International Journal of Information Security, Privacy and Digital Forensics
Vol. 4, No. 1 June 2020

A Cloud-Based Access Regulatory Model for the People Living with HIV in South Africa

Nureni Ayofe Azeez[1]
School of Computer Science and Information Systems
North-West University
Vaal Triangle Campus
South Africa
nazeez@unilag.edu.ng,

Charles Van der Vyver[2]
School of Computer Science and Information Systems
North-West University
Vaal Triangle Campus
South Africa
Charles.VanDerVyver@nwu.ac.za

Wasiu Adewale Yekinni
School of Tech.,
Computer Science Department
Lagos State Polytechnic
Ikorodu, Lagos
dewaleyk@gmail.com

Abstract: Information about the rampant nature of Human Immunodeficiency Virus (HIV) in Africa, particularly South Africa is no more a news. There is a global awareness on this. In spite of the ubiquitous nature of this ailment, patients feel highly uncomfortable with the way and manner their sensitive and classified health information are being accessed and shared by different healthcare practitioners. HIV patients opined that information about them are vulnerable that people are using it against them. Although, the traditional security mechanisms have been adopted over the years to protect health data and patient information, researches have however shown that some of these approaches are suffering from several challenges such as platform dependency, isolation, cumbersomeness as well as inflexibility. Against these backdrops, this research aims at building a cloud-based access control model for sharing information across nine (9) provinces (The Eastern Cape, The Free State, Gauteng, KwaZulu-Natal, Limpopo, Mpumalanga, The Northern Cape, North West) in the Republic of South Africa among medical experts to ensure safety, security, reliability, dependability as well as flexile information sharing framework. This work is based on the adoption and usage of Role Based Access Control (RBAC) model, Access Control List (ACL) model and Motive Based Access Control (MBAC) model in a cloud-based environment. The implementation of the proposed framework will undoubtedly provide a unique and novel approach for achieving its primary aim and objectives.

Keywords: *E-Health, Security, Cloud Computing, Role Based Access Control, South Africa, HIV.*

1.0 INTRODUCTION

The prevalence of Human Immunodeficiency Virus (HIV) in South Africa is alarming [2]. As of 21st of November 2007, the United Nation report had it that over three-quarters of HIV-AIDS associated death occurred mainly in South Africa and sub-Saharan Africa. In the same vain, the statistics provided by UNAIDS in 2016 shows that South Africa has the highest HIV epidemic across the globe with at least 7 million people living with the disease. Also, in the same period, there were over 380,000 infections and an estimated 180,000 South African citizens died of this chronic disease [17].

Consequently, patients battling with these diseases have no choice than to see medical solutions in any standard medical hospital across the country. After wide consultations with available medical experts in South Africa, it is however noted that majority of health institutions except few Teaching Hospitals, nearly all health institutions are still using traditional approach of keeping

medical information. The information of HIV patients are not excluded as well [15]. Some are also using paper-based and Electronic Health Record (EHR) while those that have fully migrated to EHR are facing several challenges.

Some HIV patients' information are vulnerable through this approach because there is no guarantee for the safety of their medical information. The main effect of this insecurity is stigmatization of patients living with HIV-AIDS. It is very clear that the advancement in Information and Communication Technology has turned around the modus operandi in Health care sector [10]. There is a complete paradigm shift from the old paper-based medical method of preserving information to Electronic Health Record (EHR) Systems [7]. The introduction of EHR has undoubtedly circumvented the problems of platform dependency, isolation, cumber-someness as well as inflexibility [1] that are commonly associated with traditional approach of keeping medical information.

It is of no doubt that EHR comes with many advantages. It offers to reduce medical errors, it provides immediate and up-to-date information about patient to all service providers. Also, EHR assists to reduce medical errors particularly during drug prescription [15]. The benefit of adopting EHR is more realizable and attained to the fullest [15] if it is deployed in a distributed environment, specifically, in a cloud-based environment. It offers seamless and limitless sharing of information about patients across various medical domains, medical research institutes and allied organizations [8].

Despite various benefits that are being maximized from Electronic Health Record, it has been established through researches that security and privacy of patients are at risk [9]. The information about patients are now vulnerable because the privacy of information could not be guaranteed [4]. Though, many researchers have proffered solutions, but there are lapses in the existing approaches to guarantee adequate security measures for EHR.

Against this backdrop, this research attempts and proposes the implementation of e-Health Access Control Model in a Collaborative Environment for HIV Patients' Information in South Africa. It is determined to achieve the following objectives:

1. real time application that will guarantee collaborative sharing of patients' information across states of the federation among designated medical personnel.
2. exclusive right for the users (patients) to determine who should access his medical profile
3. a Central Database (CD) where the population of people living with HIV-AIDS could be easily obtained and verified.
4. a framework that will assist the South African Government to plan for the medical and strategic needs of people living with HIV-AIDS

2.0 METHODOLOGY

The proposed model will be implemented by using Role Based Access Control model (RBAC), Access Control List (ACL) and Motive-Based Access Control (MBAC) in a Cloud Based Environment. These will be supported by a novel algorithm that will define working scenarios of the entire process.

2.1 Role Based Access Control (RBAC) Model

The RBAC model is defined in terms of four model components – Core RBAC, Hierarchical RBAC, Static Separation of Duty Relations, and Dynamic Separation of Duty Relations. In this work, Hierarchical RBAC [26] will be used where Role hierarchies will define an inheritance relation among roles (see Figure 1).

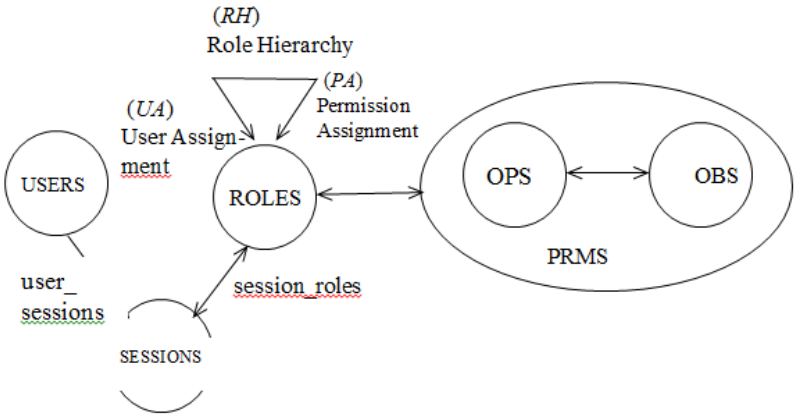

Figure 1: Role Based Access Control model (RBAC) [26]

2.2 Access Control List

An access control list (ACL) contains a list of Access Control Entries (ACE) where the latter identifies a trustee and specifies the access privileges and rights allowed, audited or denied for that trustee [4]. ACL invariably consists a list of specific permissions attached to an object. Each entry in ACL specifies a subject as well as its corresponding operation.

2.3 Motive-Based Access Control (MBAC)

Motive-Based Access Control (MBAC) has to do with the relationship between data objects and motives for seeking them. The motives usually dictate the purpose for collecting data and what they are meant for. The novel model is very flexible and useful a lot. Since health information is very important and that its privacy should be taken with utmost importance, MBAC assists to capture the main objectives and reasons for collecting data. It also explicitly defines the intentions of users of that data.

2.4 Access Control Model under Consideration

There are four main phases in the proposed access control model for HIV patients E-Health solution. The phases are: Motive Based Access Control (MBAC), Mandatory Access Control (MAC), Role Based Access Control (RBAC) and Discretionary Access Control (DAC). The standard operational protocol for the access control model is depicted in Figure 2. The assumption is such that each HIV patient in all the provinces in South Africa has a detailed and all-inclusive E-Health information which is being managed by a competent and relevant designated health authority.

The decision of a patient has to be respected and taken into consideration [22]. In the newly proposed model therefore, the HIV patient who might be from any of the provinces in South Africa will have privilege through the assistance of a designated health authority, after authorization and authentication, to access healthcare delivery system within a secured and reliable platform in a cloud-based environment. The detail shall be explained in the subsequent sections of the paper.

Interpretation and a comprehensive definition of motives is undoubtedly a complex mission that demands special attention and care. The process requires the exploration of medical-based knowledge for medical experts who can classify the benefit of various data elements in the healthcare delivery. Motive definition is a phase on its own because motives will define and govern access privilege to data in the newly proposed access model.

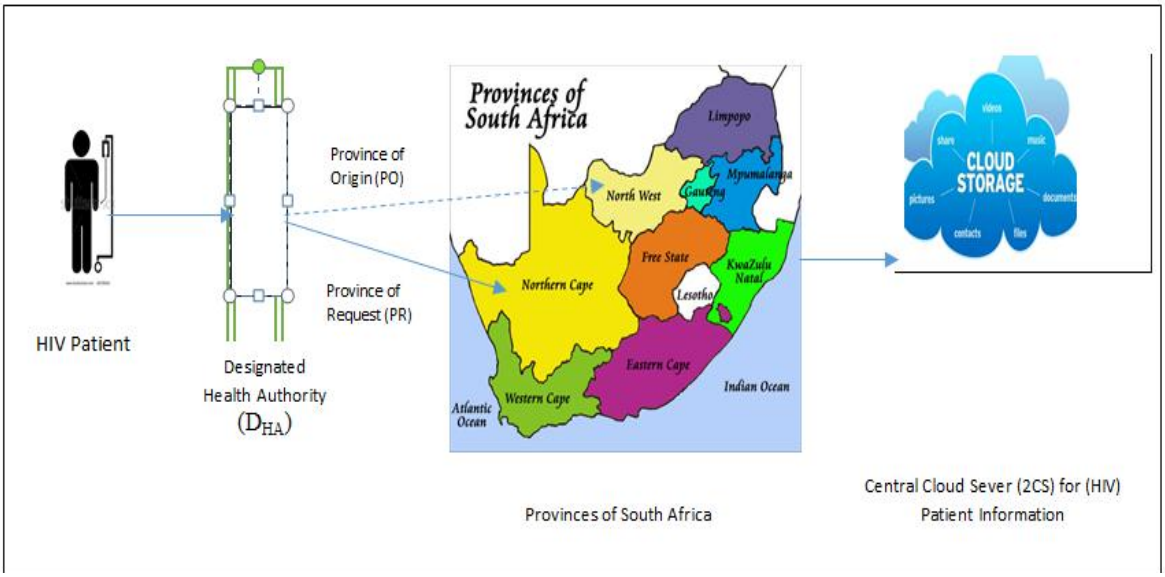

Figure 2: Patient's authorization to the Central (HIV) Patient Information Server (CPS)

The designated health authority will oversee the relationship between the data types and motives. A standard default setting will be provided for the motives for seeking any data type. The designated health authority will be in position to dictate, delete, add, remove and update motive related to data elements. This will guarantee and provide absolute assurance on the maintenance of up to date motives in the entire system. With this procedure, access privileges and requirements of healthcare providers will not be deprived of.

The health authority will manage the relationship between data types and purposes. There will be a default set of *purposes* for every data type and elements of that data type. The health authority can define, add and remove purposes related to data types and elements. This will ensure that up to date *purposes* are maintained in the systems such that the access requirements of care providers are not wrongfully denied.

Algorithm 1: Algorithm for general Authorization

Accept: Patient_ID, D_{HA} , Province: PO, PR, 2CS

$Begin$:
$Patient\_ID\_request \rightarrow Authourization\ (HA)$
$if\ Authourization\ (HA) \rightarrow True\ THEN$
$Verify \rightarrow Patient\_ID\ (Province)$
$If\ Province\_PO \rightarrow True\ AND\ )$
$If\ Province\_PR \rightarrow True\ AND\ THEN$
$Patient\_Access \rightarrow [2CS] = True$
$If\ Province\_PO \rightarrow False\ AND\ )$
$If\ Province\_PR \rightarrow False\ AND\ THEN$
$Patient\_Access \rightarrow [2CS] = False$
$Stop$

As shown in Figure 2, whenever an HIV patient intends to make use of medical facility within the country, he first gets authorised with his valid Identification Number (ID) through a Designated Health Authority (DHA). Doing this will qualify allow him/her to proceed and confirm his Province of Origin (PO) and have the capacity to specify his new Province of Request (PR). PO is the original province where the patients hails from and PR is where the patient wants to receive medical attention. The moment this phase is clarified and settled, further details regarding HIV patient will be attended to in the Central Cloud Server (2CS) where information and procedure about access privilege and patient's data reside. Further details on 2CS will be explained in the subsequent section of this paper. It is very essential to note that Data type, Data motive, ACL, a table that contains HIV Patient E-Health information, a table with access request by authorised HIV patients are all contained in the 2CS.

Table 1: Data type and Motive indicator

Data type	Determined Motive(s)
HIV1 (Stage 1)	M1, M3
HIV2 (Stage 2)	M4, M5, M6
HIV3 (Stage 3)	M3, M2
HIV4 (Stage 4)	M3, M4, M1

M1-M6: Motive

Table 1 shows how data type and motive for getting information about HIV patient are being shared. HIV patient is considered to have four different stages. This is captured as HIV1 (Stage 1), HIV2 (Stage2), HIV3 (Stage 3) and HIV4 (Stage 4). Each of the stages has a peculiar treatment as well as motive for any healthcare personnel to request for information about it.

Table 2: Access Control List

Healthcare practitioner	Patient's privilege settings	Access privilege by the Health Authority
MO1	<{eHealth}, {∅}, {HIV (Stage 1)}	<{HIV (Stage 2), HIV (Stage 3)}, {NULL}>
MO2	<{eHealth}, { HIV (Stage 1), HIV (Stage 4)}	<{ HIV (Stage 2), HIV (Stage 3)}, {NULL}>
MO3	<{eHealth}, { HIV (Stage 2), HIV (Stage 3)}	<{ HIV (Stage 1), HIV (Stage 4)} , {NULL}>
MO4	<{eHealth}, { HIV (Stage 3), HIV (Stage 4)}	<{ HIV (Stage 2), HIV (Stage 3)}, {NULL}>

MO = Medical Officer

Table 2 provides a summary of patient's privilege settings, access privilege by the health authority with their corresponding healthcare practitioners. Medical Officer (MO) has a corresponding patient's privilege settings and its access privilege as specified by the health authority. The relationship between former and the latter have been described in other section of the paper. Access Control List was used because it identifies a trustee and specifies the access privileges and rights granted, audited or denied for that trustee.

Table 3 contains HIV patient's e-Health information with comprehensive data on each of the stages that are also retrievable by any authorised MO after the motives have been verified. Invariable, access to information on each of the HIV stages are made available after the motives for request have been certified and confirmed.

Table 3: HIV Patient E-Health Information

Data type	HIV1 (Stage 1)	HIV2 (Stage 2)	HIV3 (Stage 3)	HIV4 (Stage 4)
Data element involved	Inf1, Inf2, Inf3, Inf4, Inf5	Inf1, Inf2, Inf3, Inf4, Inf5	Inf1, Inf2, Inf3, Inf4, Inf5	Inf1, Inf2, Inf3, Inf4, Inf5
Motive for retrieving Medical Information				

Table 4: Access requests by authorised HIV patients

Health Officer	Sensitivity label	Data type for access	Access Motive (M)	Province of HIV Patient PO	PR
MO1	<{eHealth}, {NULL}>	HIV1 (Stage 1)	M1, M2	XX	YY
		HIV2 (Stage 2)	M3, M4	AA	BB
		HIV3 (Stage 3)	M5, M6	CC	DD
		HIV4 (Stage 4	M6	EE	FF
MO2	<{eHealth}, {HIV2 (Stage 2)}>	HIV4 (Stage 4	M3	GG	PP
MO3	<{eHealth}, {HIV3 (Stage 3)}>	HIV2 (Stage 2)	M2	TT	RR

3.0 SENSITIVITY LEVEL

Sensitivity Level (SL) could be defined over two tuples < P_eSL, DSL> where P_eSL is given as {p_esl_1, p_esl_2…….. p_esl_n} which is equal to a set of permitted sensitivity levels.

DSL = {dsl_1, dsl_2……dsl_n} is a set of denied sensitivity levels.
P_eSL = {p_esl_j}; where j = 1 to n and it is denoted as all successors of p_esl_j with p_esl_j inclusive.

Also, DSL which is referred to Denied Sensitivity Label = {dsl_i }; I = 1……..n is represented as all of the successors of dsl_i with dsl_i inclusive.

The SL defined by HIV patients is completely different from SL defined by the HA. DSL usually set by HA will be NULL because the HA is much more concerned with granting access privilege to the MO who are the health professionals.

Denial of access is usually determined by the patients. The PeSL set by the patients precedes the PeSL set by HA particularly where there is no conflict and controversy between patient's DSL and PeSL. However, the PeSL set by HA will always precede DSL set by the patient whenever there is a conflict.

Definition for these notions are hereby represented as follows:

- IF ($P_eSL_P \geq P_eSL_{HA}$ AND $DSL_P \cap P_eSL_{HA} = \emptyset$) THEN SL_{MO} = < {P_eSL_P, { DSL_P} >
- IF ($P_eSL_P \leq P_eSL_{HA}$ AND $DSL_P \cap P_eSL_{HA} = \emptyset$) THEN SL_{MO} = < {P_eSL_{HA}} ,{DSL_P} >

- IF ($P_eSL_P \geq P_eSL_{HA}$ AND $DSL_P \cap P_eSL_{HA} = \emptyset$) THEN $SL_{MO} = < \{P_eSL_P\}, \{DSL_P \cap P_eSL_{HA}\} >$

With the above stated conditions, SLs are easily updated and various users can access different types of data in the cloud.

3.1 Sensitivity Labelling

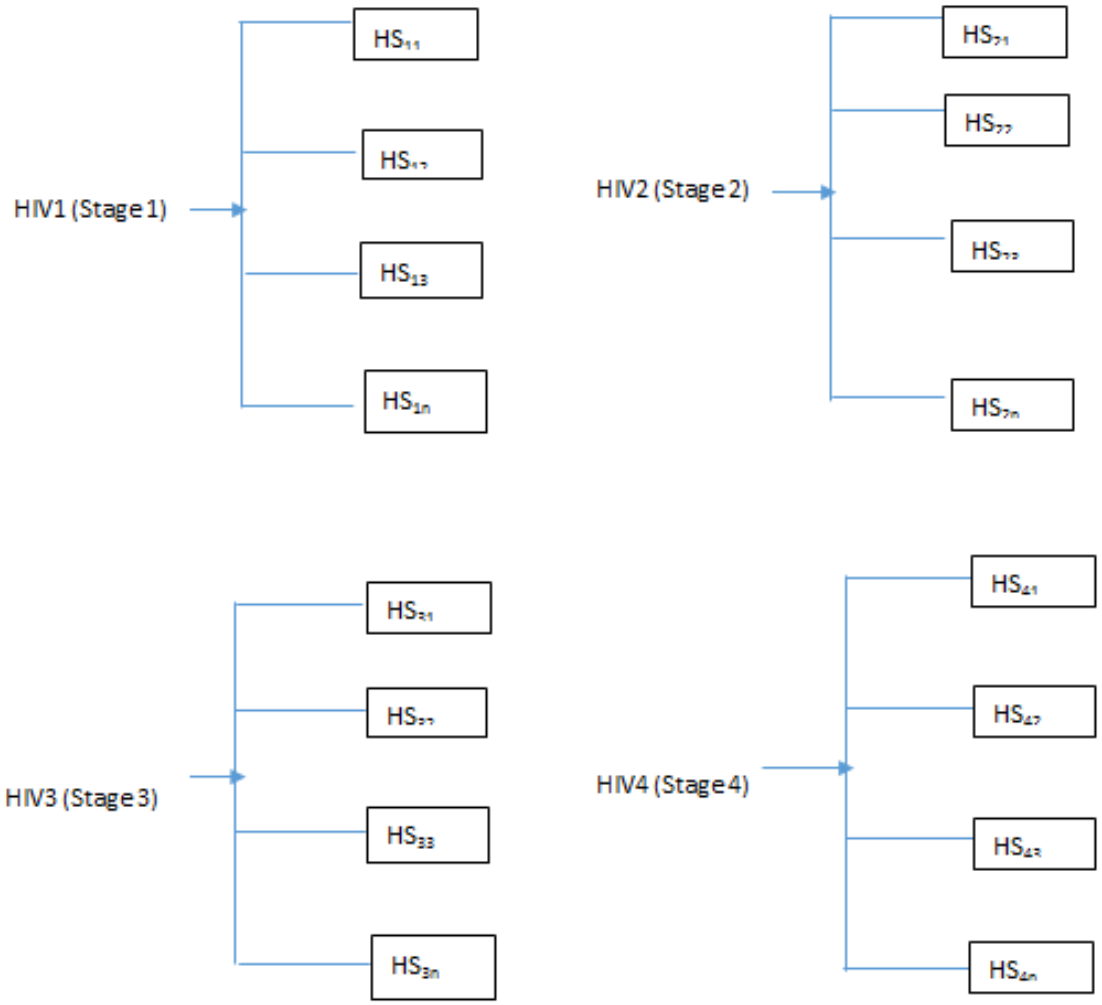

Figure 3: Sensitivity Labelling

Algorithm 2: Setting the Required Sensitivity Label

Input: Patient ID: P_ID
Begin:
$Patient_{SL-ID} \leftarrow < P_eSL_{patient-ID}, DSL_{patient-ID} >$
$HA_{SL-ID} \leftarrow < P_eSL_{HA-ID}, DSL_{HA-ID} >$
// HA = Health Authority //P_eSL = Permitted Sensitivity Level

IF
$P_eSL_{p-ID} \geq P_eSL_{HA-ID}$ *AND* $DSL_{P-ID} \cap P_eSL_{HA-ID} \neq \emptyset$) *THEN*
$SL_{-ID} \leftarrow <\{ P_eSL_{p-ID} ,\{ DSL_{P-ID} \}>$
Else if
$P_eSL_{p-ID} \leq P_eSL_{HA-ID}$ *AND* $DSL_{P-ID} \cap P_eSL_{HA-ID} \neq \emptyset$) *THEN*
$SL_{ID} \leftarrow <\{ P_eSL_{HA-ID}\},\{ DSL_{P-ID} \}>$
Else if
$P_eSL_{p-ID} \geq P_eSL_{HA-ID}$ *AND* $DSL_{P-ID} \cap P_eSL_{HA-ID} \neq \emptyset$) *THEN*
$SL_{-ID} \leftarrow \{ P_eSL_{p-ID} \},\{ DSL_{P-ID} \cap P_eSL_{HA-ID} \}>$
Else if
$P_eSL_{p-ID} \leq P_eSL_{HA-ID}$ *AND* $DSL_{P-ID} \cap P_eSL_{HA-ID} \neq \emptyset$) *THEN*
$SL_{-ID} \leftarrow \{ P_eSL_{HA-ID} \},\{ DSL_{P-ID} \cap P_eSL_{HA-ID} \}>$
End if

Algorithm 3: Access Request by HIV Patient

Accept: Patient_ID, SL_ID, Access Motives List: AccMotList, ACL (Access Control List), IntMotList

Begin:
$Dem\_Requests \leftarrow size\ (AccMotList)$
IF
$Access\ [no\_of\_requests] \leftarrow NO\ AND)$
IF
$Allow\_Data \leftarrow [no\_of\_requests] \leftarrow NO$
THEN
$Verify\_Motive\ [no\_of\_requests, no\_of\_mot\ ] \leftarrow NO$
FOR $For\ a = 1 -\ no\_of\_requests\ do$
$if\ IntMotivList(a)\ \in DSL\ (SL_{-ID})\ Then$
$Allow\_Data\ [a] \leftarrow NO$
Else
$Allow\_Data\ [a] \leftarrow YES$
End if
$for\ b = 1\ to\ size(AccMotList\ (a))\ do$
$if\ AccMotList\ [a,b]\ \subset IntMotList\ THEN$
$verify\_Motive\ [a,b] \leftarrow YES$
Else
$verify\_Motive\ [a,b] \leftarrow NO$
$if\ \{(Allow\_Data\ [a]\ = YES)\ AND$
$verify\_Motive\ [a,b]\ = YES\}\ THEN$
$Allow\_State\ [a] \leftarrow YES$
Else
$Allow\_State\ [a] \leftarrow NO$
End if

4.0 CASE SCENARIO

There is a Patient (P) and Medical Officers (MO1, MO2, MO3 and MO4) who are specialists in different areas of HIV treatments. In this case, a Patient (P) allows MO1 who is a specialist in the treatment of stage 1 of HIV to have a full access to his E-Health information. The access privilege here is absolute and exclusive. There is no restriction whatsoever in any form. He however does not give access to other stages of HIV, that is, Stages 2, 3 and 4. The access privileges to these stages are reserved for other Medical Officers.

The same Patient (P) allows MO2 to have exclusive access to Stage 2 of HIV. P however disallows MO2 to have access privilege similar to MO1.

Since MO3 is a specialist known for the treatment Stage 3 HIV, P reserves exclusive access provision for him. Finally, P allows MO4 to handle Stage 4 of HIV treatment. P does not want any interference in the sharing of HIV data without getting his consent.

In case there is need for data sharing among MO1, MO2, MO3 and MO4, Patient (P) will need to be consulted for any possible approval.

Consequently, MO2 can access P's HIV2-Stage 2 but cannot access his HIV1-Stage1, HIV3-Stages and HIV4-Stage 4 e-Health details. The access level for MO2 can therefore be denoted in terms of SL as follows:

SL_{MO2} = < {e-Health}, {HIV1-Stage1, HIV3-Stage3, HIV4-Stage 4} >

In this case, *denial* takes precedence over *permission*. Access privilege is given to the whole e-Health record but access is completely denied to some field by DSL-Denied Sensitivity Level. Doing this will assist to isolate very sensitive information in the e-Health record that deserves to be completely hidden from specific users within the same domain.

Also, the access privilege for another Medical Officer (MO), specifically MO4 could be given as follows:

SLM_{MO4} =< {e-Health}, {HIV1-Stage1, HIV2-Stage2, HIV3-Stage 3} >

This is because MO4 can only be given access to P's HIV1-Stage1, HIV2-Stage2 and HIV3-Stage3 at any Province a patient finds himself in South Africa.

5.0 MATHEMATICAL VERIFICATION OF THE PROPOSED MODEL

In order to further verify the efficiency of the proposed model, a Multi-level Logistic Regression model is considered and adapted.

$$Y = \beta_1 X_1 + \beta_2 X_2 + \beta_3 X_3 \ldots\ldots eqn\ 1$$

Where

Y = Access determinant
β = Vector of regression coefficient which comprises of β_1 , β_2 and β_3
X_1 = HIV Stage
X_2 = Medical Officer (MO)
X_3 = Motive (M)

Y which is access determinant is determined on the basis of either 0 or 1. If Y is 0, it implies that access is denied while access is permitted whenever Y is 1.

Y = Access Determinant, can further be defined under the following condition: Y<=3 (Access); this implies that "Access" Privilege will be given only when the number of trials is not more than three (3) times. However, when Y>3 (Denied); this implies that "Access" Privilege will be denied because of the value obtained for Y is greater than 3.

X_1 = HIV Stage can also be further defined as follows: the higher the complication of HIV status, the higher the assigned value.

The values for assignment are: 0.1, 0.2, 0.3 and 0.4. If HIV is at Stage 1, the value is 0.1. If, however, HIV is at Stages 2, 3 and 4, the values to be assigned are 0.2, 0.3 and 0.4 respectively.

For X_2 = Medical Officer (MO), the value assigned to it depends on the status of a Medical Doctor. If X_2 = General Medical Practitioner, the value is 0.2. If X_2 = Specialist, the value is 0.4 while 0.6 is assigned to a Consultant.

X_3 = Motive (M) can either high or low. It can equally be defined as either 1 or 0.
For a case study, if the following values are assumed for each of the variables as follows, then we can easily determine the nature of access to e-Health system.

Table 5: Assumed values for model verification

Y	X_1	X_2	X_3
0	1	2	3
1	1	1	2
0	2	1	5
1	3	2	1
.	.	.	.
.	.	.	.

From Table 5;
Since $Y = \beta_1 X_1 + \beta_2 X_2 + \beta_3 X_3$ then

$$0 = \beta_1 * 1 + \beta_2 * 2 + \beta_3 * 3$$
$$0 = \beta_1 * 1 + \beta_2 * 1 + \beta_3 * 2$$
$$0 = \beta_1 * 2 + \beta_2 * 1 + \beta_3 * 5$$

From the foregoing, values of β_1 , β_2 and β_3 can be evaluated. The most vital issue is the determination of Y which signifies whether access should be granted or not. The value of Y is significant to determine the status of access to the system.

6.0 RELATED WORK

This section presents review of several articles in journals, conference proceedings, documents from the internet, book chapters and books on various security approaches and mechanisms being used in e-Health. We did identified benefits and demerits of each of the approaches.

Shin et. al., 2014 examined various security models for healthcare applications and attempted to see how information leakage could be protected. They evaluated various security requirements to ensure security and privacy in electronic health. To find solution to identified security challenges in electronic health, they employed extended Role Based Access Control (RBAC) security model [13]. They came up with u-healthcare service integration platform where extended RBAC model was deployed. The architecture was designed to carry out four main functions: exchanging health information, meal recommendation, transaction of health information and management of health information on any smart devices [13]. It is however worthy of note that security issue was not properly resolved. The model is not suitable for a distributed environment. As a result, the solution provided has limited applications. The application does not also consider expansion in the number of users.

Simplicio et. al., 2015 present how a lightweight framework was used to present SecureHealth architecture that is based on Transport Layer Security/Secure Sockets Layer (TLS/SSL) for protecting data exchange with server that requires no extra security layer. SecureHealth which includes many security features like authorisation provides security services for transmitted and stored data. It has a good benefit of preventing alien from unauthorized access to the system that contains health information. Aside from this, it provides the manager the capability of identifying misnomer from information supplied [14]. Despite the

benefits accrued from this framework, the main challenge is that it is platform dependent and not scalable. In a cloud based environment, the security policy and framework must give room for scalability and future expansion.

In order to ensure that e-Health care service providers decrease the cost of maintaining data and allowing it to be available online in a secured manner, [6] proposed a security mechanism with different level of hierarchy. Provision of access control was carried out at a central level. They adopted Attribute Based Encryption (ABE) in such a way that privileges were mapped and juxtaposed into various roles with ABE access structures. The main challenge with this approach is the complexity of responding to various requests from different users due to storage of health information located in a centralized server [6]. Also, priority needs to be set when there is a simultaneous request by users.

In order to solve the challenge of having data storage of health information in a centralized server, Guo et. al., 2012 considered the distributed and collaborative nature of e-Health system. They didn't allow a centralized server to handle authentication and authorization procedures, instead, they allowed both the patients and doctors to carry out authorisation process. In fact, users are permitted access based on their privileges without disclosing their attributes and identities. This framework addresses and solves the problem of handling and maintaining security, privacy as well as variability of all users' attributes [9]. However, there is no room for collaborative sharing of medical data across different domains. The framework is too complex to implement. As of now, there is no real-life implementation to prove its efficiency as claimed by the authors.

With all the available literature, particularly those reviewed in the foregoing, it is very clear that nearly all the existing models are suffering from one challenge or the other. Majorly, some of the current models are having challenges of scalability. Interoperability [4], flexibility, compatibility, improper model evaluation and inability to implement in a distributed environment such as cloud computing among others.

To solve these problems, this project aims at building a very efficient, dependable, reliable and secured architecture that will allow sharing of information among health care practitioners in all the nine (9) provinces that are available in the Republic of South Africa with specific interest in HIV-AIDS data and information which has been explained in the previous sections.

7.0 CONCLUSION AND RECOMMENDATION

E-Health is a very important initiative for sharing and accessing medical information among various healthcare providers. To leverage on its benefits to the fullest, the issues of privacy and confidentiality must be considered. In order to achieve maximum security therefore, authors propose access control for HIV patients. In solving this great challenge, we propose an architectural framework with algorithms that defined various policies for authorization and authentication among entities considered. Consequently, we strongly believe that the proposed framework which is currently being implemented will assist in no small measure in securing the privacy of HIV patients' information in South Africa.

REFERENCES

[1] AL-nassar1, B. A., Abdullah, M. S., & Osman, W. R. (2011). Healthcare Professionals use Electronic Medical Records. IJCSNS International Journal of Computer Science and Network Security System (EMRs) in Jordan Hospitals, 112-118.

[2] Avert. (2016, December 01). HIV & AIDS. Retrieved June 27, 2017, from https://www.avert.org:

https://www.avert.org/professionals/hiv-around-world/sub-saharan-africa/south-africa

[3] Azeez, N. A., & Ademolu, O. (2016). CyberProtector: Identifying Compromised URLs in Electronic Mails with Bayesian Classification. International Conference Computational Science and Computational Intelligence (CSCI) (pp. 959-965). Las Vegas, NV, USA: IEEE.

[4] Azeez, N. A., & Venter, I. M. (2013). Towards ensuring scalability, interoperability and efficient access control in a multi-domain grid-based environment. SAIEE Africa Research Journal, 54-68.

[5] Bahtiyar, S., & Çağlayan, M. (2014). Trust assessment of security for e-health systems. Electronic Commerce Research and Applications, 164–177.

[6] Barua, M. R., Lu, R., Liang, X., & Shen, X. (2011). PEACE: An Efficient and Secure Patient-centric Access Control Scheme for eHealth Care System. The First International Workshop on Security in Computers, Networking and Communications (pp. 970-975). Shanghai, China: IEEE.

[7] Cornford, T., & Shaikh, M. (2013). Introduction to information. London: University of London. Fan, L., Lo, O., Buchanan, W., Ekonomou, E., Sharif, T., & Sheridan, C. (14). SPoC: Protecting Patient Privacy for e-Health Services in the Cloud. (pp. 1-6). IEEE.

[8] Gajanayake, R., Iannella, R., & Sahama, T. (2014). Privacy Oriented Access Control for Electronic Health Records. e-Journal of Health Informatics, 8, No 2, 175-186.

[9] Guo, L., Zhang, C., Sun, J., & Fang, Y. (2012). PAAS: A Privacy-Preserving Attribute-based Authentication System for eHealth Networks. 2012 32nd IEEE International Conference on Distributed Computing Systems (pp. 224-233). Macau, China: IEEE.

[10] Kumar, M. R., Fathima, M. D., & Mahendran, M. (2013). Personal Health Data Storage Protection on Cloud Using MA-ABE. International Journal of Computer Applications, 75(8), 11-16.

[11] Li, W., & Hoang, D. (2009). A new security scheme for e-health system. International Symposium on Collaborative Technologies and Systems, 2009. CTS '09. (pp. 361-366). Baltimore, MD, USA: IEEE.

[12] Liu, W., Liu, X., Liu, J., Wu, Q., Zhang, J., & Li, Y. (2015). Auditing and Revocation Enabled Role-Based Access Control over Outsourced Private EHRs. 2015 IEEE 17th International Conference on High Performance Computing and Communications (HPCC), (pp. 336-341). New York, NY, USA: IEEE.

[13] Shin, M. S., Jeon, H. S., Ju, Y. W., Lee, B. J., & Jeong, S. P. (2014). Constructing RBAC Based Security Model in u-Healthcare Service Platform. Scientific World Journal, 1-13.

[14] Simplicio, M. A., Iwaya, L. H., Barros, B. M., Carvalho, T. C., & Naslund, M. (2015, MARCH). SecourHealth: A Delay-Tolerant Security Framework for Mobile Health Data Collection. IEEE JOURNAL OF BIOMEDICAL AND HEALTH INFORMATICS, 19, NO. 2, 761-772.

[15] Sujansky, W. V. (1998, Sept). The benefits and challenges of an electronic medical record: much more. The Western Journal of Medicine, 169 n3, p176(8).

[16] Sunagar, V., & Biradar, C. (2014). Securing Public Health Records in Cloud Computing Patient Centric and Fine Grained Data Access Control in Multi Owner Settings. International Journal of Science and Applied Information Technology (IJSAIT), 3, No.4, 18-21.

[17] TB Facts. (2016, June 8). HIV Statistics. Retrieved June 2017, from http://www.tbfacts.org/hiv-statistics-south-africa/: http://www.tbfacts.org/hiv-statistics-south-africa/

[18] Zhu, H., Huang, R., Liu, X., & Li, H. (2014). SPEMR: A new secure personal electronic medical record scheme with privilege separation. 2014 IEEE International Conference on Communications Workshops (ICC) (pp. 700-705). Sydney, NSW, Australia: IEEE.

[19] Ayofe, A.N, Adebayo, S.B, Ajetola, A.R, Abdulwahab, A.F (2010) "A framework for computer aided investigation of ATM fraud in Nigeria" International Journal of Soft Computing, Vol. 5, Issue 3 pp. 78-82.

[20] Azeez, N.A, Olayinka, A.F, Fasina, E.P, Venter, I.M. (2015) "Evaluation of a flexible column-based access control

security model for medical-based information" Journal of Computer Science and Its Application. Vol. 22, Issue 1, Pages 14-25.

[21] Azeez, N. A., and Babatope, A. B. (2016). AANtID: an alternative approach to network intrusion detection. The Journal of Computer Science and its Applications. An International Journal of the Nigeria Computer Society, 129-143.

[22] Azeez, N. A., and Iliyas, H. D. (2016). Implementation of a 4-tier cloud-based architecture for collaborative health care delivery. Nigerian Journal of Technological Development, 13 (1), 17-25.

[23] Azeez, N. A., Iyamu, T., and Venter, I. M. (2011). Grid security loopholes with proposed countermeasures. In E. Gelenbe, R. Lent, and G. Sakellari (Ed.), 26th International Symposium on Computer and Information Sciences (pp. 411-418). London: Springer.

[24] Azeez, N.A., and Lasisi, A. A. (2016). Empirical and Statistical Evaluation of the Effectiveness of Four Lossless Data Compression Algorithms. Nigerian Journal of Technological Development, Vol. 13, NO. 2, December 2016, 64-73.

[25] Nureni, A. A., and Irwin, B. (2010). Cyber security: Challenges and the way forward. Computer Science & Telecommunications, 29, 56-69.

[26] David F. Ferraiolo and D. Richard Kuhn (1992) "Role-Based Access Controls" 15th National Computer Security Conference (1992) Baltimore, Oct 13-16, 1992. pp. 554-563

[27] Azeez N.A and Otudor A.E. (2016) “Modelling and Simulating Access Control in Wireless Ad-Hoc Networks”. Fountain Journal of Natural and Applied Sciences. Vol 5(2), pp 18-30.