A DATABASE SYSTEM SECURITY FRAMEWORK

Habiba Muhammad Sani[1] and Muhammad Mika'ilu Yabo[2]

[1]Department of Mathematics,Computer Science Unit Usmanu Danfodiyo University, Sokoto-Nigeria
[2]Department of Computer Science, Shehu Shagari College of Education, Sokoto-Nigeria.

ABSTRACT

Database security is a growing concern as the amount of sensitive data collected and retained in databases is fast growing and most of these data are being made accessible via the internet. Majority of the companies, organizations and teaching and learning institutions store sensitive data in databases .As most of these data are electronically accessed , It can therefore be assumed that , the integrity of these numerous and sensitive data is prone to different kind of threat such as{Unauthorized access, theft as well access denial}. Therefore, the need for securing databases has also increased The primary objectives of database security are to prevent unauthorized access to data, prevent unauthorized tampering or modification of data, and to also ensure that, these data remains available whenever needed. In this paper, we developed a database security framework by combining different security mechanism on a sensitive students information database application designed for Shehu Shagari College of Education Sokoto (SSCOE) with the aim of minimizing and preventing the data from Confidentiality, Integrity and Availability threats.

KEYWORDS

Database, Database Security Framework, Confidentiality, Integrity

1. INTRODUCTION

Database technologies are the core component of many information systems. These technologies allow data to be collected, stored and disseminated electronically. They allow data to be retained and shared electronically and the amount of data contained in these systems continues to grow at an exponential rate. So does the need to insure the integrity of the data and secure the data from unintended access.

Database security can be defined as a system or process by which the "Confidentiality, Integrity, and Availability," or CIA, of the database can be protected. Unauthorized entry or access to a database server signifies a loss of confidentiality; unauthorized alteration to the available data signifies loss of integrity; and lack of access to database services signifies loss of availability. Loss of one or more of these basic facets will have a significant impact on the security of the database [1]. Similarly, it refers to the collective measures used to protect and secure a database or database management software from illegitimate use and malicious threats and attacks[2]. Database security issues have been more complex due to widespread use of the internet. Databases are an organizational main resource and therefore, policies and measures must be put into place to safeguard its security and the integrity of the data it contains [3].

According to [4] database is always a key target for adulteration because it contains sensitive and valuable information. Therefore in every database design process the designers need to know and find way of handling the vulnerabilities that can be found in database driven system, it can be through creation stage, during application integration or even during patching and updating, which some of this vulnerabilities are:

- Deployment Failures: The database should be checked when designed to identifies all its functionality, because the common reason of most database vulnerabilities is due to lack of care when they are developed, and a database will only tested for it expected functionality without checking to see if the database is not doing things which it should not be doing them.
- Data leak: Always "back end" is what we considered a databases to be, and this database contains networking interface which help the hacker to capture it traffic and exploit it. For this to be avoided, the use of encryption communication platform is needed.
- Stolen database backups: Another database treats are internal treats, these are those that are inside the organization, they can destroy or steal the backup of a database whether for revenge, money or any other profits.
- The abuse of database features: Miss used of standard features of database made many database to be exploited. Removing the tools that are unnecessary can limited the Future abuse, not by eliminating the exploitation completely, but at least reduction the areas that hackers can study to initiate the attack.
- A lack of segregation: Separation of powers between administrator and user, also duties need to be segregated which can make fraud or theft very difficult by internal staff. In addition, the user account power limitation will make it difficult for a hacker to completely take control of the database.
- Database inconsistencies: Lack of consistency is the common thread that gives room to all vulnerabilities. And it is not a problem of database technology but rather administrative problem; therefore there is a need to consistently develop looking after the database by the database developers and system administrators, so as to be aware of any kind of threats and to take care of any kind of vulnerabilities.

The database security can be enforced and maintain throughout the system life cycle with use of Confidentiality, integrity, and availability (CIA) principles. According to [5] the Confidentiality, integrity, and availability (CIA) are principle model design to ensure information security policies within any given organization. As he explains:-

- Confidentiality: means that the prevention of unauthorised disclosure of information. That is the wrong people will not be able to get any sensitive information, and making sure the authorized or right people can easily get it. Simply means prevention of unauthorised disclosure of information [5].
- Integrity: This involves maintaining the data accuracy, consistency, and trustworthiness throughout its life cycle. Therefore the steps must be taken to make sure that data is not be altered or changed in transit by unauthorized parties. Likewise as results of non human cause such as server crash, means of detection need to be in place to detect any alteration or changes that occur, and a copy of backup must always be available for the effected data to be restored in it correct state. Simply means prevention of unauthorised modification of information [5].

- Availability: meaning that the ability of the system to make it assets accessible to only authorized users and in a timely manner as determined by the systems requirements. Simply means prevention of unauthorised withholding of information or resources [5].

1.1 Mechanisms That Enforce Confidentiality

- Encryption and Decryption Algorithm: It helps with confidentiality as it changes the format of a plaintext (clean message) to non-readable format in order to prevent any unauthorised person to read that data.
- Access Control List: it helps with confidentiality – as only authorised users should be able to access the system.
- A firewall: it also helps with confidentiality by trying to prevent the traffic getting through.
- IDS and IPS systems: they also helps with confidentiality just like firewalls they are continually monitoring traffic that should and should not enter the network and take action accordingly if traffic violates network rules.

1.2 Mechanisms That Enforce Integrity

- Encryption and Decryption Algorithm: It helps with integrity as it changes the format of a plaintext(clean message) to non-readable format in order to prevent any unauthorised person to change the content of the data.
- A message digest or checksum: it helps with integrity by providing authenticity

1.3 Mechanisms That Enforce Availability

- A honeypot: It helps availability- as it is attempting to filter or direct traffic to an area where it can cause no damage but be monitored
- Access Control List: It also help availability- as it effectively filters traffic purposely to filter out unwanted traffic.
- A firewall: It also helps availability- as like an ACL it filters traffic and trying to prevent the unwanted traffic from getting through.

The paper is organised into four sections as follows: Section 1 provides the introductory aspect of the paper. In section2, the paper presents materials and methods of the proposed database security framework. In section 3, the paper described the result and discussion of the work. In section 4 , the paper presents conclusion of the work.

2. Materials and Methods

2.1 Database System Modelling

Systems modelling of the database involve set of interrelated operations (as a whole system) that interacts in different ways to one another, so as to allow the operational and design of one part in the system to have impact to other parts of the system [6]. This research uses UseCase and ClassDiagram of StarUML Case tools to model the system.

2.1.1 Use case diagram:

Below is a UseCase Diagram design using a StarUML CASE tools.

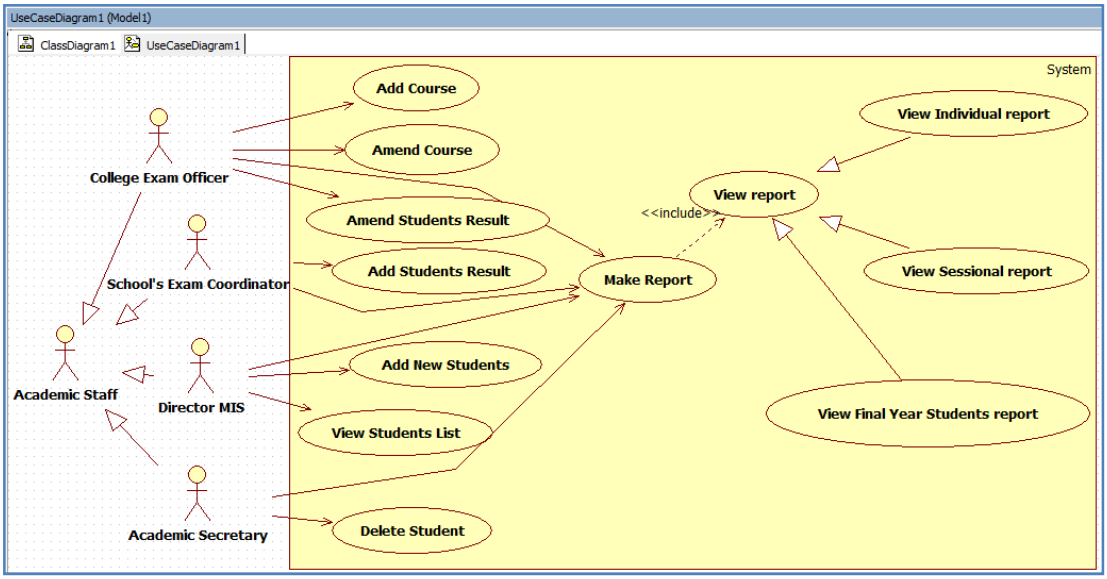

Figure 1. UseCase Diagram Design

2.1.2 Description of Usecase

The students result processing system is a system design to provide an interface for users to add new students, new courses and students exams result. It also allowed the users to view the result for them to make any of the three reports that is, Individual student report, sessional students report and final year students report. The system employs a College Exam officer who will add a new courses and amend the existing courses, it also employ a director MIS who will oversee the addition of new students. The Schools Exams Coordinators were also employs to add new students' results, and finally it employs the College academic Secretary who is responsible to delete students.

2.1.3 Justification of Usecase

The analysis of conceptual class diagram was **justi**fiably design to image all the needed classes' base on the user specification. Also a proper signs were used to characterize their expected relationship with a multiplicity.

2.2 Design class diagrams:

Below is a class diagram design and its layers using a StarUML CASE tools**.**

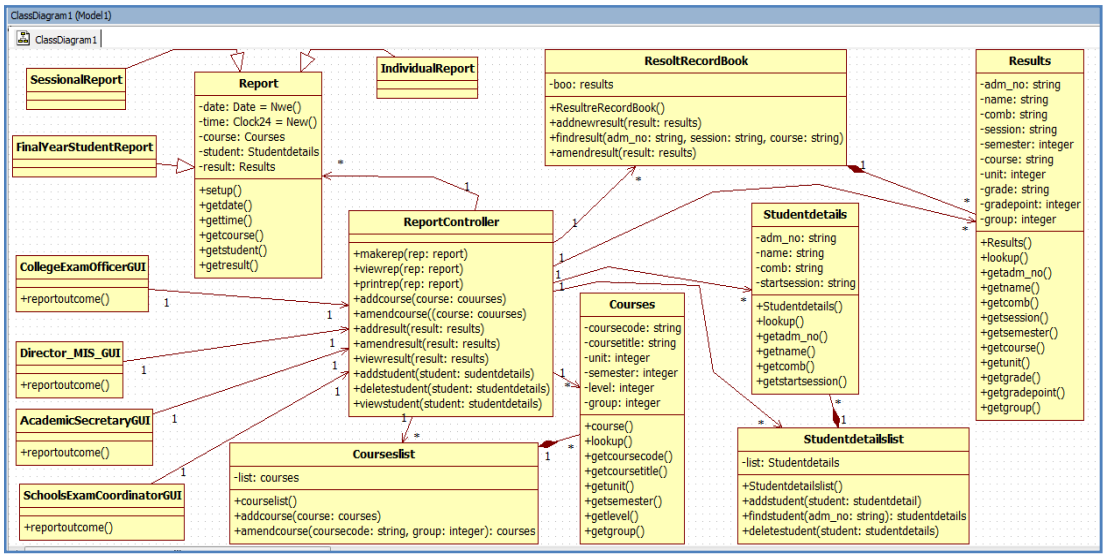

Figure 2. Design Class Diagram

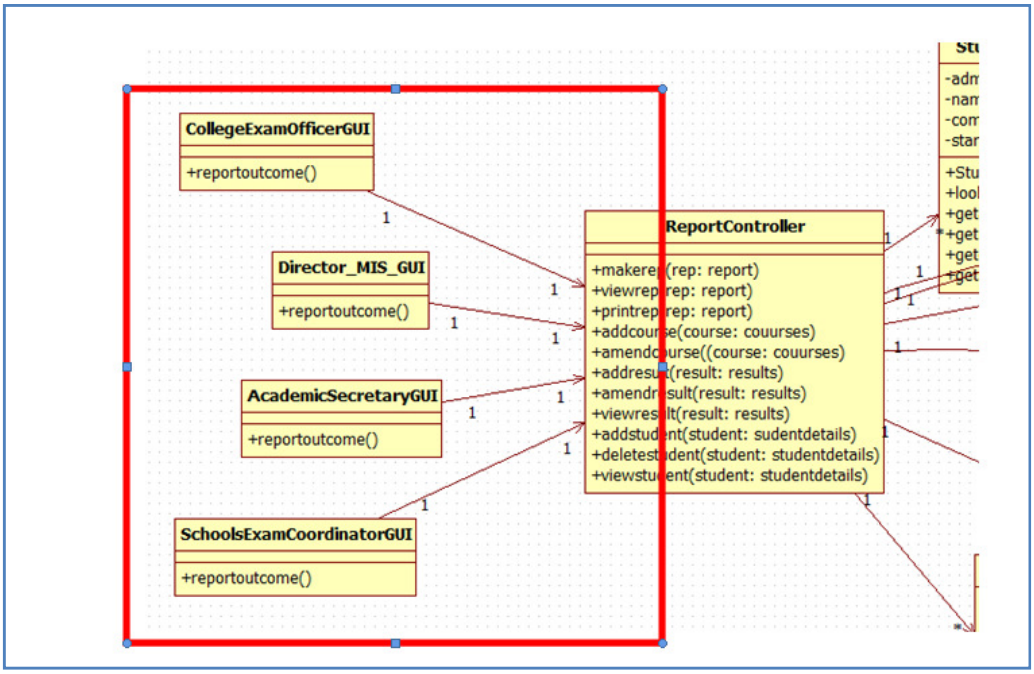

Figure 3. Design Class Diagram showing the User Interface Layer (Presentation Layer)

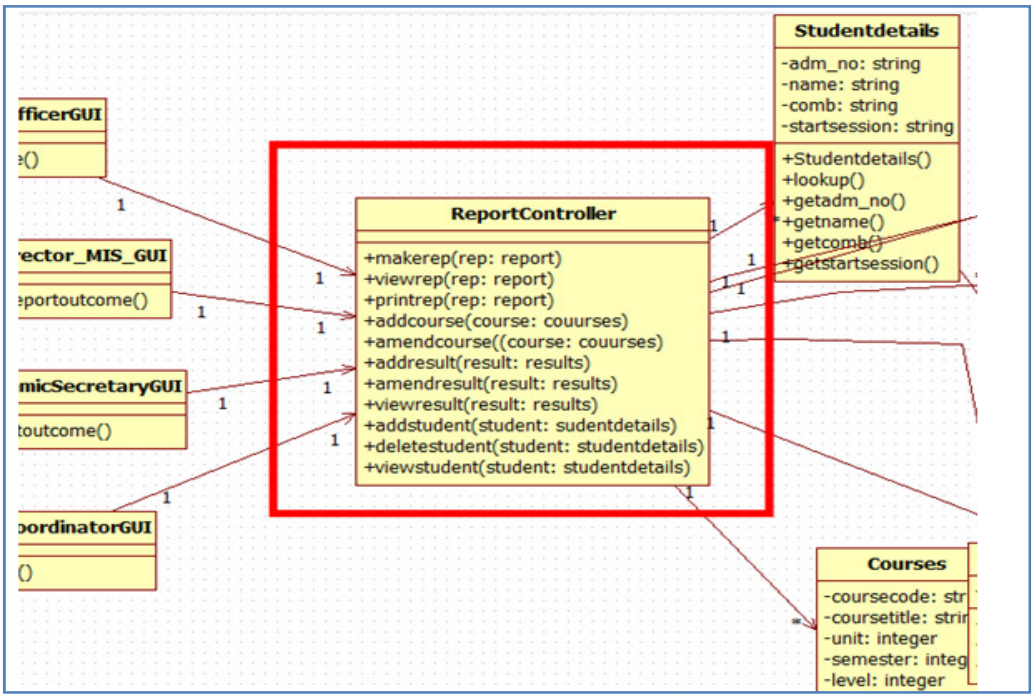

Figure 4. Design Class Diagram showing the control objects layer or application logic layer (Processing Layer).

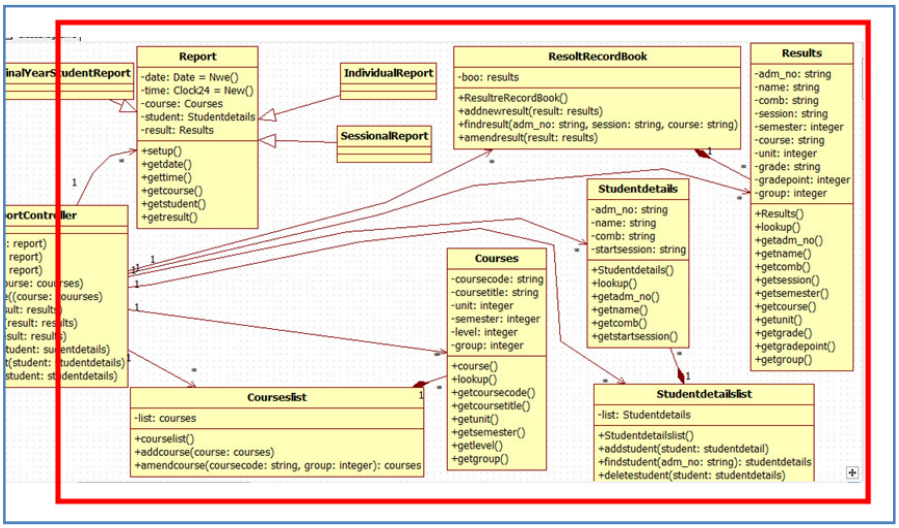

Figure 5. Design Class Diagram showing the Data Layer (Domain Layer)

2.2.1 Description of Design Class Diagrams

The system design diagram was divided into three layers namely, Application logic layer, Data/Domain Layer and User Interface Layer.

- The domain/data layer: is a layer that contains classes design to store data as an object from a business domain, these classes are Courses class, Courseslist class, Studentdetails class, Studentdetailslist class, Results class, Resultsrecordbook class, Report class, IndividualReport class, SessionalReport class and FinalyearstunedtsReport class.
- The user interface layer: is a layer design with classes to handle the input and output process, that is to allow the external actors that are outside the software boundary to send in the request as input and receive the result as output, these classes are CollegeExamOfficeGUI, Director_MIS_GUI, SchoolsExamCoordinatorsGUI and CollegeAcademicSecretaryGUI.
- The control object layer or application logic layer: is a layer that has only one class that used to provide the control logic of the use cases and their coordination, this class is ReportController class. The class serve as interface or bridge between user interface layer data layer where by the user interface layer will send request to application layer and the application layer identify the data layer class that is suitably related with the request and pass that request to the class, it also collect the output of the request from that data layer class and send it to the user interface layer class as the design class diagram indicated using a direct relationship arrows.

2.2.2 Justification of Design Class Diagrams

The researchers justifiably tries to make the design class diagram base on the specification and requirements of the system user. The design class diagram has four user interfaces that will be used by the boundary user to get access to the system, where by the College exam Officer access the system through CollegeExamOfficerGUI, Director MIS through Director_MIS_GUI, Schools Exam Coordinator through SchoolsExamCoordinatorGUI and College Academic Secretary through CollegeAcademicSecretaryGUI.

The design class also has a system controller named ReportController class so that it will give a clear meaning to its functions since it was design to control all the system activities, and the classes of data layer are all design base on the specification of the user.

2.3 Security Framework

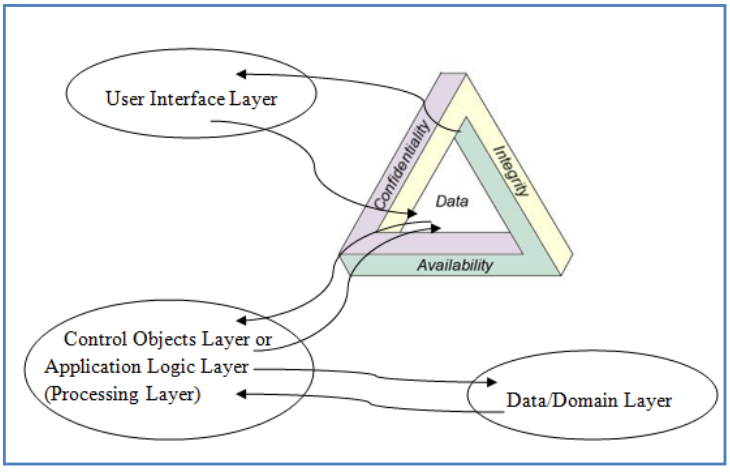

Figure 6. Database security framework Architecture

3. RESULTS AND DISCUSSION

After developing the software and the security measures to safeguard the data stored in the database. The performance of the software was tested against the security measures described/shown in figure 6 above. The result indicates that, the user can only gain access to the data after successfully being authenticated against all the CIA mechanism put in place and all assigned role are made available to the user. Similarly, the user is denied access if not authenticated.

In order to evaluate the above database application against the security mechanisms put in place, the experimental evaluation was carried out by selecting 3 examination officers as administrators to be involved in the use and management of the system. Each of the administrators was allowed to log into the system by entering their details respectively. The overall analysis of the system performance against the security mechanism was captured based on the effectiveness of the user's login details as shown below:

Administrators	WrongLoginDetail	RightLoginDetails
1	Access Denial	Access Granted
2	Access Denial	Access Granted
3	Access Denial	Access Granted

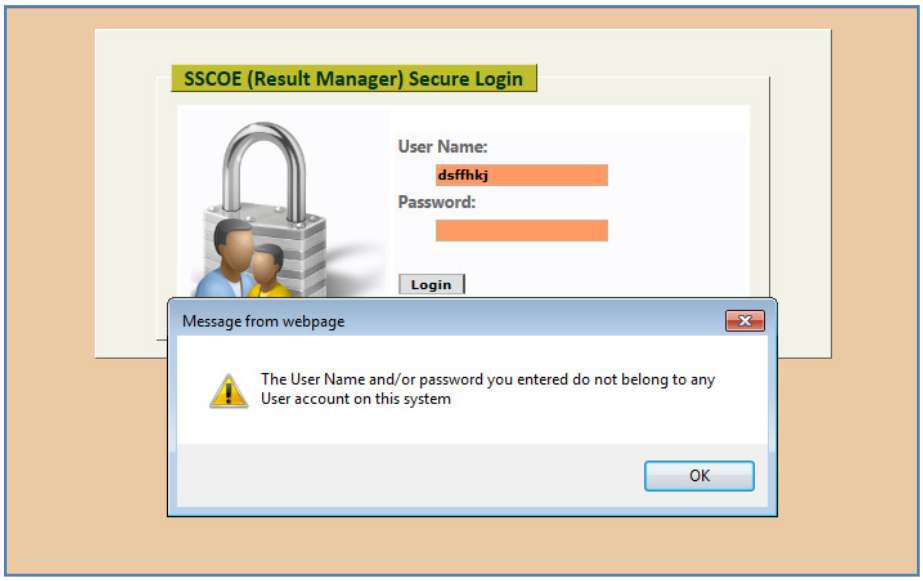

Figure 7. Screen shot of the User (admin) access denial interface

Figure 8. Screen shot of the User (admin) system login access interface

4. CONCLUSION

Despite the increased security concerns in database systems, its benefits outnumbered its shortcoming. However, as database security and in particular data protection from unauthorized users remain important goal in any organizational database management system ,In this paper, the authors proposed database securing framework aimed at minimizing different forms of security concerns against the numerous data stored in the record system of SSCOE database systems. The security framework was designed based on the core facets of database security mechanisms (CIA) to help address the issues of confidentiality, integrity and authenticity as well as availability of data. More so, the system was tested and the results of the study indicated that, the system can only grant access to only the authorized users after successfully authenticated against the CIA mechanisms in place and allowed to view only the roles assigned to them. While on the other hand, the system rejects and denied unauthorised users access to the system and data.

REFERENCES

[1] Bright Hub Inc. (2012). Database Security.[Online] Available from <http://www.brighthub.com/computing/smb-security/articles/61400.aspx.> [November/12 2015]

[2] Techopedia,2015). Databse security. [online] Available from <https://www.techopedia.com/definition/29841/database-security> [November/12 2015]

[3] Singh, S(2009) Database systems: Concepts, Design and applications New Delhi: Pearson Education India.

[4] Osborne, C. (2013) *The top ten most common database security vulnerabilities* [online] available from <http://www.zdnet.com/the-top-ten-most-common-database-security-vulnerabilities-7000017320/> [November/o1 2015]

[5] Gibilisco, S. (2013) *confidentiality, integrity, and availability (CIA)* [online] available from **<http://whatis.techtarget.com/definition/Confidentiality-integrity-and-availability-CIA> [November/24 2015]**

[6] Broy, M., Cengarle, M. V., Gronniger, H. and Rumpe, B. (2011) *Definition Of The System Model* [Online] available from <http://www.se-rwth.de/publications/Definition-of-the-UML-system-model.pdf> [November/16 2015]

AUTHORS

Habiba Muhammad Sani is a BSc. degree holder in Computer Science from the Usmanu Danfodiyo University, Sokoto (UDUS) in Nigeria and also obtained MSc. degree in Computing Information Engineering from the Robert Gordon university, Aberdeen, United Kigdom. Currently lecturing in the Department of Mathematic, Computer Science Unit of UDUS. Her major research interest area is on advanced database systems and Artificial intelligence Systems.

Muhammad Mika'ilu Yabo is a BSc.and MSc. degree holder in Computer Science and Network Computing from the Usmanu Danfodiyo University,Sokoto, Nigeria and Coventry University,United Kingdom respectively. Currently lecturing in the department of Computer Science Shehu Shagari College Of Education Sokoto, Nigeria .His major area of interest is database security and web applications.