Advances In Multidisciplinary & Scientific Research
A Multidisciplinary & Interdisciplinary Journal
Vol. 1, No. 1, June, 2015

Designing a Security-Driven Human Resource Management System

I. Odun-Ayo PSC(+) FDC(+)Ph.D MNCS FNIPM
Director of Production
Defence Industries Corporation
Kaduna, Nigeria
ayosesan@yahoo.co.uk

Abstract
Effcicent human resource management is key to the achievement of organisation's goals and a robust security-driven Human Resource Management System (HRMS) provides the much needed platform for ensuring transparency all through the way. This research presents a robust, multi-level, scalable role-based HRIS System for the Nigerian Air Force. A Model-View-Controller design pattern was employed in the implementation of the NAF HRM system. The implementation was carried out using additional levels of security and encryption. The system consists of four modules such as Admin, personnel, security and reporting, all interacting together to achieve the goal of the system.

Keywords: Design, Security-Driven, Controller, Human Resource Management , Scalable Systems

Aims Research Journal Reference Format:
I. Odun-Ayo (2015): Designing a Security-Driven Human Resource Management System. Aims Research Journal. Vol 1, No. 1 Pp1-29-42.

1. BACKGROUND OF THE STUDY

Human Resource Management is the process of acquiring, training, appraising, and compensating employees and attending to their labor relations, health and safety, and fairness concerns (Dessler, 2004). A Human Resource Management System (HRMS) is also a software application that combines human resources functions including recruiting and training, performance analysis, benefits administration and review into one package (Williams, 2001). Several organizations make use of the Human Resource Information System (HRIS) also known as HRMS. An HRIS is a systematic procedure for collecting, storing, maintaining, retrieving and validating data needed by an organization about its Human Resources (HR), personnel activities and organizational unit characteristics (Alfred, 1982). HRIS in the military is far more complex and far-reaching than personnel management in the private sector. Military personnel management has a responsibility of following the service members from the moment they are recruited into the military till they retire and essentially for the rest of their lives (Garamone, 2006).

Most HRIS are off-the-shelf system suitable for most civil organizations. Presently, countless HRIS exist in the Armed Forces of advanced countries like the United States (United States Air Force Personnel Centre, 2006). These HRIS cannot be adopted by the Nigerian Air Force (NAF) because of the size, capabilities and roles assigned to the NAF. Colin's Dictionary defines security as "the state of being secure or the protection of data to ensure that only authorized personnel have access to computer files". A HRIS system exists in the NAF, but adequate provision was not made for different levels of security. It is not surprising therefore that a lot of discrepancies exist in its personnel management department. This is as a result of insecure data leading to loss of valuable information.

In todays corporate world, Human Resources Management (HRM) has come to play a very critical role in business. It is used in employment, redeployment, training and even motivation. The human resource department of any organization enjoys a central role in not only formulating policies, but also streamlining operational process (Ambler, 2006). The NAF Human Resource Department plays a significant role in determining the quality of officers and airmen, and also in the streamlining of leadership positions.

To make a human resource department more effective and efficient, new technologies are now being introduced on a regular basis. An organization like the NAF which has been playing a leading role in contemporary African conflict resolutions will benefit immensely from the use of a security-driven HRIS.

1.1 Statement Of Problem

The NAF human resource information system falls short of an efficient and effective ways to manage its personnel record, as it is mainly paper based system and extra effort is needed to carry out daily HR task in a manner that is not sufficiently secured. The decision to conduct various HR activities on employee with a view to enhancing their skills is sometimes marred by irregularities due to misplaced or misinformed decisions which arise from inadequate organisation of personnel records. The drawback in the Existing System are as follows:

- Needs of extra manual effort.
- Not very accurate.
- Danger of losing files in some cases.
- Untimely update of personnel records.
- Lack of document security as everybody who can access the data room can access all records.
- Reduces employee's productivity level

1.2 Objective

The main objective of this study is to design and develop a robust, multi-level, scalable role-based security HRM System for the Nigerian Air Force.

2. THE PROPOSED SECURED HRIS SYSTEM

Decisions in assigning the appropriate HR request to the right personnel and timely update of such and general personnel information is an important issue in HR system. The HR administrator should be able to accurately report the right information on all personnel. The decision in making analysis about employee is a prime factor that determines the structure of the HR model. The proposed human resource management information system (HRMIS) as shown in Figure 1, could be incorporated into the automation of NAF HR system to properly organize and manage the personnel record in a more secured and efficient way.

The proposed system provides detailed general information about NAF personnel along with educational, certifications, skills, deployments, and training information. It also provides secured access to these information with various information access level that is flexible hence it can be configured by the system administrator. It enhances the HR management in adding, viewing, updating and reporting various employee details.

As depicted in Figure 1 below, the proposed system is broken down into modules which interact together to achieve the goal of the system. This approach makes it easy to add new modules such as payroll or remove existing modules without having to stop the entire system from working. These modules and the functions they provide are enumerated in Table 1.

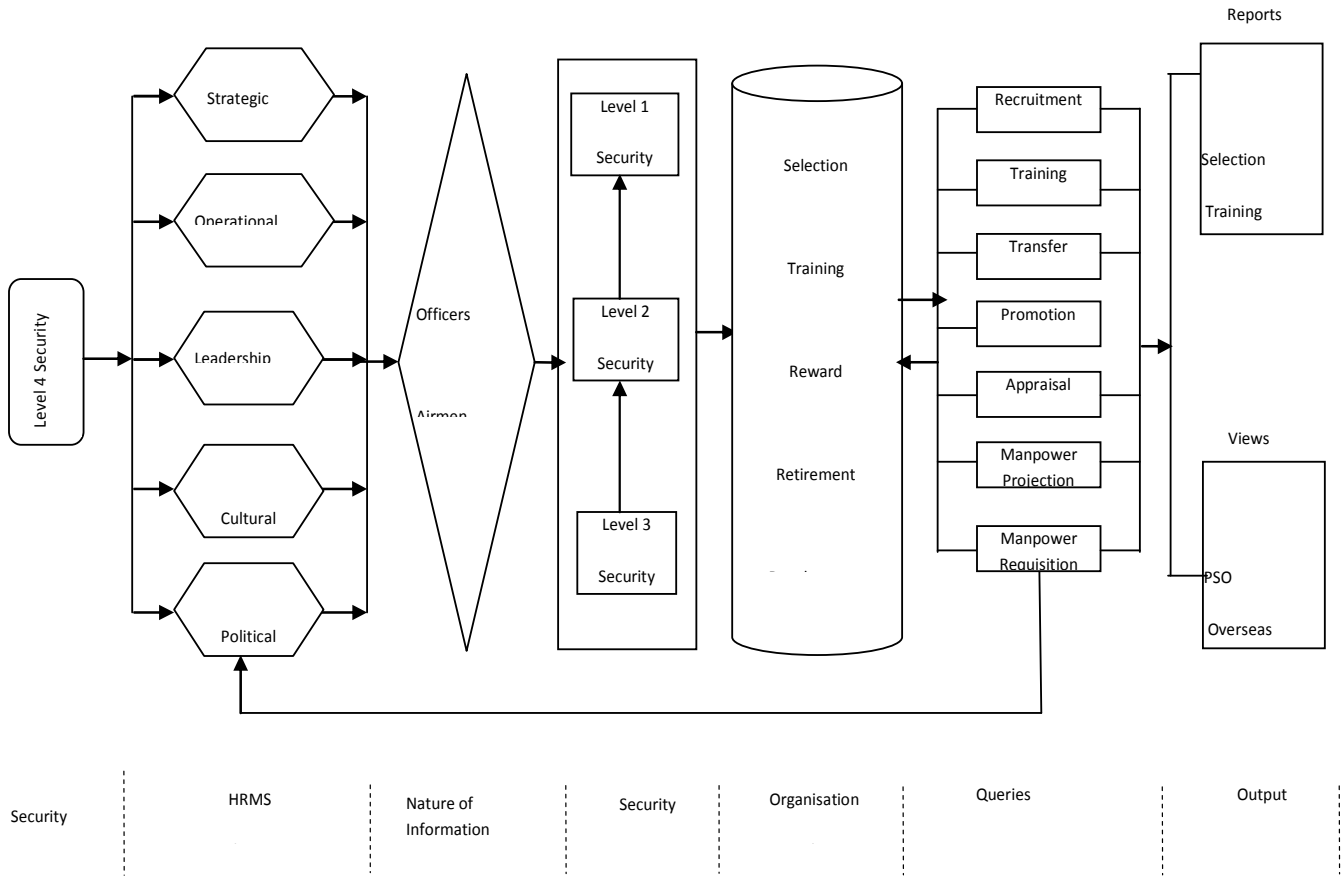


Figure 1: Proposed Secured HRIS System

Table 1 : Summary of the HRIS Modules

S/N	MODULE	FUNCTIONS
1.	ADMIN	1. Add users 2. Manage existing users 3. Manage system settings (units, rank etc.) 4. Users access control management
2.	PERSONNEL INFORMATION	1. Add personnel details 2. Update personnel details 3. Update personnel educational details 4. View personnel nominal roll 5. Create training record 6. Update personnel training record View personnel training records.
3.	REPORTING	1. View/print personnel details 2. View/print personnel training history 3. View/print personnel nominal roll 4. View/print system users list 5. View/print personnel educational qualifications 6. View/print personnel deployment history
4.	SECURITY MODULE	1. Handles users authentication and authorization 2. Encrypts in coming data 3. Decrypts outgoing data

The various users of the system are assigned roles/actions that they can perform in the system with high level of authorisation and authentication mechanism to enforce total security of the system and the information it manages. In order to ensure that operations in the system are role-based, the users are classified into two categories: Admin and Personnel.

Admin refers to the user that has the rights and priviledges assigned to him/her to add/modify records in the database of the HRIS. He/she has the right to Add/Modify all employees/officers records, Add/Modify all training details, and can as well check/view other employee and training details.

Personnel refers to the class of users in the HRIS that when they login, can only check/view their employment and training details.

3. SYSTEM DESIGN

System design is the process or art of defining the architecture, components, modules, interfaces, and data for a system to satisfy specified requirements (Dubberly, 2006). One can see it as the application of systems theory to product development.

3.1 Use Case Diagram

A **use case** in software engineering is a description of a system's behavior as it responds to a request that originates from outside of that system (Booch et al, 1998). In other words, a use case describes "who" can do "what" with the system in question. The use case technique is used to capture a system's behavioral requirements by detailing scenario-driven threads through the requirements. Figure 2 is a Use Case for the proposed system.

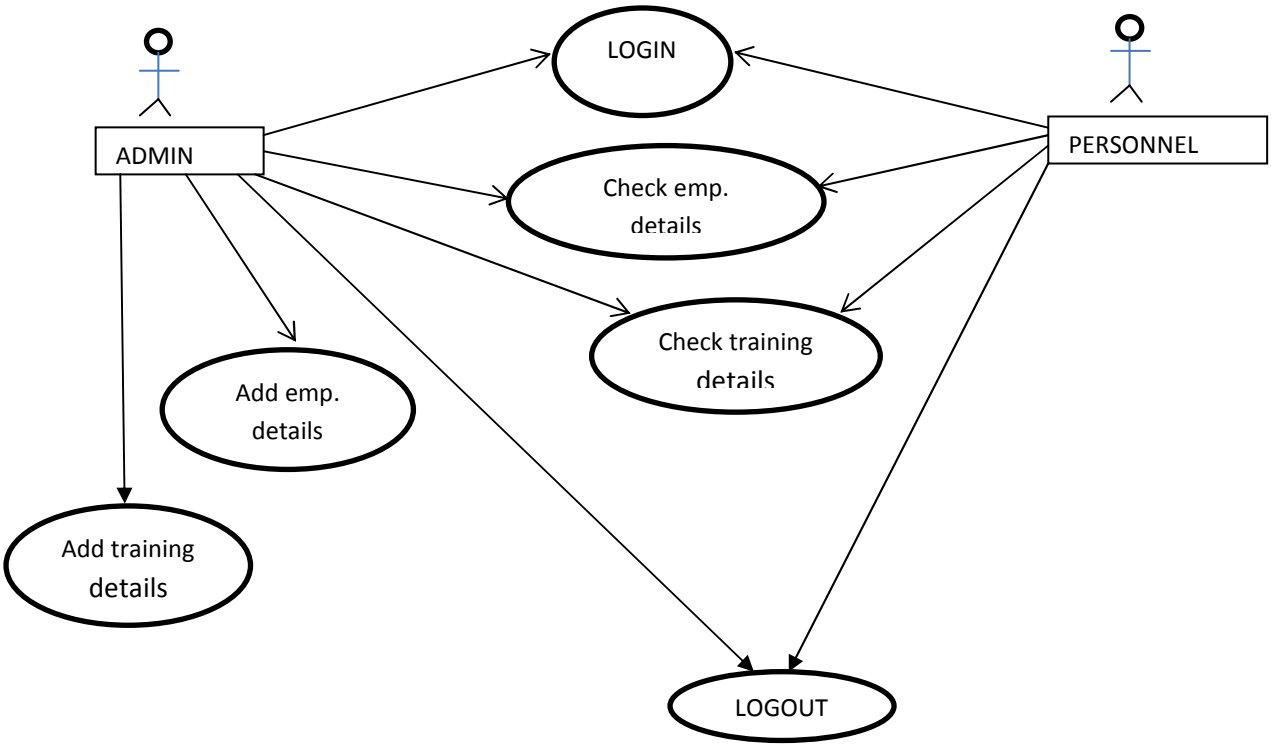


Figure 2: Use Case Diagram For The Proposed HRIS

3.2 Class Diagram

Class diagrams are the most common diagrams found in modeling object-oriented systems (Malik, 2003). A class diagram shows a set of classes, interfaces, and collaborations and their relationships. Graphically, a class diagram is a collection of vertices and arcs. Figure 3 shows the Class Diagram for the system under design.

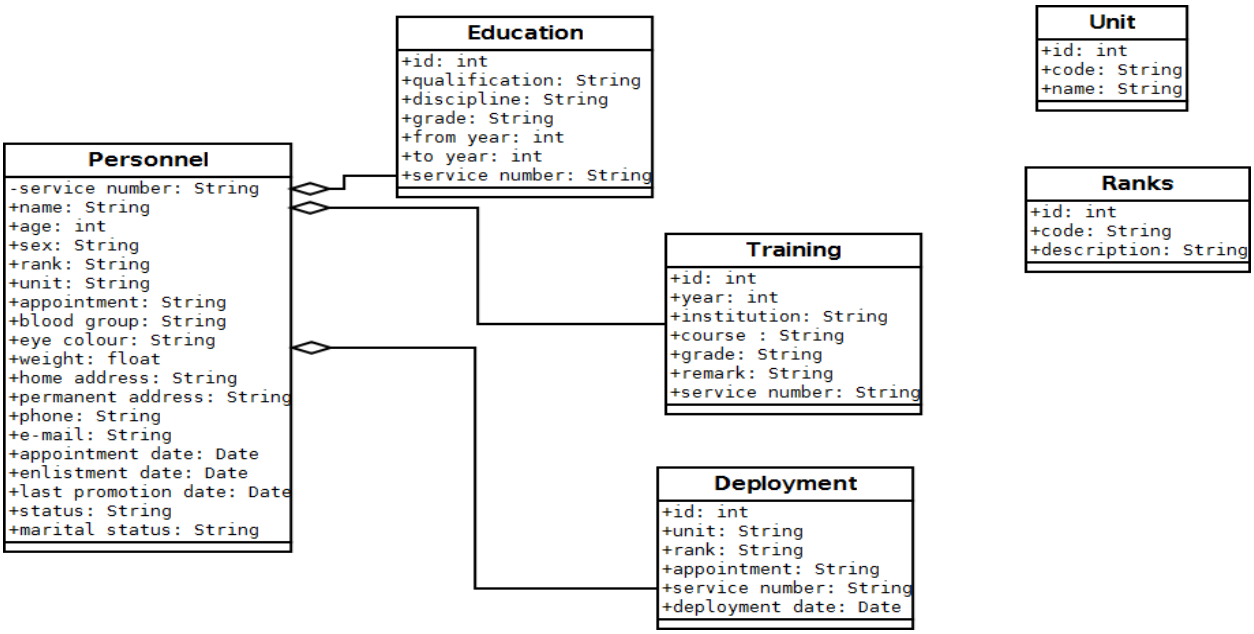


Figure 3: Class Diagram For The Proposed HRIS

3.3 Activity Diagram

An Activity Diagram in Figure 4 is essentially a flow chart showing flow of control from activity to activity. They are used to model the dynamic aspects of as system. They can also be used to model the flow of an object as it moves from state to state at different points in the flow of control (Sunye et al, 2008). An activity is an ongoing non-atomic execution within a state machine. Activities ultimately result in some action, which is made up of executable atomic computations that result in a change of state, this distinguishes a use case diagram from all other kinds of diagrams is its particular content.

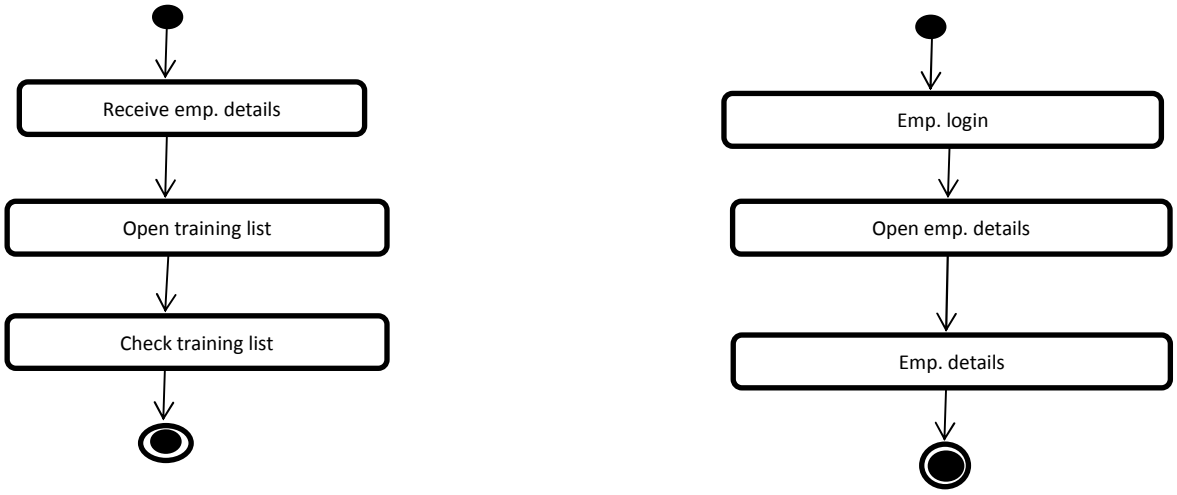


Figure 4: Activity Diagram

3.4 Dataflow Diagram

In designing a system, multiple data flow diagrams are required to represent a system. Figure 5 shows the context diagrams for the Nigerian Air Force Human Resource System. The context diagram represents the entire system under investigation. This diagram is drawn to clarify and agree on the scope of the investigation.The system under investigation is represented as a single process, connected to external entities by data flows (Weaver, 1993). A context diagram clearly shows the interfaces between the system under investigation and the external entities with which it communicates. Therefore, whilst it is often conceptually trivial, a context diagram serves to focus attention on the system boundary and can help in clarifying the precise scope of the analysis (Kozar, 1997).

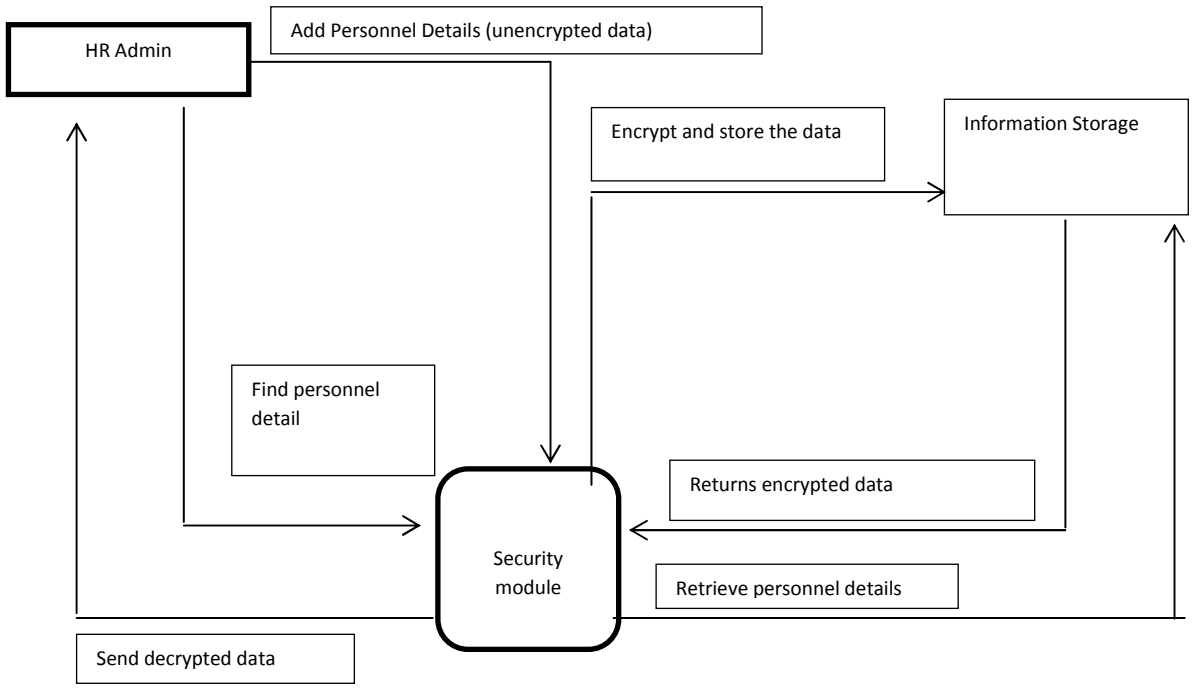


Figure 5: Context Diagram

3.5 Level-0 Diagram

A level-0 diagram is a diagram showing the system itself. It pictures the major processes along with the external entities, data stores and data flow. It is a single, top-level diagram of the system, and does not describe each process in detail. Parts of the diagram can be expended or exploded using more detail sub diagrams. It describes the overall processing of the system, show one process for each major processing step or functional requirement (Avison and Fitzgeraild, 1991). Data flows from the context appear on system diagram also (level balancing). It can show a single data store to represent all data in aggregate at this level. It can also draw duplicate sources, sinks and data stores to increase legibility as shown in Figure 6.

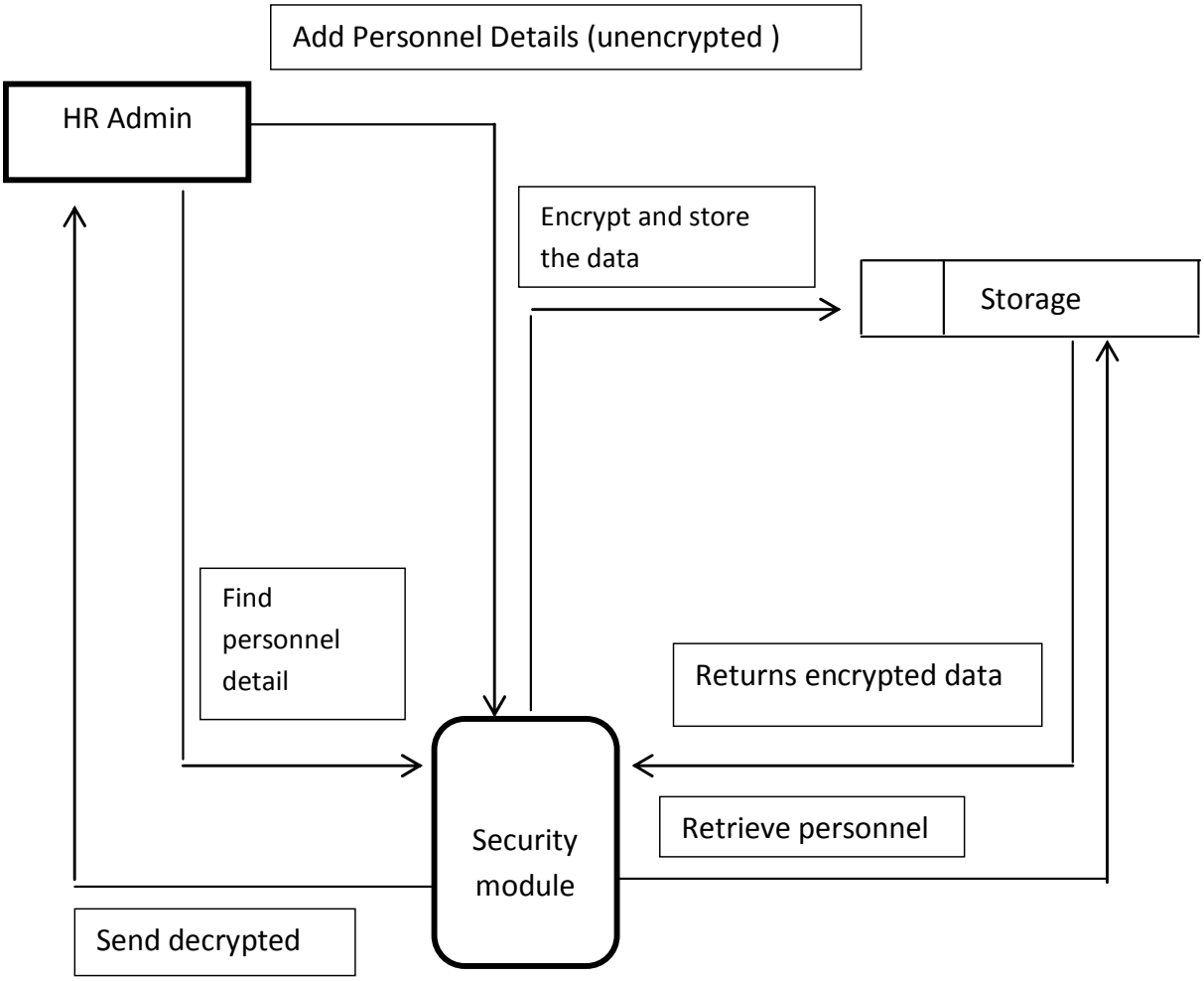


Figure 6: Level-0 Diagram

3.6 Data Flow Diagram

The data flow diagram in Figure 7 gives an overview of the security process in the proposed implementation.

Security Mechanisms

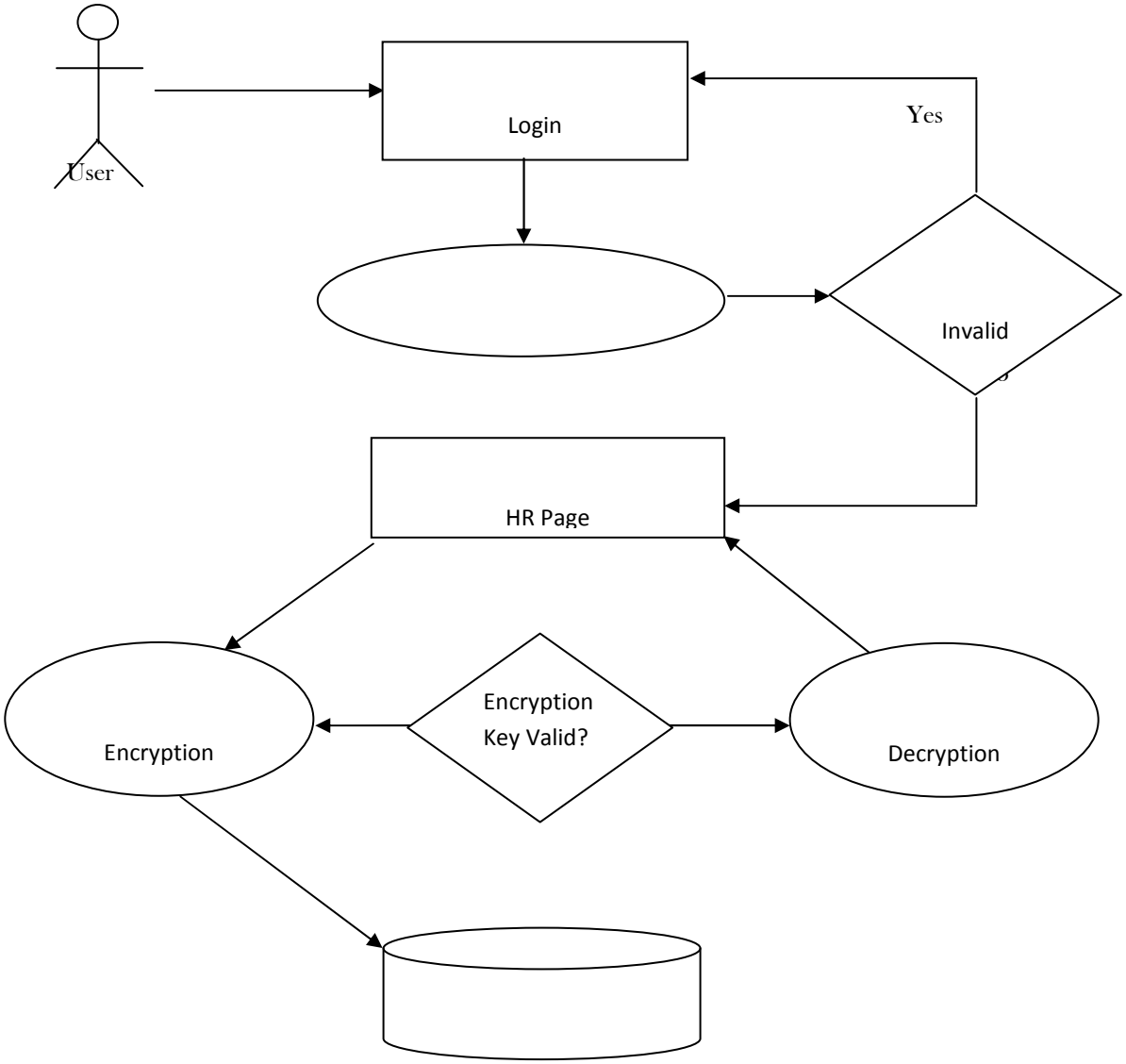


Figure 7: Security Mechanisms

4. COMPARATIVE ANALYSIS OF HUMAN RESOURCE MANAGEMENT SYSTEMS

Human resource systems involved in this comparative analysis include Orange HRM, Nigeria Defence College HRM (NDC HRM), Nigeria Air Force HRM (NAF HRM). See (Odun-Ayo, 2014) for detailed discussion on each of the system. The Nigeria Air Force Human Resource Management (NAFHRM) System is specifically built for use in highly restricted establishments like the Nigerian Air Force. It has a superior application security layer for securing operations within the system. In order to highlight the advantages and disadvantages of the applications selected for this comparative analysis certain areas common to these applications will be analysed.

These areas are namely: (i) User Authentication; (ii) User Authorisation; (iii) Operation Security Levels and (iv) Data Encryption. Each of the above bases of comparisons is described and all three human resource applications are analysed under each of the parameters.

(i) User Authentication

In computing user authentication is known as a process or set of processes that enable the system to confirm that a user is whom he/she say they are. A typical authentication process involves the system collecting login credentials (in most cases a username and a password) from the user. Once the system collects these credentials from the user it searches for matching credentials that are stored in the system's database. If there is a match, the system allows the user access and displays the next screen the user should see. If there is no match the system notifies the user with a custom message. Figures 8 – 10, are screen shots of how each of these various human resource systems implement user authentication.

Figure 8 depicts how the Orange HRM system accepts the user's login credentials. This is then compared to user credentials stored on the database. The major limitation with Orange HRM is its inability to transfer data over a secure network connection.

Figure 8: Orange HRM User Authentication

Figure 9 shows how NDC HRM accepts the user's login credentials. This is then compared to user credentials stored on the database. The major limitation with NDC HRM Applicantion is its inability to transfer data over a secure network connection.

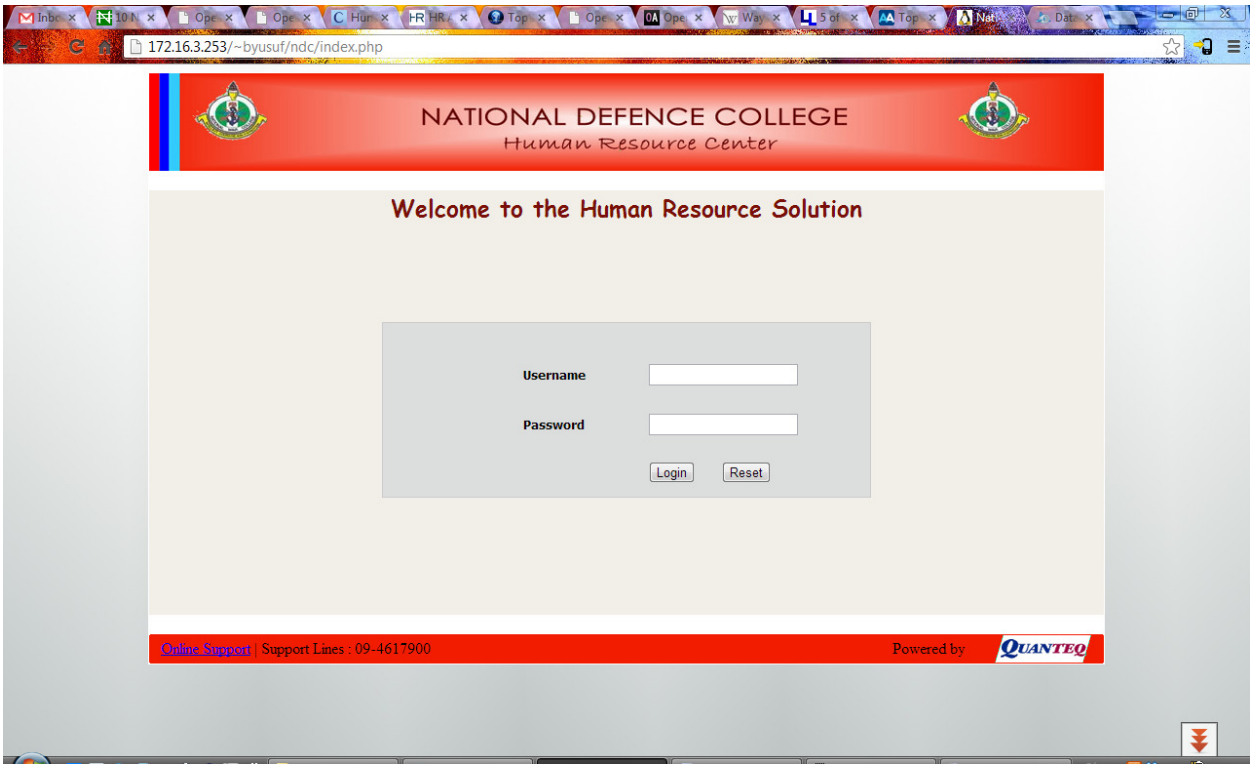


Figure 9: NDC HRM User Authentication

Figure 10 shows the screenshot of the login page of NAF HRM. The user's login credentials are accepted and compared with the records in the data store. Since NAF HRM is web based, it employs a secure (HTTPS) connection for transferring data to and from the Google server.

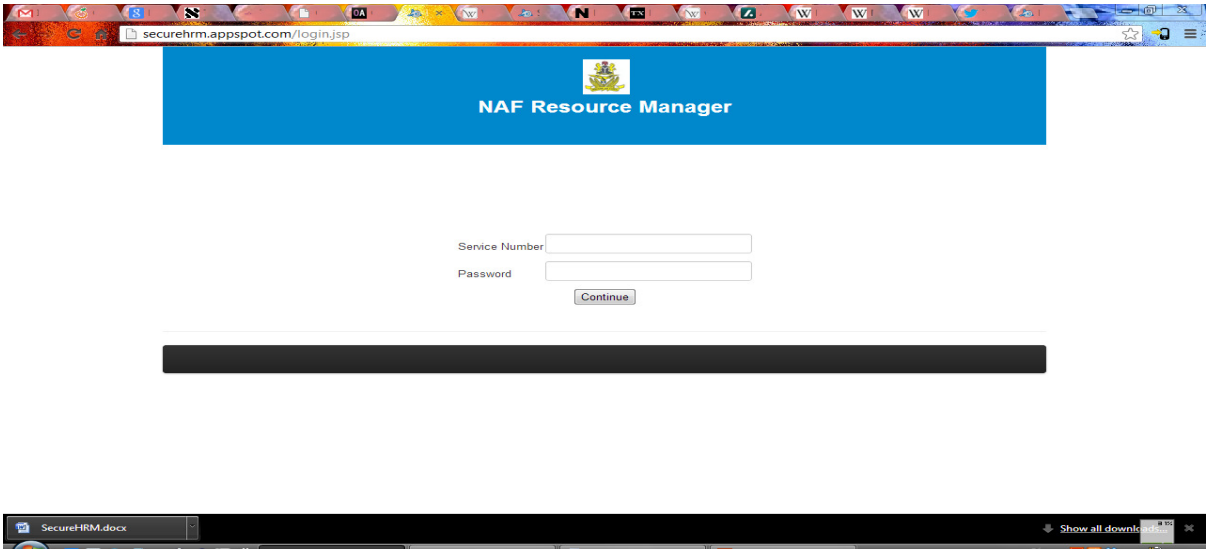


Figure 10: NAF HRM Login Screen

From the above user authentication approaches and the need for organisations to secure their human resource data, it can be seen that the first point of interaction with the user and the system for both Orange HRM and Open Applicant fail because they do not offer a secure connection for transferring the user's sensitive login credentials. Exploiting such vulnerability requires some skill on the part of the attacker, but it is possible to steal the user's data over the network. It is for this reason that NAF HRM employs a secure HTTPS connection when transferring user login credentials to and from the server. Using such a

connection allows all data transferred over the network to be encrypted, hence making it near impossible for an attacker to intercept and decrypt.

(ii) User Authorisation

Once a user says who he/she, the next thing any computer system will do is to determine what the user is allowed to do or view on the system. The process or processes involved in determining what a user can do or view on a system is known as authorisation. Different systems employ different ways of assigning and detecting what a user is authorised to do. Orange HRM, Open Applicant and NAF HRM will all be compared on this.

Orange HRM uses a role based technique to control user access to the system while the NDC HRM does not provide any interface for user authorisation. This has a drastic drawback as the admin user will have to remember and run scripts in order to configure and setup user authorisation. This makes the application hard to use and implement in an organisation. The NAF HRM like Orange HRM uses a role based model to govern user authorisation on the system. The screenshot in Figure 11 is the user management module for setting up user authorisation.

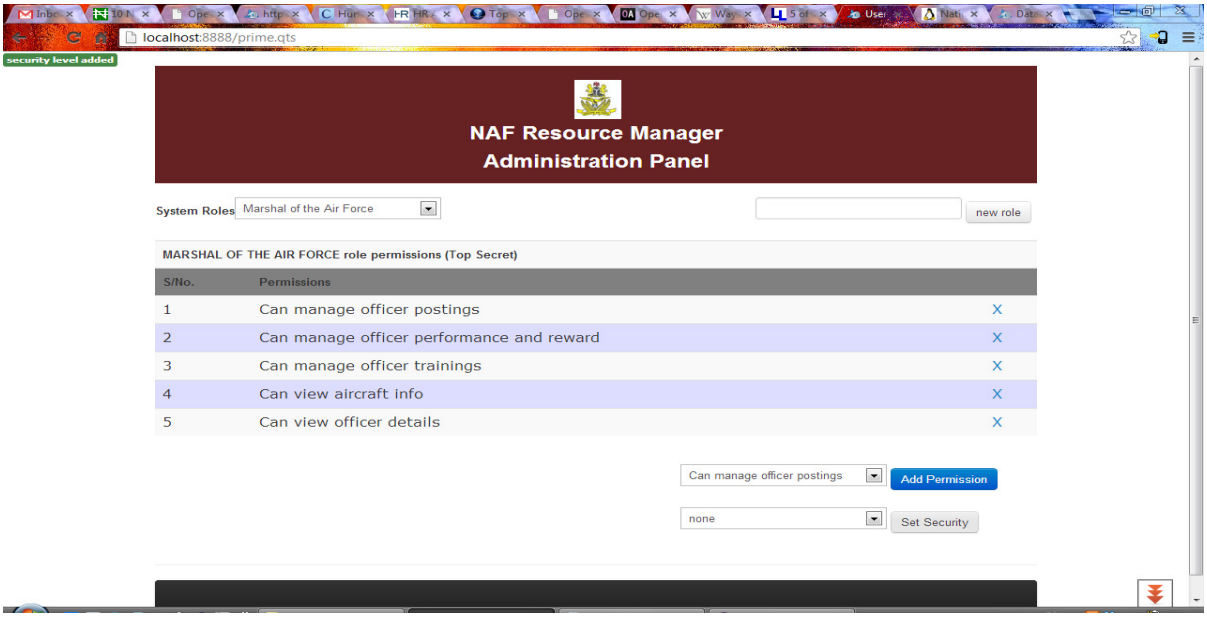


Figure 11: NAF HRM Role and Permission Settings Screen.

NAF HRM requires that ranks (Pilot officer – Marshal of the Air Force) be created first with permissions assigned to them before users are created and saved. NAF HRM uses permissions that are clearly spelt out as to what they allow the user to do. For example one of the permissions available is called "Can view aircraft info", from the name of the permission it can clearly be seen that with this permission the user is allowed to "view" – "aircraft info". This manner of managing permissions is far more user friendly than specifying "edit" or "view" or "delete", which is employed by Orange HRM.

(iii) Operation Security Levels

Users may be authenticated and authorised to view or manage a certain aspect of an application but there are situations whereby an added security level will be required especially when there are several aspects of the same operation or feature in the application or members of the same rank. For example, two ranks maybe permitted to view aircraft info but a situation may arise whereby the admin may want to allow one rank to continue view aircraft info while denying the other. Now, instead of revoking the permission on one rank, the admin may just decide to alter the security level assigned to that rank. This way, several operations in the system can be control by altering their security levels. Hence, this gives a more efficient way of managing users in any human resource management system. None of the highlighted human resource management systems excluding NAF HRM implement this feature. Operation Security Levels will be further discussed within the implementation of NAF HRM.

There is a need to secure operations on the NAF HRM so as to add another layer of security and functionality, in doing this four levels of security used by the military has been implemented in NAF HRM, they are namely in ascending order: (i) Restricted; (ii) Confidential; (iii) Secret and (iv) Top Secret. Figure 12 shows the screen where security levels are assigned to ranks in the NAF HRM

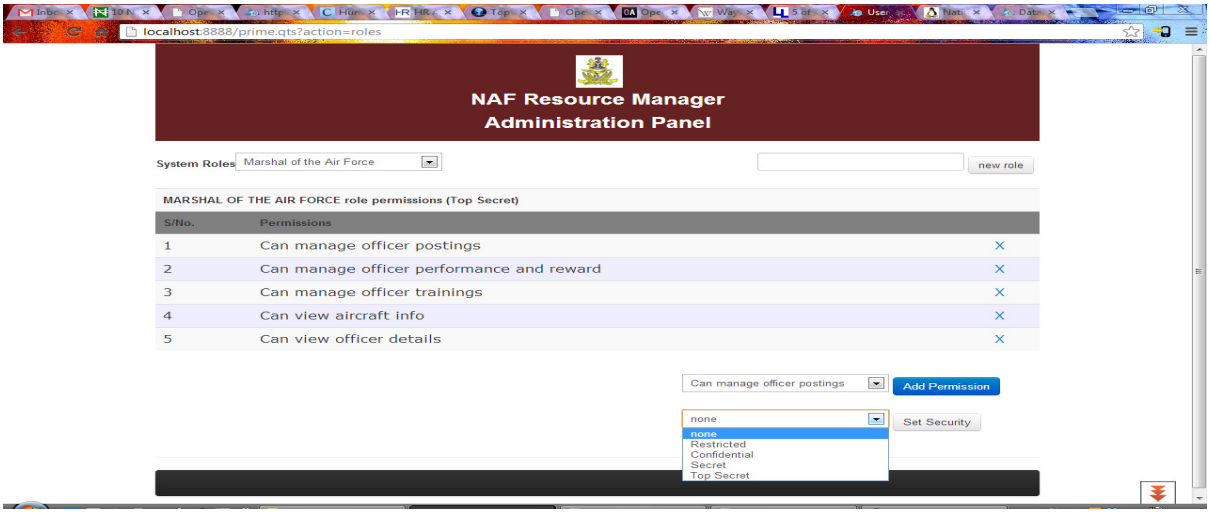


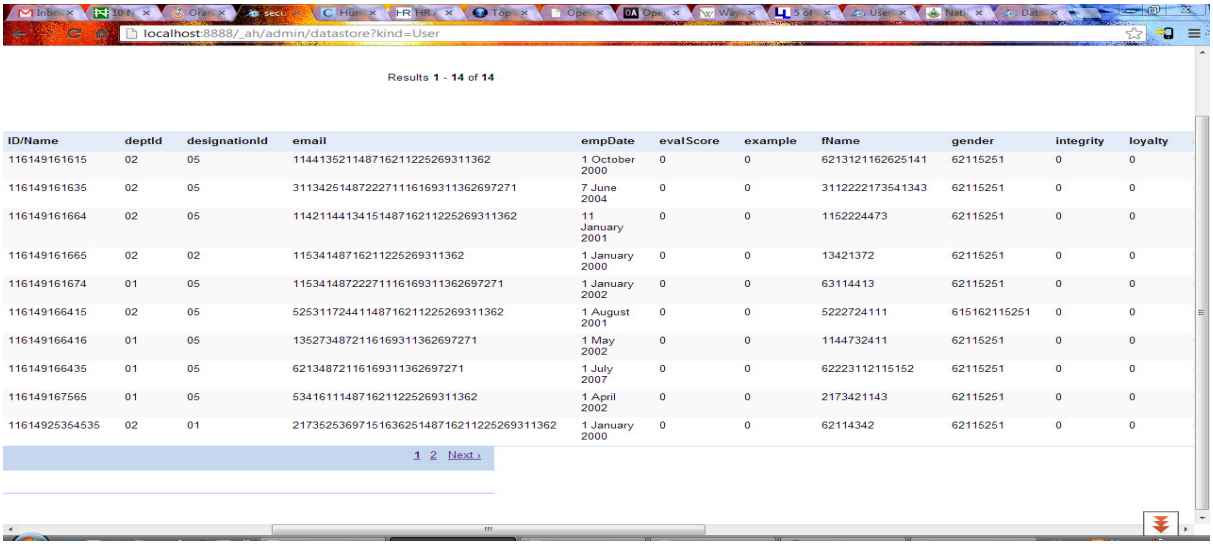
Figure 12: Rank/Permission Management Showing Security Levels.

(i) Data Encryption

Human resource systems are data intensive and all records are stored in one form of a database or the other. This database stores all the records captured by the application and is commonly the target for computer hackers. Security is usually not thought about until the application is developed and then fixes are pushed out on a regular basis. Therefore, almost all public human resource management Systems apply little or no data encryption at all. On the other hand, the NAF HRMS is deployed on a public domain with encrypted data, below is a comparison of the highlighted human resource management systems and a view as how they store their data.

Despite Orange HRM's ability to store large volumes of data, it still keeps data in plain text format in its database. This makes Orange HRM a soft target for computer hackers.

The NDC HRM also stores data in plain text format with no data encryption whatsoever. However, NAF HRM employs full data encryption. All user data stored is encrypted using a custom encryption algorithm. This means that even if the database is hacked and stolen the data stolen will be of no use to the perpetrators. Figure 13 shows how data is stored in the database.



ID/Name	deptId	designationId	email	empDate	evalScore	example	fName	gender	integrity	loyalty
116149161615	02	05	114413521148716211225269311362	1 October 2000	0	0	6213121162625141	62115251	0	0
116149161635	02	05	311342514872227111616931136269727 1	7 June 2004	0	0	3112222173541343	62115251	0	0
116149161664	02	05	114211441341514871621122526931 1362	11 January 2001	0	0	1152224473	62115251	0	0
116149161665	02	02	115341487162112252693113 62	1 January 2000	0	0	13421372	62115251	0	0
116149161674	01	05	1153414872227111616931136269727 1	1 January 2002	0	0	63114413	62115251	0	0
116149166415	02	05	5253117244114871621122526931 1362	1 August 2001	0	0	5222724111	615162115251	0	0
116149166416	01	05	1352734872116169311362697271	1 May 2002	0	0	1144732411	62115251	0	0
116149166435	01	05	6213487211616931136269727 1	1 July 2007	0	0	62223112115152	62115251	0	0
116149167565	01	05	5341611148716211225269311362	1 April 2002	0	0	2173421143	62115251	0	0
11614925354535	02	01	2173525369715163625148716211225269311362	1 January 2000	0	0	62114342	62115251	0	0

Figure 13: NAF HRM Data Store Screen.

From the figure above it can clearly be seen that all user records are encrypted. These records appear in form of numbers when viewed from the database but appear as plain text when view from the application by any user with the appropriate privileges. This ensures that even if the data is stolen all the person or group of persons will have is a bunch of numbers which remains meaningless until decrypted. As mentioned earlier the encryption algorithm is custom made and cannot be decrypted using known standard decryption approaches.

5. CONCLUSION

In managing employees, human resource managers have to assimilate masses of data, convert that data into information, form conclusions about that information and make decisions leading to the achievement of organisational objectives. Managers administer the personal activities associated with company employees; recruiting, training, promoting, demoting, and recordkeeping. Information technology has made it easier and cheaper for managers to gather and maintain an infinite amount of data about present and prospective employees.

An essential component in the success of managing this data is the Human Resource Information System (HRIS), a data base of personal information about each employee. Unfortunately, almost all organizations that use information technology in any substantial way are also struggling to maintain effective information security. The study established a robust, multi-level, scalable security HRM System for the Nigerian Air Force. The research work examined several existing HRIS models and to this end: A secured, roled-based HRIS that can be used by the NAF and other related organisations was designed and implemented. A Model-View-Controller (MVC) Design pattern was employed in the implementation of the NAF HRM system. The implementation was carried out using additional levels of security and encryption.

6. CONTRIBUTION TO KNOWLEDGE

This research establishes a design and implementable secured HRMS for the Nigerian Airforce.

REFERENCES

1. Alfred, W.J. (1982). HRIS Development. Wiley, John & Sons.
2. Ambler, S.W. (2006) "Justifying a Software development Project". Ambysoft, Vol. 30, No. 15, pp.3-6.
3. Avison D. E., Fitzgeraild A(1991) "Information Systems Development". Blackwell.
4. Bagshaw M. (2004) "Is diversity divisive? A Positive Training Approach", *Industrial and Commercial Training*. Vol 36, No 13, pp. 153-157
5. Booch Grady, Rumbaugh James and Jacobson Ivar. (1998) "The Unified Modeling Language User Guide". Addison-Wesley.
6. Dessler, G. (2003) "Human Resource Management", 9th edition, Prentice Hall
7. Dessler, Gary (2004) Human Resource Management. Pearson Education
8. Hugh Dubberly (2006) "What is System Design?".
9. http://www.dubberly.com/articles/
10. Jim Garamone. (2006) New System Integrates Military Pay, Personnel System. US Armed Forces Press service.
11. Kozar K. A. (1997) "The Techniques of Data Flow Diagramming" http://spot.colorado.edu/~kozar/DFDtechniques.html/ Retrieved 20 July 2006.
12. Malik A. (2003) "Design XML Schemas using UML". IBM DeveloperWorks. http://www.ibm.com/developerworks/library/x-umlschem/
13. Odun-Ayo (2014) Security-Driven Human Resource Management System. Ph. D Thesis. University of Benin, Benin City, Nigeria.
14. Simon Williams (2001) "The Associative Model of Data". From http://en.wikipedia.org/wiki/Hierachical_model_of_data. Retrieved 5 Oct 2008
15. Sunye G., Le Guennec A. And Jezequel M. (2008) "Design Patterns Applications in UML". IRISA/CNRS. Cedex.
16. United States Air Force Personnel Center (2006). AFPC Site Index.
17. Weaver, P. L. (1993) "Practical SSSADM", Pitmant.