

Cloud-Based Security Driven Human Resource Management System

Isaac ODUN-AYO^{a,1} Sanjay MISRA^a Nicholas OMOREGBE^a Emmanuel ONIBERE^b
Yusuf BULAMA^b and Robertast DAMASEVIČIUS^c

^aCenter of ICT/ICE Research, CUCRID Building, Covenant University, Ota, Nigeria

^bUniversity of Benin, Benin-City, Nigeria

^cKaunas University of Technology, Kaunas, Lithuania

Abstract. With the emergence of cloud computing, it has become easy to store large volumes of data in the cloud to enhance Human Resource Management (HRM), based on the elasticity and scalability that cloud computing offers. This paper proposes the OnibereOdunayoSecurity-4 (OOS-4) security model for Human Resource Information System (HRIS) deployed on a cloud platform. The OOS-4 framework is a holistic and integrated model that is expected to allow for better interrelatedness of the various components of a HRM organization with adequate consideration for security. Furthermore, utilizing the Platform as a Service (PaaS) cloud computing architecture, the model was implemented using the Google App Engine. The result is a scalable application in which the data in storage is encrypted and visible on the Google Cloud Platform data store. The application is secured by proving encryption for data in storage on the Google Cloud Platform. The application will enhance HRM.

Keywords. Cloud Computing, Human Resource Management System, Platform as a Service, Google App Engine

1. Introduction

“HRM is the process of acquiring, training, appraising, and compensating employees and attending to their labor relations, health and safety, and fairness concerns” [1]. A HRM 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 [2]. 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” [3]. In today’s 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 [4]. To make a human resource department

¹ Corresponding Author, Isaac Odun-Ayo, Department of Computer and Information Sciences, Covenant University, Ota, Nigeria; E-mail: isaac.odun-ayo@covenantuniversity.edu.ng.

more effective and efficient, new technologies are now being introduced on a regular basis.

“Cloud computing is an information processing model in which centrally administered computing capabilities are delivered as services, on a need basis, across the network to a variety of user-interfacing devices” [5]. Cloud computing has added a new dimension to IT in terms of provisioning of various kinds of services to the client. Cloud computing is presently utilizing vast amount of storage and computing power available to cloud service providers to make computing easier to consumers. Cloud computing can be seen as a model that allows access to various services by users on demand anywhere in the world [6].

The services being provided by the major players like Amazon, Google and Microsoft include software as a service (SaaS), platform as a service (PaaS) and infrastructure as service (IaaS). The PaaS process allows users to develop and deploy their applications without having to bother about the processor or storage utilized [6] Google App Engine is an example of PaaS that provides users with the ability to deploy applications using Python or Java programming language.

Cloud computing can also provide great leverage for human resource management system. This is because of large volumes of data that need to be stored and accessed with ease. The cloud platform allows the resource manager to focus on the application, while the cloud service providers offer the required facilities. There are lots of discussions relating to security in computing and in terms of cloud activities. Obviously, both computing assets and data require security. In as much as the cloud offers several opportunities, there are concerns that another user may access a customer’s data on the cloud platform [7]. However, one unique way to alleviate security challenges in the cloud is for organizations to ensure that roles and privileges are assigned to those utilizing an application. [8]. There is no doubt that the number of attacks on the cloud has increased, but so also are the measures being designed to mitigate the situation [9]. The presented level of security in cloud computing is supposedly sufficient, hence proving the needed confidence to use the cloud. Nonetheless, our application was deployed on the Google Cloud Platform with an additional measure of encrypting the data in storage. Therefore, this paper was motivated by the need to provide an extra level of security. This paper examines various HRMS model and proposes a model, which was implemented and deployed on the Google Platform. The organization of the paper is as follows: section 2 discusses related work in HRMS. The proposed model and its implementation are discussed in section 3. The results and conclusion are presented in Section 4 and Section 5 respectively.

2. Related Work

The HRM Framework Model in [10] describes HRM related processes throughout an organization. HRM roles, systems, resources except security are all considered in the model. While MIS and healthcare management in [11] [12] examine HRM system in relation to healthcare. The focus is on utilizing information in a process-oriented manner for healthcare delivery. The Matching Model in [13] considers the human resource as important in terms of production. It aims to develop strategies that seek to provide increased productivity in a competitive environment, while the Contextual Model in [14, 15] considers the relationship between various factors in conjunction technology is expected to improve productivity. The Integrative Model of HRM in [15]

defines HRM in differing dimensions taking into consideration the human resource vis-a-vis organizational strategies and processes and the Harvard Model in [13] [16-19] is associated with the human relations, individuals' talents and human willingness to create and work. The Michigan Model in [20-21] expects that people should be managed like any other resources and so obtained cheaply, used sparingly, developed and exploited fully. The Choice Model in [17] [22] [23] [24] [25] discusses the drivers for formulating HRM policies and frameworks namely: the organization, personnel and external. It provides a more comprehensive approach to HRM. From the existing survey, adequate and extensive discussion were carried out as it affects HRIS. However, sufficient attention was not given to security, almost no consideration was given to utilizing the cloud for HRIS.

A survey of security issues for cloud computing in [9] took a detailed look at various threats to cloud computing security and conducted a comprehensive analysis. Furthermore, several aspects of cloud security were discussed and some solutions proffered. The study in [7] addressed customer security in cloud computing focusing on data confidentiality, integrity and availability. It affirms that the level of cloud usage will be directly proportional to the level of cloud security.

A survey on cloud computing security: issues, threats and solution in [8] conducted an overview of cloud security concerns such as sharing and virtualization of resources. Thereafter, solutions were proffered with a view to enhancing security on the cloud.

Cloud computing: A solution to HRM System in [26] proposed the service of a cloud HR Management. The cloud HR manager has several modules for enhancing HR activities. For example, selecting the Benefit Module enables the management access to the entire employee benefit program. Through the Benefits module other plans such as health savings, child education and payroll schedule can be accessed.

The study in [27] proposes architecture for cloud based HRM for higher education. The proposed system is broken down into three sections for the client, application and the platform. Each section aims to enhance the way HRMS is utilized in a higher institution.

Cloud computing in HRM enterprises HRM system in [28] proposed to adopt cloud computing technology in SME, for HRM. The proposed model takes advantage of the services available on the cloud to provide a custom built HRMS. The proposed system allows adequate interaction between small business owners and the cloud service providers.

All the papers examined did very comprehensive and useful work in the area of HRMS. However, little attention was given to the issue of securing the HRMS. In addition, while some work utilized cloud computing, others did not. Furthermore, the ones that utilized cloud computing did not focus on the need to encrypt data in storage. Based on this, in the next section we proposed an HRMS model with focus on security and also leveraging on the benefits of cloud computing.

3. Proposal and Implementation

In developing a cloud-based security-driven HRM System, several HRMS models were investigated. A model was proposed and based on that model; the proposed HRMS was implemented, using the Role-Based Security Model as a guide. The exact descriptions of the features that make up the security model applied in the proposed Human Resource Model are discussed further. All access to the system is role/permission based.

This means that the operations of users on the system are done and executed based on the permissions assigned to their roles. To cater for one of the main problems with the role-based access model, specifically; the lack of the ability to specify a fine-grained control on individual users in certain roles and on individual object instances, which makes it unsuitable for collaborative environments, another layer of security was developed and implemented. The Operation Security Tagging feature further defines security levels for every task that can be executed on the Nigerian Air Force (NAF) HRM System. The following explains the security levels employed and the criteria an operation has to meet in order to be classified under any security level:

Table 1. The Secure HRM Virtual Grid

	1	2	3	4	5	6	7
1	a/A	b/B	c/C	d/D	e/E	f/F	g/G
2	h/H	i/I	j/J	k/K	l/L	m/M	n/N
3	o/O	p/P	q/Q	r/R	s/S	t/T	u/U
4	v/V	w/W	x/X	y/Y	z/Z	0	1
5	2	3	4	5	6	7	8
6	9						

The NAF Encryption algorithm, which is based on the Simple Substitution Ciphers, is an enhancement of ROT-13, which makes use of Table 1. The virtual grid is made up of seven (7) columns and six (6) rows. The rows and columns are designed to have either alphabets or numbers. In this instance row number 6 has only a number, which is the last digit of the numbers 0-9. Each character is represented by its column number (c) and its row number (r) such that (cr) represents a character. It should be noted that the encryption algorithm is not case sensitive. The grid can also be used to encrypt special characters. There is no maximum depth for encryption of data since the algorithm recognizes numerical data and is able to also encrypt them. This means that one can perform several encryption cycles on any input. In other words, one can continue to encrypt data that has been encrypted in a recursive manner. It will take the exact number of encryption cycles to decrypt the encrypted data.

The proposed OOS-4 Model is depicted in Figure 1. This model to a great extent explains the importance of using all five HRM activities of planning for the recruitment of employees, training of employees, performance evaluation, keeping track of employee activities such as postings, promotions, and finally manpower development in achieving the organization’s strategic needs. Furthermore, the proposed model shows the interrelatedness of these activities. Synthesizing from the various HRIS models examined, the OOS-4 model is proposed. The OOS-4 model provides global and local security architecture for a HRIS that can be applied in a military environment. A multi-level protection is applied to secure sensitive nature on information in a military environment. In line with the concept of executive information system model, OOS-4 is designed to provide management and departmental level security. Permission is also required to generate and post summaries.

The OOS-4 model does not represent any specific security model currently in use. Like the NATO HR Framework, it is also meant to create an organization containing the right people at the right place and at the right time. More importantly, the OOS-4 framework is expected to do this in a secure environment. The operational HRM process of recruiting, training, deployment and retirement is expected to be carried out in a confidential environment that is not subject to external influences due to leakage of information. Also, the strategic level HRM that provides the future direction of the

organization will also be subjected to checks. Analysis of existing strategies viz-a-viz strategic goals should not be exposed, so as not to jeopardize future plans.

OOS-4 models also focuses on how integrated administrative, personnel and management systems in the military can be adequately deployed to support operational processes within and outside the country. For example, making information on the personnel needed for UN Observation Mission available to all could lead to severe lobbying by the personnel. As discussed earlier, HRM models assist in investigating and understanding workforce governance, work organization, staffing and reward system. HRM basically supports the management of employee relationship influenced by various factors. In a military environment, these factors can affect the confidential nature of the system. The generic functions of HRM such as selection, appraisal, rewards and development are usually subjected to external influences.

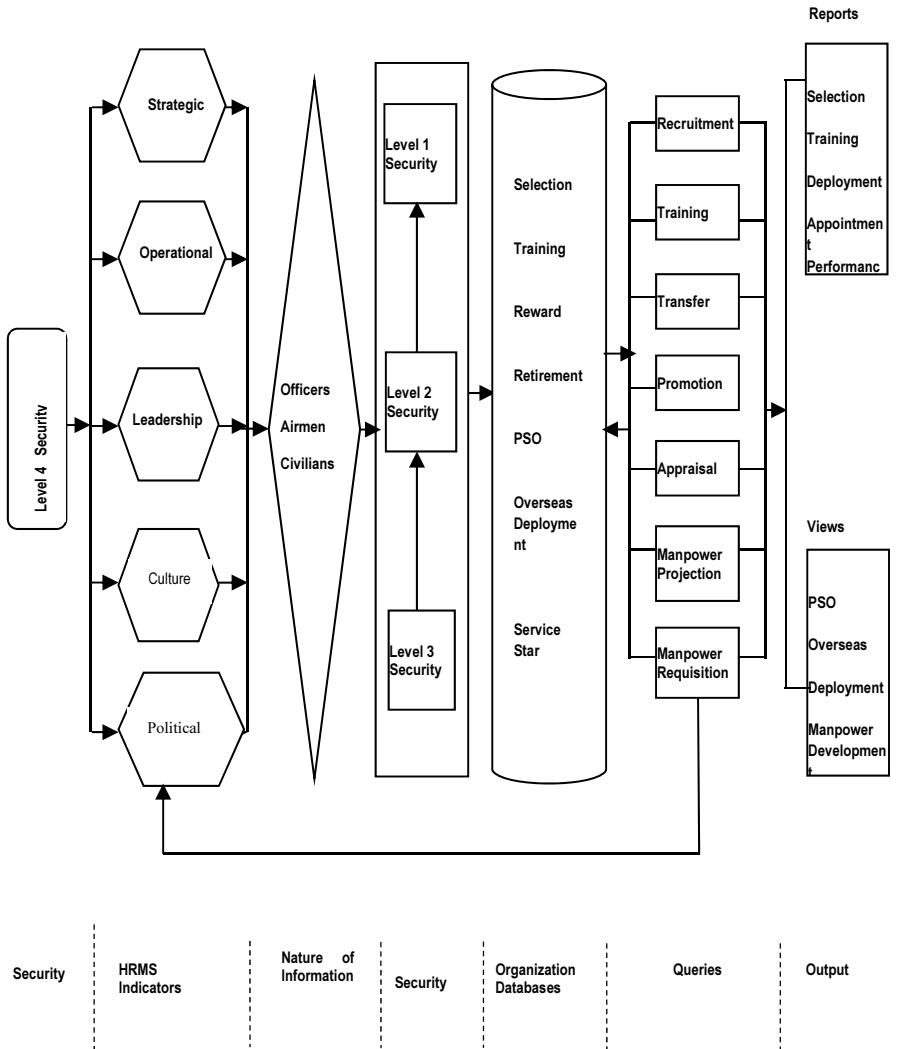


Figure 1. The Proposed OOS-4 HRIS Framework.

The OOS-4 model also seeks to protect these various stages and also changes in HRM, based on strategy changes. As espoused in the contextual model, there are external and internal environments that affect the HRM generic functions. Such external issues like socio-economic and political factors also affect HRM military system. However, we have added religion and ethnicity based on the peculiar nature of our environment. In addition, the internal factors like culture and leadership affect the HRM functions. The OOS-4 framework seeks to also provide security at the global level to drive successful conduct of personnel management. The more secured the process, the less likely that the system will be negatively influenced. These sets of external and internal influence will affect the integrated set of practices, policies and strategies, which the military use to manage their human capital. It is not surprising therefore that the OOS-4 model bears similarly to the Martin-Alcazar framework [15]. The military operates on a high level of the need-to-know principle; hence the various levels of security classifications are applied. This is to mitigate the organizational, social and individual effects of any lapse in the HRM security framework.

Human resource flow into an organization is meant for recruitment, selection, placement, promotion, rewards and termination. Some of these processes of HRM are visible to all personnel. For example, the performance evaluation reports needed for promotion is made available to the staff in most establishments. However, the reward system in a HRM must be secured. All persons can deliberately behave in line with the set criteria if they are known. The effect may be to reward indolence. This is however contrary to the reward system meant to enhance high employee commitment that leads to better job performance. As mentioned earlier, it is surprising that all HRM framework examined focused of HRM strategies like differentiation, innovation, quality, cost reduction expected to lead to better training, appraisal, selections, rewards and job design, without any consideration for security. Therefore, the proposed OOS-4 framework is a holistic and integrated model that is meant to consider various levels of security in the internal and external environment of HRM. It allows for better planning and forecasting, and it integrates the interrelatedness of the various component of a HRM organization suitable for military purposes.

An Application Programming Interface (API) is a set of programs that encapsulate commonly used and required functionality in an application. The API used in building the Secure HRM System is the Java Enterprise Edition Application Programming Interface (JEE API). The JEE API exposes a host of utilities used in building the Secure HRM application. The JEE APIs are a layer above the core Java Standard Edition APIs. The JEE API layer allows applications importing them to interface with web servers and database servers. At the heart of the JEE API is a set of programs that allow for the creation of servlets, which serve as request handlers and response generators. Given the fact that Plain Old Java Objects (POJOs) are used at the core of the Secure HRM System, the core JEE APIs is also employed.

The NAF HRM system is a three-tier web based JEE cloud application. The primary means of accessing the system is through a web browser. A Model-View-Controller (MVC) design pattern was employed in the implementation of the NAF HRM system. The system is broadly broken into the following major parts, namely:

- Application Frontend (View).
- Application Business Logic (Controller).
- Application Backend (Model).

Table 2. Software and Hardware Requirements

Platform	Java Enterprise Edition (JEE)
Application Server.	Google App Engine (GAE).
Database.	Bigtable (Google App Engine implementation).
Object Persistence Technology.	Java Database Objects (JDO).
Data Inter-change Technology.	JavaScript Standard Object Notation (JSON).
Library GUI CSS.	Google GSON Bootstrap.
Operating System.	Windows/Linux.
Server Hardware Requirements	
RAM.	2 GB+.
Processor speed.	2.0 GHz+.
Hard Disk.	250 GB+.
Client Hardware Requirements	
RAM.	1 GB+.
Processor speed.	1.2 GHz+.
Hard Disk.	50 GB+.
Browser.	Mozilla Firefox, Google Chrome.

The application frontend is made up of components and technologies that are related to displaying, presenting and collecting data to/from the end user. Table 2 describes the technologies used in implementing the frontend as discussed below:

- HTML 5: The latest version of HTML is used in building the web pages that make up the NAF HRM. This has played a very important role in ensuring that the graphical user interface (GUI) is clean and simple.
- JavaScript: JavaScript is used to implement form validations and extra intelligence required on web pages that need to be executed in the client's browser.
- Cascading Style Sheet (CSS): A CSS library called bootstrap (developed by twitter) was used in styling the web pages. Form components and other web pages widgets were all styled using bootstrap CSS. This gives NAF HRM its unique look and feel.
- JSP: For added functionality and intelligence Java Server Pages were used as the main container for HTML, JavaScript and CSS code. Server side code can be easily executed and managed in JSPs hence the heavy reliance on JSPs for all the web pages in the NAF HRM system.
- The Business Logic tier of the NAF HRM sits in-between the view and the model parts of the NAF HRM. It is at this tier that all business rules of the NAF HRM are implemented and enforced. It is written in pure Java and is made up of a servlet and a couple of Plain Old Java Objects (POJOs). This tier is further broken into two packages as follows:
 - * Managers: This package contains two classes namely: UserManager.java and RoleManager.java. These classes carryout functions on the data stored in the application.
 - * Controller: This package contains one class called Prime.java. All requests and responses pass through this class. This class delegates tasks to the appropriate classes for execution and delivers results and responses to the view (web pages).

An Object Oriented Database Management System was used in implementing the backend of the NAF HRM system. This was done due to the following reasons:

- a) Scalability across a distributed architecture: Given the fact that the NAF HRM is cloud based, it means that once the application is deployed in the cloud, it may run in any of the distributed servers that make up the cloud network. Hence, only an Object Based Database Management System can handle multiple distributed requests and still maintain consistency and data integrity. A relational database management system would not function well in a distributed environment.
- b) Large Data Management: Object Based Database Management Systems are known to handle large volumes of data efficiently.
- c) Speed: Read and Write speeds of Objected Based Database Management Systems is in a way faster than a relational database system because the object based database is more often than not executed in an object oriented environment. Java Database Objects (JDO) is used to persist objects in the data store. JDO provides object manipulation interfaces that make it easy to create, manipulate and store Plain Old Java Objects (POJOs).

4. Results

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. Most public HRM Systems apply little or no data encryption at all. On the other hand, the HRMS (securehrm1) we created is deployed on a public domain with encrypted data, and Figure 2 is a view of how the data is stored. The Google Platform allows application to be written in any program language and deployed using either the Java or Python runtime environment. The application can be accessed on the user's domain name or a free name on the console.cloud.google.com domain [5]. Figures 2 and 3 show the Google Cloud Platform Dashboard and how the data appears in the data store respectively. This application was developed and deployed under the PaaS cloud type using the the Google AppEngine as shown in the Compute part Google Cloud Platform

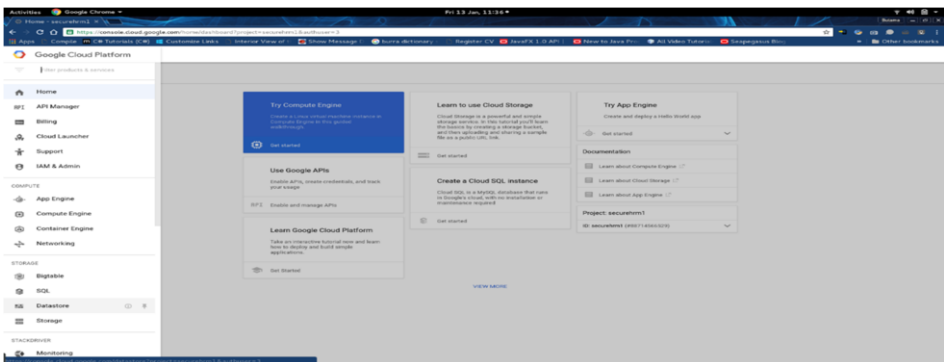


Figure 2. Google Cloud Platform Dashboard.

Name/ID	deptid	designationid	email	empdate	endscore	example	Non
name=16149161615	02	05	11441321148716211225269311382	1 October 2000	0	0	621
name=16149161655	02	05	31132514872221116169311382697271	7 June 2004	0	0	317
name=16149161644	02	05	1142114415415148716211225269311382	11 January 2001	0	0	1152
name=16149161665	02	02	11534148716211225269311382	1 January 2000	0	0	1342
name=16149161674	01	05	1153414872221116169311382697271	1 January 2002	0	0	631
name=1614916415	02	05	5253117241148716211225269311382	1 August 2001	0	0	922
name=1614916416	01	05	1352734872116169311382697271	1 May 2002	0	0	114
name=16149164435	01	05	621487216169311382697271	1 July 2007	0	0	622
name=16149167365	01	05	5341611148716211225269311382	1 April 2002	0	0	217
name=1614925354535	02	01	2173525369716169311382148716211225269311382	1 January 2000	0	0	621
name=152535152535	01	01	11534148716211225269311382	1 January 2000	0	0	11
name=5316164	01	01	11534148716211225269311382	1 January 2001	0	0	231
name=7211616947452535	02	04	223222637348716211225269311382	13 October 2006	0	0	222
name=721161673955	01	03	11531148716211225269311382	10 July 2007	0	0	621

Figure 3. HRM Data Store Screen in the Google Cloud Platform.

Dashboard. The primary purpose is to display the encrypted information in storage as displayed in the Datastore of the Google Platform. The details of what is in the datastore is displayed in Figure 3. The email addresses, name, gender and other items in storage are displayed as series of figures with the file name securehrm1.

As suggested in literature it is essential to assign roles and privileges to users of an application on the cloud. There is a unique level of authorization employed in this application that ascribes suitable roles and privileges to the various categories of users. These records appear in form of numbers when viewed from the database but appear as plain text when viewed 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. Furthermore, the HRMS was created and hosted on the Google App Engine.

Another aspect of the secure HRMS is that the encryption of data can be done at several levels. This simply means that the result of an encryption can be the input data for another level of encryption using the same encryption algorithm. This presents a situation whereby data stored can be encrypted at several levels hence making it even harder to crack. Different columns of data can have different levels of encryption and this can be done in a varying pattern.

The virtual grid which serves as the core of the encryption and decryption algorithm can also be reordered for several deployments of Secure HRMS. The virtual grid shown in Table 1 can have the columns and rows rearranged in memory and used to encrypt and decrypt data in a random manner. This gives another layer of security since one may not know or be able to guess the underlying virtual grid used to encrypt the specific set of data.

Combining the ability to have numerous levels of encryption and alternating the virtual grid used to encrypt and decrypt the data in the Secure HRMS makes it virtually impossible for an attacker to steal and make sense of the encrypted data. This offers a compelling reason for organizations of any type to rely on Secure HRMS for storing and protecting their data. Organizations can also, as part of their security policy rotate their underlying virtual grid after a given period of time.

5. Conclusion and Future Work

HRIS provides an avenue for computerized information about an organization's personnel with a view to enhancing productivity. Employee information spans the period of recruitment to retirement and it involves various departments and aspects such as health and benefits. Clearly, the human resource of an organization is the most valuable asset and efficient management of their information is vital to the success of that organization. It is important to secure employee information in the application of HRMS. Also, large volumes of data is usually generated, hence the need to take advantage of the provisions of cloud computing.

Fortunately, the coming of cloud computing has enhanced the way data can be stored and managed. The huge cloud infrastructure is already enhancing the effective utilization of HRMS. We established a robust, multi-level, scalable security HRM System using a cloud platform. We examined several existing HRIS models and to this end: The OOS-4 model framework was created and an adapted ROT-13 encryption algorithm established. A secure, cloud-based HRIS was created and deployed on the Google App Engine. The HRMS we created has shown and proven that HR systems can be built and deployed in cloud environments, with the benefit of scalability. The HRM organization utilizing this application does not have to bother about the platform required to deploy the application because it is running on the cloud. Furthermore, additional security measures were provided in addition to the security available on the cloud. Clearly, cloud computing is highly beneficial to the development and deployment of the client's application as seen from the result. Further research can be carried out on how to link the HRMS with an automated filing system.

Acknowledgements

We acknowledge the support and sponsorship provided by Covenant University through the Centre for Research, Innovation and Discovery (CUCRID).

References

- [1] G. Dessler, *Human Resource Management*, Pearson Education, 2004.
- [2] W. Simon, *The Associative Model of Data*, Lazy Software Ltd, Great Britain, 2001.
- [3] W.J. Alfred, *Human Resource Information System Development*, Wiley, John & Sons, 1982.
- [4] S.W. Ambler, *Justifying a Software development Project*, Ambysoft, 30 (2006), 3-6.
- [5] J.S.C. Brian, and F. Curtis Jr., *Cloud Computing Technologies and Strategies of The Ubiquitous Data Center*, Taylor & Francis, 2010.
- [6] R. Buyya, J. Broberg, A. Goscinski, *Cloud Computing Principles and Paradigms*, Wiley, 2011.
- [7] A.C. Carlos, B. Westphall, C.M. Westphall, and G.A. Gerônimo, *Customer Security Concerns in Cloud Computing*, IARIA, 2011.
- [8] S. Saurabh, J. Young-Sik, H.P. Jong, *A Survey on Cloud Computing Security: Issues, Threats and Solution*, *Journal of Network and Computer Applications*, 2016.
- [9] M.A. Khan, *A Survey of Security Issues for Cloud Computing*, *Journal of Network and Computer Applications*, 2016.
- [10] O. Karasakal, *Human Resources Management Framework Model*, *NATO RT Journal*, 79 (2008), 50-60.
- [11] W.W. Stead, N.M. Lorenzi, *Healthcare Informatics: Linking Investment to Value*, *J Am Med Inform Assoc*, 5 (1999), 341-348.
- [12] D.L. Flarey, *Redesigning Nursing Care Delivery*, J.B. Lippincott Company, Philadelphia, 1995.
- [13] M. Armstrong, *A Handbook of HRM*, Cambridge University Press, 2006.
- [14] M.H. Tayeb, *International HRM: A Multinational Company Perspective*, Oxford University Press, 2005.
- [15] F. Martín-Alcázar, P.M. Romero-Fernandez, and G. Sanchez-Gardey, *Strategic HRM: Integrating the Universalistic, Contingent, Configurational and Contextual Perspectives*, *International Journal of Human Resource Management*, 16 (2005) 633-659.
- [16] L. Gratton, V.H. Hailey, P. Stiles, and C. Truss, *Strategic HRM*, Oxford University Press, 2003.
- [17] C. Hendry and A. Pettigrew, *HRM: an Agenda for the 1990s*, *International Journal of HRM*, 1 (1990), 17-43.
- [18] K. Legge, *HRM: Rhetorics and Realities*, Macmillan Business, Basingstoke, 1995.
- [19] M. Armstrong, *HRM: A Case of The Emperor's New Clothes*, *Personnel Management*, 19 (1987), 30-35.
- [20] C.J. Fombrun, M.M. Tichy, and M.A. Devanna, *Strategic HRM*, John Wiley, New York, 1984.
- [21] M. Cusworth, and T. Franks, *Managing Projects in Developing Countries*, Longman, New York, 1993.
- [22] F. Analoui, *The Changing Patterns of HRM*, Ashgate, UK, 2002.
- [23] F. Analoui, *Strategic HRM: Towards Constructing a Choice Model*. Conference on Human Development Practices and Practitioners: Beyond the Year, Development and Project Planning Centre, University of Bradford, 1999.
- [24] J.P. McDuffie, *Human Resource Bundles and Manufacturing Performance*, *Industrial and Labour Relations Review*, 48 (1995), 197-221
- [25] M. Hiley, *The Strategic Role of Human Resources in Corporate Strategies*, Ashgate, Aldershot, UK, 1999.
- [26] A. Datta, R. Islam, A.K. Mukherjee and D. Kandar, *Cloud Computing: A Solution to HRM System*, 2012 International Conference on Radar, Communication and Computing (ICRCC) SKP Engineering College, Tiruvannamalai. TN., India, (2012), 176-179.
- [27] Q. Chen and J. Ni, *Systems Architecture Design of Cloud-based Human Resources Information Management (CHRIMS) for Higher Education Institutions*, in *Seventh International Conference on Internet Computing for Engineering and Service*, 2013.
- [28] X.L. Wang, L. Wang, Z. Bi, Y.Y. Li, Y. Xu, *Cloud computing in HRM (HRM) System for Small and Medium Enterprises (SMSs)*, *International Journal on Advanced Manufacturing Technology*, 84 (2016), 485-496.