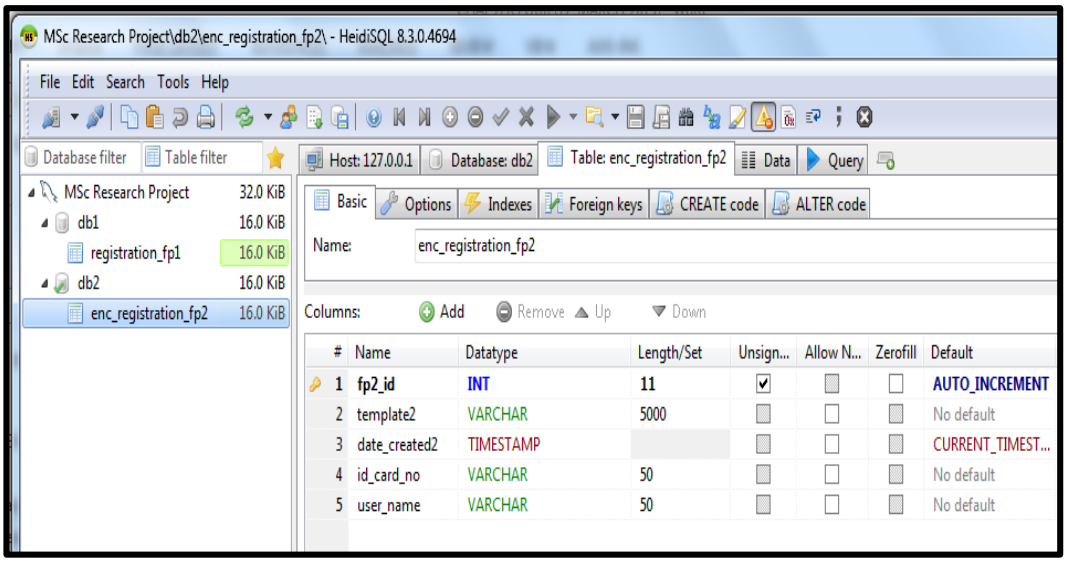

Figure 5.9. Enc_registration_fp2 Table

5.8 System Implementation

5.8.1 Tools and Technologies

The system was implemented using Java programming language. Netbeans 8.0 IDE was used to develop the presentation and business layer. Netbeans is the world's modular Swing application framework, used for mission-critical scenarios (Böck & Heiko, 2011). The presentation layer largely employed use of Java's Jswing

components while the business logic was implemented using object oriented concept of Java programming language thus allowing for creation of objects, methods re-use and class inheritance during runtime.

Griaule 2009 SDK and AFIS java framework library were used to extract, enroll and match templates captured from fingerprint images using a Digitalpersona U.are.U 4000 fingerprint reader. Griaule 2009 SDK was utilized as it provisioned for storing of fingerprint minutiae data in the standard ISO 19794-2 templates (Alexandru et al., 2012).

5.8.2 Database and Database Tools

MySQL 5.1 database was used to create the two databases required by the two-step biometric fingerprint encryption and decryption system. HeidiSQL 8.3 database manager was employed to aid in the visual design and modelling of the table structures in the two databases. HeidiSQL provides a browser for viewing data in tables and an easier way of running SQL CRUD queries from its GUI.

5.9 System Graphical User Interface

5.9.1 Fingerprint View Panel

When a fingerprint is presented on a fingerprint reader, the captured fingerprint image is displayed on the system's fingerprint view panel. The fingerprint view panel shows ridges i.e. bifurcations and ridge endings patterns on a fingerprint image which are the physiological patterns that uniquely identify a person from another. Figure 5.10 shows physiological patterns captured and displayed on a fingerprint view panel.

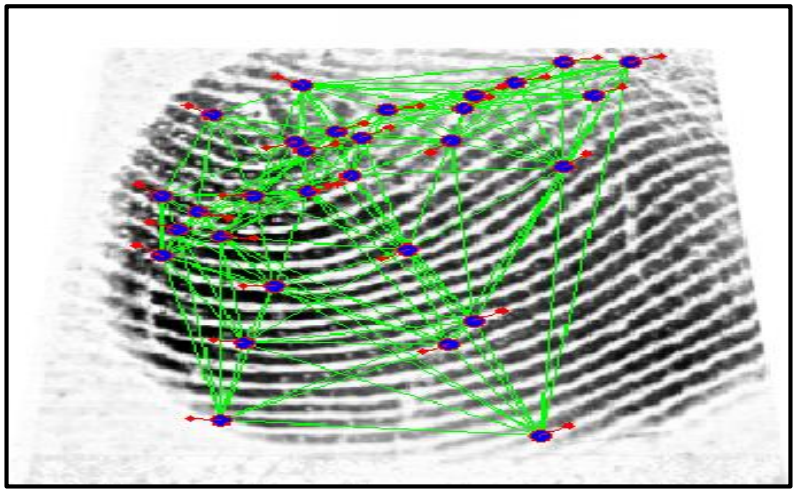

Figure 5.10. Fingerprint View Panel

5.9.2 System Logs Panel

The logs of events and activities taking place in the system are logged at the system logs panel. A system user is notified of events such as successful system initialization, plugged in fingerprint reader, unplugged fingerprint reader and captured fingerprint image. These events are tracked and logged by the system logs panel as shown in figure 5.11 below.

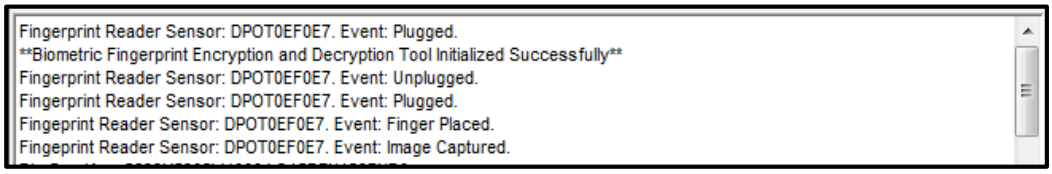

Figure 5.11. System Logs Panel

5.9.3 System Buttons Panel

Buttons which are used to do the main functions of the system i.e. fingerprints enrolment, user verification and user identification are docked in the system buttons panel. System buttons panel is also used to hold the following buttons; refresh button which resets the whole system, clear log button which cleans all displayed system logs and the ‘clear fingerprint and data table’ button which clears fingerprint view panel and fingerprint minutiae data table panel. This panel is also used to display the

biometric key label which outputs the derived biometric key, auto extract check box which is used to prompt the system to perform automatic identification and fingerprint template extraction. System buttons panel is shown in figure 5.12 below.

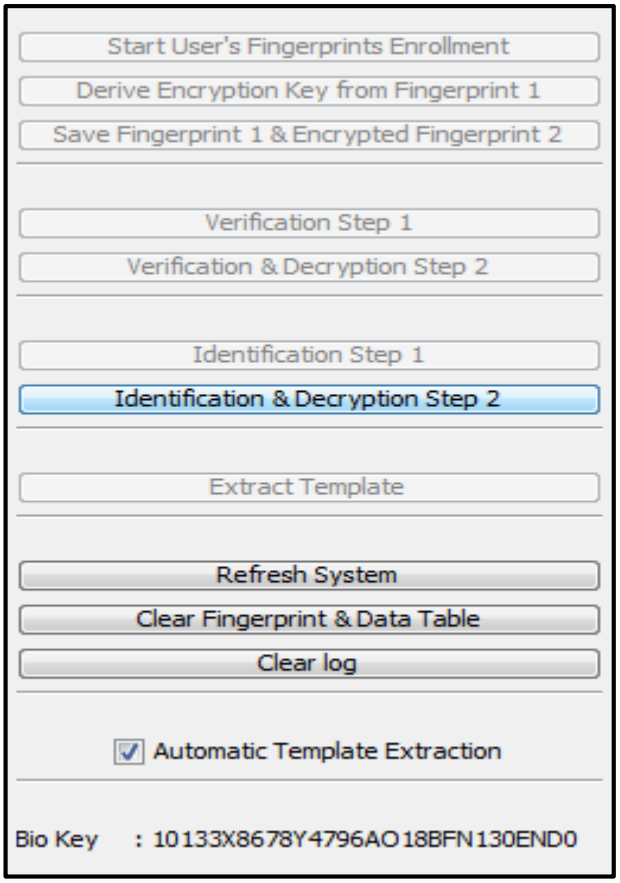

Figure 5.12. System Buttons Panel

5.9.4 Fingerprint Minutiae Data Table Panel

The fingerprint minutiae data table panel displays minutiae data of templates extracted from fingerprint images. It is refreshed and repopulated again with minutiae data of a fingerprint image every time a fingerprint image is captured form the fingerprint reader sensor module. Minutiae column shows the number of minutia, **X** column shows the minutia's position on the x axis, **Y** column shows the minutia's position on the y axis, **DIRECTION** column shows the minutia's angle of orientation given its x and y coordinates and **RIDGE TYPE** column determines

whether the ridge type is a bifurcation or an ending. Figure 5.13 shows minutiae data extracted from a template and displayed in a fingerprint minutiae data table panel.

MINUTIAE	X	Y	DIRECTION	RIDGE TYPE
1	115	235	112	Bifurcation
2	258	266	160	Ending
3	197	209	24	Ending
4	133	145	248	Ending
5	223	160	152	Ending
6	124	218	120	Bifurcation
7	213	144	20	Ending
8	145	184	0	Ending
9	214	284	32	Bifurcation
10	270	315	148	Ending
11	137	246	0	Bifurcation
12	158	249	144	Bifurcation
13	121	302	236	Ending
14	107	223	240	Bifurcation
15	175	260	28	Bifurcation
16	179	286	152	Ending
17	239	324	140	Ending
18	189	305	136	Ending
19	219	306	156	Ending
20	284	338	140	Bifurcation
21	223	315	148	Ending
22	258	338	136	Ending
23	101	246	228	Bifurcation
24	157	277	144	Ending
25	153	283	16	Ending
26	101	205	232	Ending
27	169	290	148	Ending
28	156	322	236	Bifurcation
29	124	92	252	Ending
30	249	81	152	Ending

Figure 5.13. Fingerprint Minutiae Data Table Panel

5.9.5 System's Main Frame

The main frame in which the user interacts with the system is the system's main frame. It has on its menu bar the following items; a provision for loading and saving fingerprint images and a provision for viewing researchers' particulars. Figure 5.14 below shows the system's main frame which anchors the fingerprint view panel, system logs panel, system buttons panel and the fingerprint minutiae data table panel.

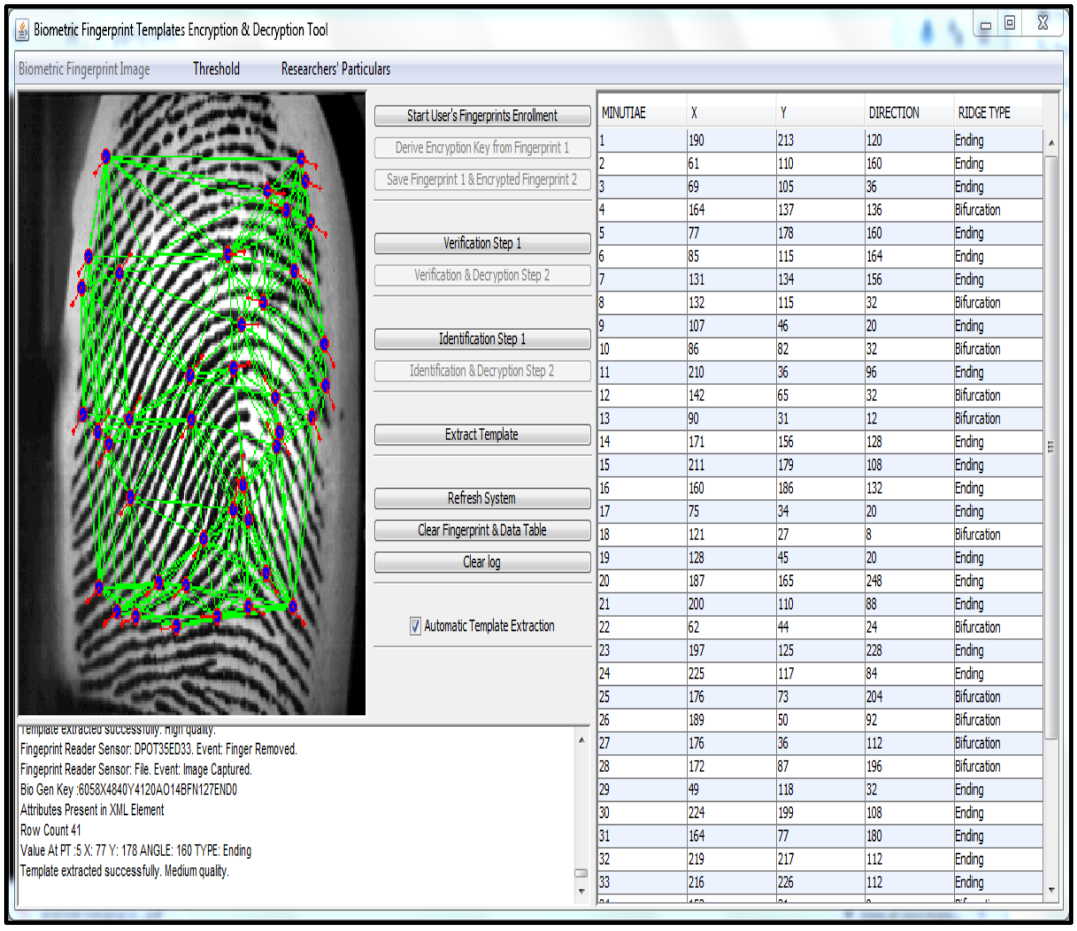

Figure 5.14. System's Main User Interface

5.10 Test Results

5.10.1 Introduction

In testing of the biometric fingerprint encryption and decryption tool, 600 fingerprint templates were extracted, enrolled and saved to the system's database. Portions of fingerprints in this study's test used the CASIA-FingerprintV5 collected by the Chinese Academy of Sciences' Institute of Automation (CASIA). The fingerprint images were captured using Digitalpersona U.are.U fingerprint readers (CASIA-FingerprintV5, n.d.).

Fingerprint images used during test were majorly categorized into two (2) i.e. fingerprints used to derive encryption keys in the 1st step of enrollment and authentication. The other category of fingerprints were used in 2nd step of enrollment

and authentication where they were encrypted before being saved to database and decrypted before authentication of fingerprints. Out of the 600 fingerprint images used, 300 were used to derive encryption keys using the proposed technique in section 2.11. This study derived encryption keys from fingerprints of the left hand and used them to encrypt fingerprints from the right hand. Table 5.1 below shows this data where out of each of the three fingers types used from each hand i.e. thumb, index and middle fingers, each finger type had one pair from which an encryption key was derived in 1st step of enrollment then used to encrypt the other pair in 2nd step of enrollment.

LEFT HAND FINGERPRINTS WHICH WERE USED IN 1ST STEP OF AUTHENTICATION AND TO DERIVE ENCRYPTION KEYS			RIGHT HAND FINGERPRINTS WHICH WERE ENCRYPTED AND USED IN 2ND STEP OF AUTHENTICATION		
RIGHT HAND FINGER TYPE	TOTAL FINGER TYPE COUNT	TOTAL COUNT OF RIGHT HAND FINGERPRINT TEMPLATES USED	LEFT HAND FINGER TYPE	TOTAL FINGER TYPE COUNT	TOTAL COUNT OF LEFT HAND FINGERPRINT TEMPLATES USED
THUMB	100	300	THUMB	100	300
INDEX	100		INDEX	100	
MIDDLE	100		MIDDLE	100	

Table 5.1. Fingerprint Types used in 1st and 2nd stages of Verification and Identification

5.10.2 Overall Test Results

From the test results carried out, 181 (60.33%) of fingerprints templates in 2nd step of verification and identification were decrypted successfully and matched to their corresponding fingerprint type using technique proposed by this study in section 2.11. 119 (39.67%) of fingerprints did not pass the decryption test. These results are shown in Table 5.2 below.

VERIFICATION AND IDENTIFICATION STATUS AFTER DECRYPTION OF LEFT FINGERPRINT TEMPLATES	COUNT	PERCENTAGE
PASS	181	60.33%
FAIL	119	39.67%
ALL STATUS COUNTS	**300**	**100%**

Table 5.2. Overall Test Results for Pass and Fail during Decryption in 2nd step of Verification and Identification

5.10.3 Finger Type allocations for Test of Decryption before Authentication

Three fingerprint types were used to carry out tests. They were the thumb, index and middle finger. From each finger type, 100 fingerprint images from 100 persons were used to test the decryption capability of the developed system such that the total number of fingerprint images encrypted and tested during decryption and authentication step were all together 300 fingerprint images. Table 5.3 represents these allocations per finger type as shown below.

FINGER TYPE USED FOR VERIFICATION AND IDENTIFICATION OF DECRYPTED LEFT FINGERPRINT TEMPLATES	TOTAL LEFT FINGER TYPE COUNT
THUMB FINGERS	100
INDEX FINGERS	100
MIDDLE FINGERS	100
TOTAL FINGERS DECRYPTED	**300**

Table 5.3. Statistics of Finger Types used to Test for Decryption in 2nd step of Verification and Identification

5.10.4 Respective Finger Type Results during Authentication after Decryption

From the finger types used, verification and identification results after decryption of fingerprint templates in 2nd step of authentication showed that 63 (63%) of Thumb fingerprint templates were decrypted and authenticated successfully while 37 (37%) could not be verified or identified after decryption. 60 (60%) of Index fingerprint templates were decrypted and authenticated successfully while 40(40%) could not be verified or identified after decryption and lastly 58(58%) of middle fingerprint templates authenticated successfully while 42(42%) could not be verified or identified after decryption. These results are represented in Table 5.4.

FINGER TYPE	VERIFICATION AND IDENTIFICATION STATUS AFTER DECRYPTION OF LEFT FINGERPRINT TEMPLATES	STATUS COUNT PER LEFT FINGER TYPE	OVERALL LEFT FINGER TYPE COUNT	STATUS PERCENTAGE PER LEFT FINGER TYPE
THUMB	PASS	63	100	63%
	FAIL	37		37%
INDEX	PASS	60	100	60%
	FAIL	40		40%
MIDDLE	PASS	58	100	58%
	FAIL	42		42%

Table 5.4. Test Results for all the Finger Types used in Encryption and Decryption at 2nd step of verification and Identification

5.10.5 Test Results Analysis and Summary.

The biometric fingerprint encryption and decryption tool demonstrated encryption and decryption of fingerprint templates in a unimodal biometric system using encryption keys derived from other biometric fingerprint templates as a robust technique of securing biometric fingerprint templates in database. Results from tests carried out confirmed it is a viable approach towards alleviating type 6 attacks on biometric systems which is the attack of biometric templates in a biometric system's database.

Test results showed that 63 (63%) of thumb, 60(60%) of index and 58 (58%) of middle fingerprint templates could be decrypted and authenticated with the corresponding finger type but 37 (37%) of thumb, 40 (40%) of index and 42 (42%) of middle fingerprint templates could not be authenticated after decryption. To evaluate these discrepancies, the particular fingerprints that failed the tests were critically observed and analyzed. This study found out that some of these fingerprint

images did not have elaborate physical feature traits. This can be attributed to the bearer's fingerprints being worn out from doing heavy menial jobs. Another factor that could have contributed to failed decryption and authentication of fingerprints is the inability of fingerprint sensor used, to be able to capture clear fingerprint images from sweaty and dry hands. The other likelihood of low quality images that did not pass decryption and authentication step could possibly have been significant intra-class variations of fingerprint images resulting from the various levels of pressure and rotation of fingerprints on the fingerprint reader by the volunteers who donated fingerprints.

Test results with positive status outcomes after decryption and authentication of fingerprints can be improved by using advanced fingerprint readers like laser based finger sensors which can capture exceptional fingerprint images despite the known existing caveats that impede efficient extraction of fingerprint templates from fingerprint images. To reduce capture of low quality fingerprint images from sweaty and dry fingerprints, the following two practices can be put into practice. Persons with sweaty and wet fingers could be asked to dry their fingerprints on a piece of cloth before presenting them on reader sensor e.g. rub their fingers on their clothes while persons with dry fingers could be requested to rub their fingers on their face to make them moist. Washing of hands and oiling them could also aid in reducing capture of low quality fingerprint images.

5.10.6 Strengths and Weaknesses of Developed Biometric Encryption Tool

The following are the advantages of the biometric fingerprint encryption and decryption tool this study proposed and developed that make it superior over other biometric template protection techniques. The strength of the proposed tool lays within the way the biometric fingerprint encryption and decryption key has to be derived from a biometric fingerprint template for it to be used in 2nd step of enrollment, verification and identification of fingerprints. These strengths are;

i. The biometric decryption key cannot be misplaced or forgotten.

Encrypted biometric fingerprint templates *et2* in database *db2* are encrypted using encryption keys derived from biometric templates in database *db1*. A user has to be verified or identified in step 1 of verification and identification in order for the biometric decryption key for decrypting their other fingerprint template in step 2 to be released. Unlike a technique where a single encryption key is used for encrypting all biometric fingerprints in a database, in this technique each biometric template is encrypted using a unique biometric encryption key derived from the bearer's other fingerprint thus the biometric encryption key cannot be shared or forgotten. One of the advantages of a good biometric encryption key as compared to passwords is that it cannot be forgotten or misplaced (Das, 2011).

ii. Biometric encryption and decryption keys cannot be gleaned, copied or distributed.

In a *fuzzy vault* scheme it is possible to glean over biometric templates if they are temporarily exposed (Hooda & Gupta, 2013) but in this study's proposed encryption and decryption tool, encrypted templates are meaningless and not useful in the hands of an adversary. The biometric encryption and decryption keys in the proposed encryption and decryption tool do not exist openly in a way that they can be singled out, gleaned over, copied and distributed. They have to be derived from biometric templates of the user. When the biometric template is matched in step 1 of verification and identification, only then can a biometric decryption key be derived from it for use in decrypting the other user's fingerprints for purpose of verification in step 2 of verification and identification. The user is successfully verified or identified after the 2nd step of verification and identification.

iii. Biometric encryption keys are easy to generate but hard to forge and reverse engineer

It is not possible for hackers to gain access to biometric encryption keys to be able to reverse engineer them. Hackers would have to know how to pass the 1st step of identification which requires a user to get verified or identified for decryption keys

to be released for 2nd step of verification and identification which happens after the decrypted fingerprint template is matched to the 2nd user's fingerprint which is presented to the system in the 2nd step of verification and identification. Though it is easy to generate encryption key from the developed biometric encryption and decryption tool as is observed in chapter 2, on deriving encryption key from a biometric fingerprint template, it is notably difficult to generate a key with high stability and entropy in a *secure sketch* and *fuzzy extractor* technique (Jain et al, 2008).

iv. Biometric encryption and decryption keys cannot be guessed.

Hackers will have an uphill task if they embarked on guessing decryption keys for encrypted biometric fingerprint templates and if they were to succeed to get one decryption key, it would only decrypt one biometric template only because all the encrypted biometric templates are encrypted using unique biometric encryption keys derived from their bearer's other fingerprint template. The system only considers a verification or identification successful after it passes the 1st and 2nd steps of verification and identification. When compared and contrasted with a *fuzzy commitment* scheme, this biometric encryption and decryption tool has excelled in concealing the biometric encryption keys unlike a fuzzy commitment scheme which does not guarantee satisfactory hiding and binding of biometric fingerprint traits as is observed in (Al-Saggaf & Acharya, 2013).

v. Matching speeds do not degrade

The matching of the biometric encryption and decryption tool does not degrade as is the case of a salting technique like the invertible *bio-hashing* transformation technique. The system is able to verify and identify users after the 2 step authentication process in less than 1 minute as is one of the non-functional requirements of the biometric encryption and decryption tool this study developed. In a *bio-hashing* technique there is reduced performance in speeds of the biometric system when there is presence of large intrauser variations of biometric fingerprints (Jain et al, 2008).

vi. Cross matching of fingerprint templates across databases not possible

In a noninvertible biometric template protection technique e.g. cancellable biometric scheme, if transformational parameters are leaked or known to adversaries, it is possible to retrieve original fingerprint templates and use them to spoof other biometric systems databases (Rathgeb & Uhl, 2011) but in this study's proposed biometric and encryption tool, if hackers spoofed the encrypted biometric fingerprint templates, they would not be able to use them elsewhere because they are unusable until they are decrypted by their original bearer's other fingerprint.

The proposed techniques encountered the following bottlenecks which posed as weaknesses that lower its viability and effectiveness. These weaknesses are;

i. Fixed Image Resolution

The technique proposed and developed in this study is only capable of reading fingerprint images from fingerprint readers which capture images of 500dpi resolution. Images with lower or higher resolutions than 500 dpi cause errors during extraction of fingerprint features.

ii. Low Quality Images

The biometric encryption and decryption tool developed encounters problems of verification and identification of fingerprints during authentication of persons when low quality images are captured or presented on its sensor reader. It currently works well with fingerprint images of medium and high quality but fails on low quality fingerprint images.

5.10.7 Conclusion

This chapter has presented a conceptual technique for encrypting and decrypting biometric fingerprint templates using encryption keys derived from other biometric fingerprint templates. This study has designed, developed and implemented a biometric fingerprint templates and encryption and decryption tool based on this technique. This study has provided a secure and optimized way of securing biometric fingerprint templates in a database by developing a biometric and encryption tool which mitigates against 'type 6' attack which is attack of biometric templates in a

database. Test results demonstrating use of this technique are presented and evaluated. A discussion of the developed tool's strengths and weaknesses as compared to existing biometric templates protection schemes is presented in order to determine its viability and efficiency.

CHAPTER SIX

CONCLUSION AND RECOMMENDATIONS

The main purpose of this study was to develop a more secure and effective technique for securing biometric fingerprint templates stored in a database that would be predicated on encrypting fingerprint templates with encryption keys derived from other biometric fingerprint templates. To accomplish this objective, it was essential to ascertain the various biometric attacks and threats that have been documented in existing literature and determine the biometric template protection schemes and techniques currently being used towards securing biometric templates against biometric systems' database attacks.

The study sought to establish a robust approach aimed at protecting biometric fingerprint templates in the frugal and easy to implement unimodal biometric fingerprint systems because the schemes in current literature are more emphatic on securing biometric templates in multimodal biometric systems which unlike unimodal biometric systems are very intricate, expensive and only affordable to sizably voluminous corporations and are a preserve for affluent regimes (Das, 2012).

In order to validate the justification this research was based on, it was essential to study and provide empirical evidence on existing biometric template protection techniques and schemes with regards to unimodal biometric fingerprint systems. The study sought to answer the following questions;

1 What are the existing biometric templates protection schemes and approaches used to secure biometric fingerprint templates?
2 What are the shortcomings of the current biometric fingerprint templates protection schemes and approaches?
3 What are the features of an ideal biometric fingerprint template protection technique?
4 How will the quality of the developed biometric fingerprint encryption and decryption tool be assessed to determine if it meets the required specifications of an ideal biometric fingerprint template protection scheme?

6.1 Empirical Research Findings

This section provides a synthesis of the empirical findings from the study with reverence to the study's four research questions.

1. **What are the existing biometric templates protection schemes and approaches used to secure biometric fingerprint templates?**

   The biometric template protection schemes are largely categorized to *feature transformation* and *biometric encryption* in existing theoretical literature. From the sampled respondents 16 (20.5%) used feature transformation to secure biometric templates while half of the respondents i.e. 39 (50%) used biometric encryption. 23 (29.5%) of respondents did not use any of these two categories. It was evident from sampled respondents feedback that biometric encryption was the most prevalent technique for securing biometric templates.

   Schemes and approaches documented under these two categories and identified by existing literature in feature transformation are the invertible biohashing and the non-invertible cancellable biometrics while under biometric encryption's key binding there is fuzzy vault and fuzzy commitment. Secure sketches and fuzzy extractors were identified as key generation methods in biometric encryption techniques. The other biometric template protection schemes that do not virtually fall under these two categories but were listed by respondents are watermarking, AES, RSA and ECC algorithms.

2. **What are the shortcomings of the current biometric fingerprint templates protection schemes and approaches?**

The study explored the following biometric template protection schemes and approaches and discovered their shortcomings as shown alongside them below.

i) Cancellable biometrics: In an instance where transformational parameters are known or leaked to hackers, this approach will not be secure and parameters will need to be changed to deter adversaries from cross matching users' fingerprint templates (Rathgeb & Uhl, 2011). In addition, high variance

brought about by transformation of biometric data reduces authentication speeds (Du et al, 2011).

ii) Bio-hashing: There are possibilities of unavoidable information leakage from biometric template data during computing of bio-hash (Das et al, 2012) and reduced system performance when a legitimate token is retrieved and presented by an adversary purporting to be a legitimate user (Gaddam & Lal, 2011).

iii) Secure Sketches and Fuzzy Extractors: Analysis on reusability of secure sketches and fuzzy extractors' scheme implored that they could not be safely applied severally on the same biometric template thus significantly limiting and reducing their usable practicability in biometric systems (Blanton & Aliasgari, 2013).

iv) Fuzzy vault: First there is difficulty in revoking a compromised vault which is prone to crossmatching. Secondly, it is possible to stage attacks after statistically analyzing points in a vault. Thirdly, an attacker can easily substitute their fingerprint templates with those of a user he targets and lastly, templates of users can be gleaned over if they are temporarily exposed (Hooda & Gupta, 2013).

v) Fuzzy commitment: Not only will an ordinary fuzzy commitment scheme not satisfy hiding and binding properties of biometric traits but is also considered insecure (Al-Saggaf & Acharya, 2013).

vi) RSA and ECC algorithms: A considerable amount of time is taken by these algorithms in decryption of images during verification and identification of persons in a biometric system while using these algorithms (Maniroja & Sawarkar, 2013).

vii) Watermarking: A greater amount of time is required to insert a watermark into a biometric fingerprint image and that most watermarking algorithms required the original image to be present to extract the watermark which increases overheads in a biometric system's database (Poongodi & Betty, 2014).

3. **What are the features of an ideal biometric fingerprint template protection technique?**

It was tenacious from the study that the following security measures would aid in securing biometric fingerprint templates in a biometric system. They are; encryption of biometric templates before saving them in a database, changing of database passwords every so often, use of strong database passwords and reduced levels of access to database. Majority of the sampled respondents 59(75.6%) indicated that encrypting of biometric templates would ascertain safe storage of biometric templates in a database. Other respondents mentioned that clearing of biometric system's enrollment and authentication activities would be consequential in averting access of biometric data by malevolent software. The study further established that an ideal biometric protection technique should encrypt or transform biometric templates before archiving them to a database in a way that will deter adversaries from spoofing them (Jain et al, 2008). According to Maltoni et al., (2003), an ideal biometric template protection scheme should consist of the following four major attributes.

i) Diversity: It should not be possible for a secure biometric template to support cross matching across databases, thus ascertaining the bearer's privacy. The developed biometric template protection technique's encrypted fingerprints cannot be used in other databases if they fall in the hands of adversaries. They can only be used for authentication after they are decrypted on their host system only.
ii) Revocability: It should be straightforward to revoke a compromised biometric template and reissue an incipient one based on the same biometric physical traits of the initial bearer. If it is suspected that fingerprints of an individual have been compromised in the proposed biometric technique, they can be easily revoked and new ones enrolled. This is such that it will be possible for new encryption and decryption keys to be derived from them.
iii) Security: It should not be possible to invert engineer the secure biometric template to obtain the pristine biometric template. This property deters adversaries from reconstructing original biometric traits and utilizing them as

a physical spoof in stolen templates. Encrypting biometric fingerprint templates using AES algorithm with encryption keys from other fingerprint templates hashes the biometric fingerprint data in a way that it is impossible for hackers to retrieve original biometric data.

iv) Performance: The biometric template protection scheme should not reduce the matching speeds of templates or trigger an upward surge in Erroneous Acceptance Rates and False Rejection Rates. The speed of the developed biometric encryption and decryption tool is within 1 minute when carrying out verification and identification of biometric fingerprint templates. A biometric authentication system which is fast in authenticating individuals is efficient where there is heavy traffic of individuals waiting to be identified or verified.

4. **How will the quality of the developed biometric fingerprint encryption and decryption tool be assessed to determine if it meets the required specifications of an ideal biometric fingerprint template protection scheme?**

Encrypting fingerprint templates with encryption keys derived from other biometric fingerprint templates before saving them in a database will provide more security to archived biometric templates and strengthen levels of security of biometric data in biometric systems as this will minimize and prevent adversaries from waging ‘type 6 attack’ which is the attack on a biometric system’s database.

There will be no need for biometric systems developers to use global encryption keys for all biometric templates in a biometric system’s database since the biometric encryption key derived from a user’s fingerprint data will be used to uniquely secure and encrypt their other fingerprints enrolled in the biometric system differently from fingerprints of other users enrolled in the same database implying that users will be able to decrypt their enrolled fingerprints only for purposes of verification and identification.

6.2 Recommendations for Improving This Study

This study has presented a new approach for securing biometric fingerprint templates in a biometric system database using encryption keys derived from other biometric fingerprint templates to encrypt biometric fingerprint templates. The following are recommendations for augmenting this study research:

i. Other feasible counter measures that assist in deterring 'type 6 attack' i.e. spoofing of biometric fingerprint templates in a biometric system's database need to be introduced and incorporated among measures used to protect biometric templates to bolster levels of security of the developed fingerprint encryption and decryption technique.
ii. System Audits of all verification and identification activities need to be done at the database level to determine all successful and failed fingerprint matching attempts for analysis and scrutinizing by biometric system developers. Performing system audits is significant in detecting anomalies and identifying threats that pose security threats in a biometric system.

6.3 Recommendations for Future Research

Directions for future research work will require researchers to address the following;

i) Research on ways to derive encryption keys from fingerprints that will produce encryption keys that do not vary with repeated scans of a fingerprint due to the noisy nature of fingerprints and at the same time not generate an encryption key that is easy to attack by use of brute force.
ii) Researchers should device intelligent means of identifying and preventing any abnormal and suspicious fingerprint verification and identification activity during runtime so that the two-step verification and identification process is suspended before it compromises security of the system and that of the users' biometric fingerprint templates.
iii) Databases of biometric systems where biometric fingerprint templates are stored should have their access levels controlled by utilizing biometrics in preference to use of traditional authentication modes like passwords so that

only authorized and trusted users e.g. biometric system developers are able to manage these databases and this will in addition, prevent hacking of database passwords.

REFERENCES

Ahmad, S. M., Ali, B. M., & Adnan, W. A. (2012, November). Technical Issues and Challenges Of Biometric Applications as Access Control Tools Of Information Security. *International Journal of Innovative Computing, Information and Control, 8*(11), 7983-7999.

Alanazi, H., Zaidan, B., Zaidan, A., Jalab, H., Shabbir, M., & Al-Nabhani, Y. (2010, March). New Comparative Study Between DES, 3DES and AES within Nine Factors. *Journal of Computing*, 152-157.

Alexandru, E., Alexandru, S., & Florica, M. (2012). Biometric identity management for standard mobile medical networks. *Engineering in Medicine and Biology Society (EMBC), 2012 Annual International Conference of the IEEE* (pp. 2186-2189). IEEE.

Al-Saggaf, A. A., & Acharya, H. (2013). Statistical Hiding Fuzzy Commitment Scheme for Securing Biometric Templates. *International Journal of Computer Network and Information Security*, 8-16.

Aly, O. M., Onsi, H. M., Salama, G. I., & Mahmoud, T. A. (2012, November). Multimodal Biometric System using Iris, Palmprint and Finger-Knuckle. *International Journal of Computer Applications, 57*(16), 1-6.

Arjunwadkar, M., & Kulkarni, R. V. (2010). Robust Security Model for Biometric Template Protection using Chaos Phenomenon. *International Journal of Computer Applications*, 10-12.

Arjunwadkar, M., Kulkarni, R. V., & Shahu, C. (2012, November). Biometric Device Assistant Tool: Intelligent Agent for Intrusion Detection at Biometric Device using JESS. *International Journal of Computer Science Issues, 9*(6), 366-370.

Balakumar, P., & Venkatesan, R. (2011). Secure Biometric Key Generation Scheme for Cryptography using Combined Biometric Features of Fingerprint and Iris. *International Journal of Computer Science*, 349-356.

Bansal, R., Sehgal, P., & Bedi, P. (2011, September). Minutiae Extraction from Fingerprint Images. *International Journal of Computer Science Issues, 8*(5), 74-85.

Bhatnagar, G., Wu, Q. J., & Raman, B. (2010). Biometric Template Security based on Watermarking. *Procedia Computer Science 2 (2010) 227–235*.

Blanton, M., & Aliasgari, M. (2013). Analysis of Reusability of Secure Sketches and Fuzzy Extractors. *Journal of Computer and System Sciences, 58*, 148-173.

Böck, & Heiko. (2011). In *The Definitive Guide to NetBeans™ Platform 7.*

Brindha, V. E. (2012). Biometric Template Security using Dorsal Hand Vein Fuzzy Vault. *Journal of Biometrics*, 1-6.

CASIA-FingerprintV5. (n.d.). Retrieved from Biometrics Ideal Test: http://biometrics.idealtest.org/

Chandra, S., Paul, S., Saha, B., & Mitra, S. (2013, May-June). Generate an Encryption Key by using Biometric Cryptosystems to secure transferring of

Data over a Network. *IOSR Journal of Computer Engineering (IOSR-JCE), 12*(1), 16-22.

Cheol-Joo , C., Kwang-Nam, C., Kiseok, C., Jae-Soo, K., & YongJu, S. (2014, November). Enhanced biometric encryption algorithm for private key protection in BioPKI system. *Journal of Central South University, 21*(11), 4286-4290.

Coakes, J. S., & Steed, L. (2009). *SPSS: Analysis without anguish using SPSS version 14.0 for Windows.* John Wiley & Sons, Inc.

Das, A. K. (2011, March). Cryptanalysis and Further Improvement Of a Biometric-Based Remote User Authentication Scheme Using Smart Cards. *International Journal of Network Security & Its Applications (IJNSA), 3*(2), 13-28.

Das, P., Karthik, K., & Garai, B. C. (2012, September). A robust alignment-free fingerprint hashing algorithm based on minimum distance graphs. *Pattern Recognition, 45*(9), 3373-3388.

Das, R. (2012, February). Multimodal biometric systems How they can help to protect against physical and logical threats. *Keesing Journal of Documents & Identity*(37), 1-4.

Deshpande, A., & Joshi, R. B. (2013). Information Security using Cryptography and Image Processing. *IJSRD - International Journal for Scientific Research & Development, 1*(9), 1905-1907.

Devlin, A. (2006). Research Methods: Planning, Conducting and Presentation Research. (pp. 131-135). Belmont: Wadsworth.

Dodis, Y., Ostrovsky, R., Reyzin, L., & Smith, A. (2008). Fuzzy Extractors: How to Generate Strong Keys from Biometrics and Other Noisy Data. *SIAM Journal on Computing, 38*(1), 97-139.

Du, E. Y., Yang, K., & Zhou, Z. (2011, October). Key Incorporation Scheme for Cancelable Biometrics. *Journal of Information Security*, 185-194.

El-Sisi, A. (2011). Design and Implementation Biometric Access Control System Using Fingerprint for Restricted Area Based on Gabor Filter. *The International Arab Journal of Information Technology, Vol. 8, No. 4, October 2011*, 355-363.

Eshwarappa, M. N., & Mrityunjaya, V. L. (2010, August). Bimodal Biometric Person Authentication System Using Speech and Signature Features. *International Journal of Biometrics and Bioinformatics (IJBB), 4*(4), 147-160.

Fazli, S., & Zolfaghari-Nejad, M. (2012, March). An Improved Watermarking Algorithm for Hiding Biometric Data. *International Journal of Science and Engineering Investigations, 1*(2), 11-15.

Frink, A. (2006). How to Conduct Surveys: A Step-by-step Guide. Sage.

Gaddam, S. V., & Lal, M. (2011). Development of Bio-Crypto Key From Fingerprints Using Cancelable Templates. *International Journal of Academic Excellence in Computer Applications, 4*(8), 137-145.

Geethanjali, N., Thamaraiselvi, K., & Priyadharshini, R. (2012, December). Feature Level Fusion of Multibiometric Cryptosystem in Distributed System.

International Journal of Modern Engineering Research (IJMER), 2(6), 4643-4647.

Geetika, & Kaur, M. (2013, April). Fuzzy Vault with Iris and Retina: A Review. *International Journal of Advanced Research in Computer Science and Software Engineering, 3*(4), 294-297.

Hooda, R., & Gupta, S. (2013, April). Fingerprint Fuzzy Vault: A Review. *International Journal of Advanced Research in Computer Science and Software Engineering, 3*(4), 479-482.

Imamverdiyev, Y., Teoh, A. B., & Kim, J. (2013). Biometric cryptosystem based on discretized fingerprint texture descriptors. *Expert Systems with Applications 40 (2013) 1888–1901*.

Jadhav, S. (2014, April). A Review on Template Security Scheme for Secure Biometric Authentication. *International Journal of Pure and Applied Research in Engineering and Technology*, 650-660.

Jain, A. K., Ross, A., & Uludag, U. (2005). Biometric Template Security: Challenges and Solutions. *European Signal Processing Conference (EUSIPCO), (Antalya, Turkey), September 2005*, (pp. 1-4).

Jain, A., Nandakumar, K., & Nagar, A. (2008). Biometric Template Security. *EURASIP Journal on Advances in Signal Processing (2008)*, 1-17.

Jain, A., Ross, A., & Prabhakar, S. (2004, January). An introduction to biometric recognition. *Circuits and Systems for Video Technology, IEEE Transactions, 14*(1), 4-20.

Jaiswal, S., Bhadauria, S. S., & Jadon, R. S. (2011, October). Biometric: Case Study. *Journal of Global Research in Computer Science, 2*(10), 19-49.

Jeny, J. V., & Jangid, C. J. (2013, March). Multibiometric Cryptosystem with Fuzzy Vault and Fuzzy Commitment by Feature-Level Fusion. *International Journal of Emerging Technology and Advanced Engineering, 3*(3), 449-452.

Juels, A., & Sudan, M. (2002). A Fuzzy Vault Scheme. *IEEE International Symposium Information Theory*.

Kannan, D., & Thilaka, K. (2013). Multibiometric Cryptosystem Based On Fuzzy Vault with Biohashing. *IOSR Journal of Electronics and Communication Engineering(IOSR-JECE)*, 34-43.

Kaur, M., Sofat, S., & Saraswat, D. (2010, July). Template and Database Security in Biometric Systems: A Challenging Task. *International Journal of Computer Applications, 4*(5), 1-5.

Li, C. T., & Hwang, M. S. (2010). An efficient biometric-based remote authentication scheme using smart cards. *Journal of Network and Computer Applications*, 1-5.

Malhotra, S., & Kant, C. (2013, May). A Novel approach for securing biometric template. *International Journal of Advanced Research in Computer Science and Software Engineering, 3*(5), 397-403.

Malhotra, S., & Verma, C. K. (2013, June). A Hybrid Approach for Securing Biometric Template. *International Journal of Engineering and Advanced Technology, 2*(5), 72-76.

Maltoni, D., Maio, D., Jain, K., & Prabhakar, S. (2003). *Handbook of Fingerprint Recognition.* Berlin, Germany: Springer.

Maniroja, M., & Sawarkar, S. (2013, May). Biometric Database Protection using Public Key Cryptography. *IJCSNS International Journal of Computer Science and Network Security, 13*(5), 20-28.

Meenakshi, V. S., & Padmavathi, G. (2010, September). Securing Revocable Iris and Retinal Templates using Combined User and Soft Biometric based Password Hardened Multimodal Fuzzy Vault. *IJCSI International Journal of Computer Science Issues, 7*(5), 159-167.

Menariya, D., & Ojha, D. B. (2012, October). A vital application of security with biometric templates. *International Journal of Engineering Research and Applications (IJERA), 2*(5), 328-332.

Morwal, P., Singh, P., & Tripathi, R. (2012). Security in e-Governance using Biometric. *International Journal of Computer Applications, 50*(3), 16-19.

Muthukuru, J., & Sathyanarayana, B. (2013, January). A Survey of Elliptic Curve Cryptography Implementation Approaches for Efficient Smart Card Processing. *Global Journal Of Computer Science and Technology*, *12*(1), 7-12.

Naik, A. K., & Holambe, R. S. (2010). A Blind DCT Domain Digital Watermarking for Biometric Authentication. *International Journal of Computer Applications, 1*(16), 11-15.

Nasir, M. S., & Kuppuswamy, P. (2013, October). Implementation of Biometric Security using Hybrid Combination of RSA and Simple Symmetric Key Algorithm. *International Journal of Innovative Research in Computer and Communication Engineering, 1*(8), 1741-1748.

Nawaz, A., Hossain, F. S., & Grihan, K. (2013). An Energy Efficient ATM System Using AES Processor. *Electrical Engineering Research (EER), 1*(2), 42-47. Retrieved from www.seipub.org/eer

NIST. (2001, November 26). *Advanced Encryption Standard (AES).* Retrieved from National Institute of Standards and Technology (NIST): http://csrc.nist.gov/publications/

Poongodi, P., & Betty, P. (2014, January). A Study on Biometric Template Protection Techniques. *International Journal of Engineering Trends and Technology, 7*(4), 202-204.

Prakash, O., & Bharathan, D. (2012, March). A New Palm Print Based Fuzzy Vault System for Securing Cryptographic Key. *International Journal of Information and Electronics Engineering, 2*(2).

Radha, N., & Karthikeyan, S. (2010, July). A Study on Biometric Template Security. *ICTACT Journal on Soft Computing*(01), 31-41.

Radha, N., & Karthikeyan, S. (2011, July). An Evaluation Of Fingerprint Security Using NonInvertible Biohash. *International Journal of Network Security & Its Applications, 3*(4), 118-128.

Raju, S. V., Vidyasree, P., & Madhavi, G. (2014, February). Enhancing Security Of Stored Biometric Template in Cloud Compuuting Using FEC. *International Journal of Advanced Computational Engineering and Networking*, *2*(2), 35-39.

Ramchander, L., & Deepika, S. (2013, October). An Efficient Implementation of AES-256 Cryptographic Algorithm. *International Journal of Scientific Engineering and Technology Research*, *2*(14), 1557-1562.

Ratha, N. K., Connell, J. H., & Bolle, R. M. (2001). An Analysis of Minutiae Matching Strength. *Proceedings of Third International Conference on Audio and Video-Based Biometric Person Authentication* (pp. 223–228). Halmstad: Sweden.

Ratha, N., Chikkerur, S., Connell, J., & Bolle, R. (2007, April). Generating Cancelable Fingerprint Templates. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, *29*, 561-572.

Rathgeb, C., & Busch, C. (2012). Multi-Biometric Template Protection: Issues and Challenges. *INTECH*, 173-190.

Rathgeb, C., & Uhl, A. (2011, September). A survey on biometric cryptosystems and cancelable biometrics. *Journal on Information Security*, *3*, 1-25.

Sanjekar, P. S., & Patil, J. B. (2013, February). An Overview Of Multimodal Biometrics. *Signal & Image Processing : An International Journal (SIPIJ)*, *4*(1), 57-64.

Schmitt, V., & Jordaan, J. (2013, April). Establishing the Validity of Md5 and Sha-1 Hashing in Digital Forensic Practice in Light of Recent Research Demonstrating Cryptographic Weaknesses in these Algorithms. *International Journal of Computer Applications, 68*(23), 40-43.

Seung-hwan Ju, J., Hee-suk, S., Sung-hyu, H., Jae-cheol, R., & Jin, K. (2013). A Study on User Authentication Methodology Using Numeric Password and Fingerprint Biometric Information. *BioMed Research International*, 1-7.

Stallings, W. (2011). *Cryptography and Network Security Principles and Practice.* New York, United States of America: Pearson Education, Inc.

Tan, Z. (2013). An efficient biometrics-based authentication scheme for telecare medicine information systems. *Przeglad Elektrotechniczny*, 200-204.

Venkatesh, D., Balaji, S., & Chakravarthy, A. (2012, April). Security Evaluation Of Fingerprint Based Authentication. *International Journal of Engineering & Science Research, 2*(4), 158-175.

Westland, J. C. (2010). Lower bounds on sample size in structural equation modeling. *Electronic Commerce Research and Applications, 9*, 476-487.

Yates, D., & Moore, D. (2008). *The practice of statistics.* New York: W.H. Freeman.

Zhou, X., & Tang, X. (2011). Research and Implementation of RSA Algorithm for Encryption and Decryption. *The 6th International Forum on Strategic Technology*, 1118-1121.

APPENDICES

Appendix 1 Letter of Introduction

JOMO KENYATTA UNIVERSITY OF AGRICULTURE AND TECHNOLOGY

SCHOOL OF COMPUTING AND INFORMATION TECHNOLOGY

School of Computing and Information Technology

P. O. Box 62000- 00200

Nairobi, Kenya

Joseph Mwema

P. O. Box 54891- 00200

Nairobi, Kenya

Dear Sir/Madam,

RE: A SURVEY OF ENCRYPTION OF BIOMETRIC FINGERPRINT TEMPLATES USING ENCRYPTION KEYS OBTAINED FROM OTHER BIOMETRIC FINGERPRINT TEMPLATES

I am a postgraduate student at the Jomo Kenyatta University of Agriculture and Technology undertaking Master of Science Degree (Computer Systems). As a component of my course requisite, I am carrying out a survey on Encryption of Biometric Fingerprint Templates Using Encryption Keys Obtained from Other Biometric Fingerprint Templates.

The information gathered from this Questionnaire will be used to assess the challenges experienced by Biometric Systems Developers in protecting biometric templates in storage from adversary attacks.

I am hereby requesting you to assist me by completing the attached questionnaire. Please be assured the information collected through the questionnaire shall be used for the purpose of academic study only and shall be treated in confidentiality.

I will highly appreciate your correspondence.

Yours faithfully,

Joseph Mwema

Appendix 2 Research Questionnaire

A SURVEY OF ENCRYPTION OF BIOMETRIC FINGERPRINT TEMPLATES USING ENCRYPTION KEYS OBTAINED FROM OTHER BIOMETRIC FINGERPRINT TEMPLATES

Section A: Biometric System Developer's Background

1. What is your gender?
   - ○ Female
   - ○ Male
2. What is your age bracket?
   - ○ 20 years and below
   - ○ 21 - 25 years
   - ○ 26 - 30 years
   - ○ 31 - 35 years
   - ○ 36 years and above
3. Have you undertaken any studies, courses in Biometric Systems Development?
   - ○ Yes
   - ○ No
4. How long have you worked as a Biometric Systems Developer?
   - ○ 1 – 5 years
   - ○ 6 – 10 years
   - ○ 11 – 15 years
   - ○ 16 years and above

5. Which Biometric Systems have you developed before?

   ☐ Fingerprints

   ☐ Face

   ☐ Iris

   ☐ Voice

   ☐ Palm Vein Recognition

   ☐ Other(s)

   If you selected **Other(s)** (Please Specify)……

6. In your own understanding based on your experience with biometric systems, do you consider biometrics to be more secure than passwords, PINs or access codes?

   ○ Yes

   ○ No

7. How would you rate your knowledge on Data Encryption?

   ○ Excellent(5)

   ○ Above Average(4)

   ○ Average(3)

   ○ Very Poor(2)

   ○ Poor(1)

8. Which of the following do you think have been the impediments towards wide scale adoption of biometrics? (Select as many as apply)

   ☐ High Costs of Biometric Hardware & Software

   ☐ Known Security Flaws

   ☐ Lack of Expertise to Develop, Implement & Support Biometrics Systems

   ☐ Accuracy (False Acceptance Rate and False Rejection Rate)

☐ Big data size of Biometric Templates in storage space

☐ Other(s)

If you selected **Other(s)** (Please Specify)…….

Section B: Biometric Template Security

1. How do you save Biometric Templates for the Systems you develop?

   ○ Folders

   ○ Databases

   ○ Smart Cards

   ○ USB Modules

   ○ Other(s)

   If you selected **Other(s)** (Please Specify)……
2. Are there measures you use to protect Biometric Templates?

   ○ Yes

   ○ No
3. Do you have policies in place that emphasize on securing biometric templates before they are stored?

   ○ Yes

   ○ No
4. If your answer to 3 above is **No**, What measures have you put in place to mitigate Biometric Template attacks in storage?

   ……..

5. Which Biometric Template Protection Techniques do you use?

   ○ Feature Transformation

   ○ Biometric Encryption

   ○ None

6. If your answer in **5** above is **Biometric Encryption**, please specify which Biometric Encryption method you use?

   ○ Key Binding

   ○ Key Generation Method

7. Which Biometric Encryption scheme(s) do you use in securing Biometric Templates in storage? (Select as many as apply)

   ☐ Fuzzy Vault

   ☐ Water Marking

   ☐ RSA and ECC

   ☐ Fuzzy Commitment

   ☐ Cancellable Biometric

   ☐ None

   ☐ Other(s)

   If you selected **Other(s)** (Please Specify)……

Section C: Efficiency of Encryption Methods

1. With respect to Encryption method used, Please indicate the extent to which you agree or disagree with the following statements.

   SD = Strongly Disagree

   D = Disagree

   N = Neutral

A = Agree

SA = Strongly Agree

The risk of hacking into biometric systems is high	○ SD	○ D	○ N	○ A	○ SA
The encryption methods I use are fool proof	○ SD	○ D	○ N	○ A	○ SA
I am satisfied with the security of biometric templates	○ SD	○ D	○ N	○ A	○ SA

2. Would you keep encryption keys in the same storage space with your encrypted biometric templates?

○ Yes

○ No

3. Which of the following practices do you suppose will improve Biometric Encryption? (Select as many as apply)

☐ Improving Image Acquisition Process

☐ Making Biometric Encryption Resilient against attacks

☐ Improving Accuracy and Security of Biometric Encryption Algorithms.

☐ Use of Multimodal Biometrics

☐ Develop Biometric Encryption Applications

☐ Other(s)

If you selected **Other(s)** (Please Specify)……

4. Would you derive encryption keys from biometric fingerprint templates and use them to protect data in storage?

   ○ Yes

   ○ No

5. In your own opinion, do you think encryption keys derived from biometric templates would be more strong and rich in entropy for encrypting data than a combination of passwords and access codes?

   ○ Yes

   ○ No

   If your answer above is **No**, (Please explain why)……

6. Do you foresee in future, encryption of data using biometric encryption keys become a common practice among systems developers?

   ○ Yes

   ○ No

Section D: Biometric Templates Security Challenges

1. Do you face any Security Challenges with regards to Biometric Template Security?

   ○ Yes

   ○ No

   If your answer above is **Yes**, (Please Specify)…….

2. Which of the following biometric attacks have you ever encountered? (Select as many as apply)

   ☐ Spoofing (Fooling biometric system by using fake finger, face or iris templates)

   ☐ Replay attacks (Beating sensor by running pre-saved biometric template)

   ☐ Substitution attacks (Attacker replacing user's biometric templates with theirs)

   ☐ Tampering (Feature sets getting modified to obtain high verification scores)

   ☐ Trojan attacks (e.g. matcher is replaced with a program that always allows

   ☐ Other(s)

   If your answer above is **Other(s)**, (Please Specify)……..

3. Has your biometric templates storage area ever been compromised?

   ○ Yes

   ○ No

   If your answer above is **Yes**, (What measures did you take to prevent a future occurrence of the same?)

   ……

4. In your own opinion do you consider saving of biometric templates in databases as being the most ideal choice in preference to other storage areas?

   ○ Yes

   ○ No

If your answer above is **No**, (Please Specify why)……

5. If your answer in 4 above is **Yes**, which of the below options would you use to ensure that biometric templates are safely stored in database? (Select as many as apply)

   ☐ Change Database passwords oftenly

   ☐ Use strong passwords

   ☐ Reduce levels of access to database

   ☐ Encrypt biometric templates before saving them in database

   ☐ Other(s)

   If your answer above is **Other(s)**, (Please Specify)……

6. Any other comments?

   ……..