

ACCESS CONTROL MEASURES FOR UGANDA NATIONAL LAND INFORMATION SYSTEMS TOWARDS CLOUD.

PRIVACY AND SECURITY ISSUES.

Jimmy ALANI, Godfrey TOKO, Lenin Victor OONYU, Richard OPUT and Joseph MIVULE, Uganda

Key words: Land Information System, UgNLIS, Cadastre Data, Privacy, Security, Access Control, Cloud Platform.

SUMMARY

The establishment of the Land Information System is based on the need to replace, the archaic manual land registration system with a reliable and secure Land Information System that allows stakeholders to make reliable and cost-effective decisions. In accomplishing these strategies, MLHUD adhered to ISO 27001:2013 and Uganda National IT Security Framework: 2014 as an Information security management framework, which is to provide reliable and secure Land Information System.

Land being a resource of utmost importance and there is increasing need to host the LIS in the cloud, this has become an attraction to cyber-attacks and hackers with primary goal of altering digitalized land and cadastral records. To secure the data in the land information systems, different access control mechanisms have been suggested by different scholars. The UgNLIS uses RBAC for user privileges and rights. As the LIS migrates to the cloud, there is need to implement the required access control systems and mechanisms to eliminate un-authorized access.

This paper presents an overview of the security of the UgNLIS, The different privacy and security challenges, current access control models and their suitable for the cloud.

1.0 Introduction

Land Information Systems (LIS) assist Uganda government in expediting delivery of Land services to the public. Some of the services include: - Transfer of interests, Registrations of mortgages, Securing Land tenure rights among others. [1] Defines LIS as a system made for land records, human and technical resources and appropriate procedures and techniques to collect analyze, maintain, disseminate and use this information.

The Uganda government secured funding from World Bank to support the development and implementation of the land information system. This was carried out in (03) three phases: - With the first phase having the baseline study, Preliminary Design of the Land Information System and Strategy for securing of land records which was completed in 2007. This was followed by the detailed design, Installation and pilot implementation in 2010. Phase III, rolled-out and decentralized the National Cadastre and the LIS across (22) twenty-two locations (zones) [2]. With the migration from the manual records (paper-based) to digitalization of the cadastral data and land records, it is important that the CIA triad is put into consideration.

2.0 PRIVACY AND SECURITY ISSUES IN LAND INFORMATION SYSTEMS

Security of the Land Information begins with the guarding of the sensitive records of personal land details thereby ensuring that the privacy, confidentiality and integrity of this information is achieved and maintained at all time in the system.

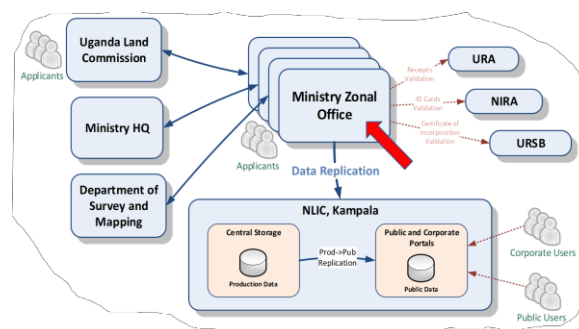


Figure 1: Architecture of the UgNLIS

Many Organizations and enterprises have shifted their Information systems to the Cloud for example IaaS (Infrastructure as a Service), PaaS (Platform as a Service) and SaaS [2] (Software as a Service. [3] The cloud provides enormous benefits however there is still prevailing

concerns regarding the aspect of its security and privacy. It is an obligation for CISO's to identify the challenges and benefits attributed to the cloud before deployment and migration of the LIS is performed. The research categories security challenges into the following: - Law and Ethics, Human Factors and CIA protection [4].

A. Human Factors

[3], argues that most of the security issues have been attributed to human behavior for example: BYOD where most of these devices bring vulnerabilities to the network. While technology alone cannot completely solve the issue of security risks, human element have to be equipped with the necessary IT security trainings and also adhere to the strict application of the security policies in place. Similarly, research from [3], indicate that Malware and spyware incorporated in mobile devices rose to 3,324 percent in previous seven months in year 2011. [3].

B. Law and Ethics

Regarding cloud computing, there are no specific laws to govern and regulate its usage, however different laws for example ISO/IEC 27017:2015 and GDPR Act have been developed internationally to address information security controls for cloud services. The international Security of Standardization (ISO) has played a big role in guiding use of cloud platform with aim of inducing confidence in the cloud users. There are laws that govern personal data protection in Uganda, these include: - Data Protection Act

2019, Electronic Signature Act, 2011 and Electronic Transaction Act, however all these laws do not specifically address all the issue of cloud usage. Currently, DPPA under National Information Technology Authority-Uganda (NITA-U) is responsible for overseeing the implementation and enforcement of Data Protection across data collectors and controllers. Users of UgNLIS are mandated to follow the IT Security Policy and ensure compliance as stated in the security document however, this policy is also limited to the local operating environments and does not address cloud based environment.

C. Confidentiality, Integrity and Availability (CIA) Protection

Migration from the manual based land records through digitalization of the cadastre and Land Information exposes the data to security breaches with compliance and privacy issues. CIA protection is vital while implementing information systems, the UgNLIS allows users to access specific land transaction records through the public and corporate portal using public internet which is most of the time utilized under public cloud services without notice [4].

(i) Confidentiality:

This is the ability to leverage safety of information in the Land Information System to only authorized users, this is normally through different roles specified by the developers. Similarly, user privileges and rights are accessed from the pre-defined access control list. The UgNLIS harbors information regarding spatial data, personal information for example land owner identification documents, their signatures and sensitive information regarding mortgage details among others. This information should be kept confidential and only accessible to specific users at different levels of access. Therefore, as data in the UgNLIS is migrated to the cloud, it is paramount that the cloud vendors ensure that authorization of resources is strictly accessible to only intended users through the customized cloud authorization mechanisms since cloud vendor centers are normally geographically dispersed in different locations.

(ii) Integrity:

It is always paramount that the integrity of data stored in the LIS is maintained even in case of any alteration made. In many occasions data might lose its authenticity during migration of data. It is therefore important that data in the UgNLIS is accurate to avoid such issues. Most of the data integrity issues in the LIS are caused by authorized users who erroneously make entries in the system without validation of data for example Identification numbers and Tax Identification Numbers while running a transaction.

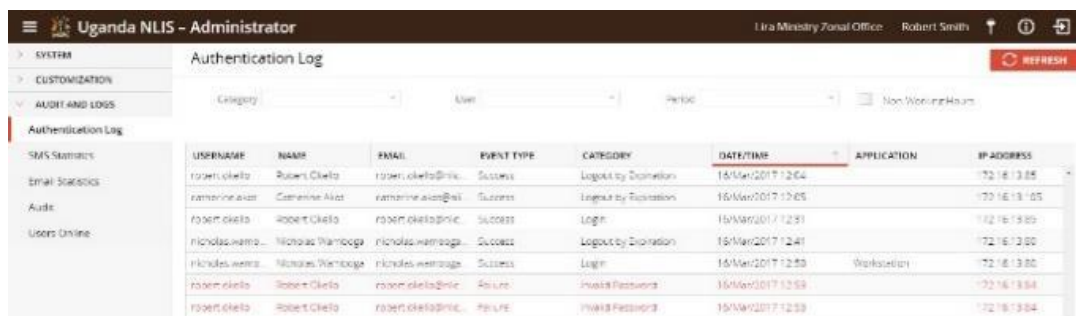
(iii) *Availability:*

The UgNLIS should be accessible to authorized users during official working hours, [5] calculated availability as the percent of time an application and its corresponding services are accessible in a given time interval. According to [6]), it was reported that cloud Foundry losses almost

\$336,000 of revenue and PayPal approximately \$225,000 per hour due to system availability issues. Delivering and ensuring higher level of availability is one the biggest challenges faced by cloud vendors today. As UgNLIS migrates to the cloud it is important that cloud providers address service availability issue to reduce on loss of revenue to the government during downtime and to meet the quality of service (QoS) requirements, service level agreements thereby increasing on profitability of the LIS. There is increasing need to deploy highly reliable and uninterrupted cloud services while effectively utilizing all the resources [7].

3.0 AUTHENTICATION IN THE UGNLIS

Authentication is defined as the process of granting and denying a user access to a system. Users of the UgNLIS system are requested to provide correct user login details: - that is a “username” and “password” in order to authenticate into the system. The system will then validate the details provided factoring in other attributes like location of the subject requesting for access to the system. On this ground, the centralized user system management grants or deny access to a user. The UgNLIS has the capability to log and report authentication activity provided in the system dashboard thus tracking any login successes and failures.



USERNAME	NAME	EMAIL	EVENT TYPE	CATEGORY	DATE/TIME	APPLICATION	IP ADDRESS
robert.okeja	Robert Okeja	robert.okeja@nlis...	Success	Logout by Discretion	15/Mar/2017 12:04		72.16.13.85
ramonine.alex	Catherine Alex	ramonine.alex@nlis...	Success	Logout by Discretion	15/Mar/2017 12:05		72.16.13.105
robert.okeja	Robert Okeja	robert.okeja@nlis...	Success	Login	15/Mar/2017 12:01		72.16.13.85
nicholas.wambo	Nicholas Wambo	nicholas.wambo@nlis...	Success	Logout by Discretion	15/Mar/2017 12:41		72.16.13.80
nicholas.wambo	Nicholas Wambo	nicholas.wambo@nlis...	Success	Login	15/Mar/2017 12:55	Workstation	72.16.13.80
robert.okeja	Robert Okeja	robert.okeja@nlis...	Failure	Invalid Password	15/Mar/2017 12:59		72.16.13.84
robert.okeja	Robert Okeja	robert.okeja@nlis...	Failure	Invalid Password	15/Mar/2017 12:59		72.16.13.84

Figure 2: Illustration of the Authentication log dashboard

4.0 ACCESS CONTROL IN LAND INFORMATION SYSTEMS

Access control is the basis for all security disciplines, not just IT security. The purpose of access, control is to allow authorized users access to appropriate data and deny access to unauthorized users. Seems simple, right? It would be easy to completely lock a system down to allow just predefined actions with no room for leeway. In fact, many organizations, including the U.S. military, are doing just that restricting the access users have to systems to a very small functional capability. However, with increasing dependence on the Internet to perform work, systems must be flexible enough to be able to run a wide variety of software that is not centrally controlled. [8]

Access controls protect against threats such as unauthorized access, inappropriate modification of data, and loss of confidentiality. Access control is performed by implementing strong technical, physical, and administrative measures. [8] [9] The UgNLIS comprises of sensitive personal data, cadastre and land information that is required to be accessed by specific categories of users. According to (cite), organizations with information systems needs to ensure that the CIA triad is fully achieved by adopting the appropriate access control mechanisms to ensure data privacy and security protection of resources. Different organization apply specific access control models basing on the structure of data and company resources to be utilized. Below are some of the available traditional access control methods: - Discretionary Access Control, Mandatory Access Control and Role Based Access Control.

A. *Discretionary Access Control (DAC)*

The owner of the data places controls on data. The owner determines who has access to the data and what privileges they have. Discretionary controls represent a very early form of access control and were widely employed in VAX, VMS, UNIX, and other minicomputers in universities and other organizations prior to the evolution of personal computers. Today, DACs are widely employed to allow users to manage their own data and the security of that information, and nearly every mainstream operating system, from Microsoft and Apple to mobile operating systems and Linux supports DAC. The advantage of a DAC-based system is that it is primarily user-centric. The data owner has the power to determine who can (and

cannot) access that data based on the business requirements and constraints affecting that owner. While the owner never has the ability to ignore or contradict the organization's access control policies, he or she has the ability to interpret those policies to fit the specific needs of his or her system and his or her users. [9]

[10], asserts that DAC provides full control of objects created by owner for example: - subjects (owners) have control of their data and can share it with other subjects without any say from the system administrators. Therefore, such in a scenario, a slight mistake made by subjects (owners of files) can lead to a data integrity issues for instance sharing a file with another user in the windows environment. Discretionary Access Control has been defined by TCSEC as “*way of restricting access to objects based on identity of subjects and groups they belong*”. This kind of access control provides the capability of passing privileges to other subjects. [11].

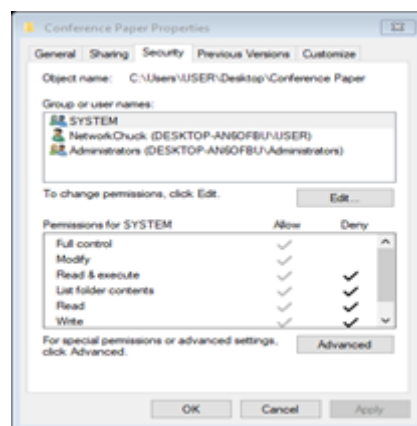


Figure 3: Showing Grant and Deny permission of file (DAC) in windows Environment

DAC is based on Access Control Lists and therefore gives grant or deny permissions to users (owners of the objects) unlike the MAC. [12].

B. Mandatory Access Control (DAC)

Mandatory Access Control (MAC) is system-enforced access control based on subject clearance and object labels. Subjects and objects have clearances and labels, respectively, such as confidential, secret, and top secret. A subject may access an object only if the subject's

clearance is equal to or greater than the object's label. Subjects cannot share objects with other subjects who lack the proper clearance, or "write down" objects to a lower classification level (such as from top secret to secret). MAC systems are usually focused on preserving the confidentiality of data. [10]

The MAC model is built on a distributed administrative architecture which is more secure than the Discretionary Access Control Model, in this access control the subject (owner) of the resource does not have the rights to decide who gets access to that specific resource however the access remains with an individual or a group and dictates who can have access to the resource. Most resources that use the MAC are normally labeled as *Secret*, *Top Secret* etcetera [13]. MAC is usually implemented in government agencies with information regarded as very sensitive therefore access to these specific resources is always exclusive. This model is considered as rigid because it is not operated using dynamic or context-aware conditions for example accessing a resource from a different device, location or time period. The MAC model has some limitations that include: - unable to cater for least privilege, separation of duties and inheritance [14].

C. Role-Based Access Control (RBAC)

Role-Based Access Control (RBAC) defines how information is accessed on a system based on the role of the subject. [10] A role could be a registrar of titles, a land administrator, a surveyor, etc. Subjects are grouped into roles, and each defined role has access permissions based on the role, not the individual. According to the National Institute of Standards and Technology (NIST), RBAC has the following rules:

1) Role assignment: A subject can execute a transaction only if the subject has selected or been assigned a role. The identification and authentication process (e.g., login) is not considered a transaction. All other user activities on the system are conducted through transactions. Thus, all active users are required to have some active role.

2) Role authorization: A subject's active role must be authorized for the subject. With (1) above, this rule ensures that users can take on only roles for which they are authorized.

3) Transaction authorization: A subject can execute a transaction only if the transaction is authorized through the subject’s role memberships, and subject to any constraints that may be applied across users, roles, and permissions. With (1) and (2), this rule ensures that users can execute only transactions for which they are authorized [1] [10].

RBAC came into existence when organizations started using multi-user applications and online applications in 1970s. The model is based on the notion that permissions are associated with roles and users are assigned role depending on job function in the organization [15]. Roles in the RBAC models are regarded as a representation of natural language which is constructed in a semantic way to allow formulation of access control policy. A role can be described as an ability to perform specific tasks for example: Data Entry, Scanning Clerk or Registrar. According to study by NIST, RBAC is able to address government and most organizational needs that have concerns relating to: - privacy protection, restriction from unauthorized access, adherence to professional standards and customer & stakeholder confidence [16]. The following aspects have to be put into consideration while implementing the RBAC, these include: - transaction *assignment*, *role authorization* and *role assignment*. *Transaction authorization*: - This aspect addresses the fact that transactions can only be performed by an authorized subjects with active roles in the system as illustrated below.

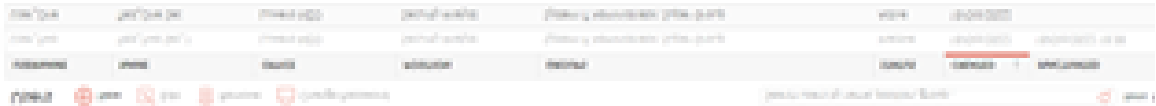


Figure 4: Illustration of transaction authorization

As depicted in the illustration above, the security Analyst, “*Test_Two_Sec_1*” cannot perform any transactions in the system since the status of the role is inactive therefore a transaction can only be performed by another active user “*Test_One_Sec*”.

Role Authorization: - Ensures that users of the system have access to only roles that have been assigned to them (authorized roles) thereby leveraging data integrity. This is however different when it comes to DAC since it allows inheritance of roles and privileges which can eventually end up compromising the confidentiality of information in the system.

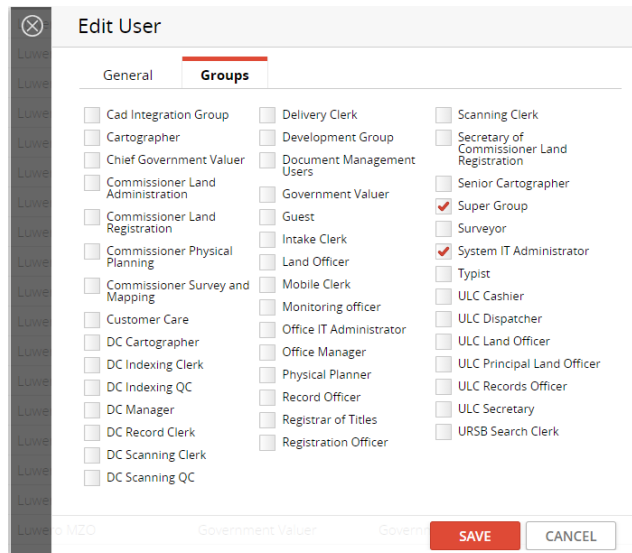


Figure 5: How roles are assigned to users

Role assignment: This allow fine grain access to LIS resources by only authorized subjects (users). For example, transactions can only be executed by resource owner if this condition is met. (“A role has been assigned”). Likewise, RBAC model has objects that can be defined as files, directories or sometimes referred to as resources.

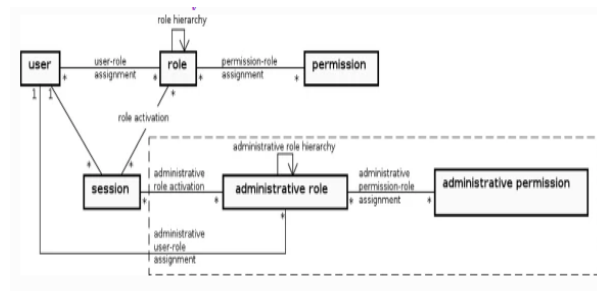


Figure 6: Illustration of RBAC

The primary benefit of RBAC is that it allows customization to suit organization needs, furthermore, the support of top fundamentals of security which is data abstraction and separation of duty make it richer than the DAC and MAC.

Data Abstraction: It is through RBAC that a subject is able to access requests for specific object from the UgNLIS database for example request to know who owns a specific land parcel

through providing the *Block* and *Plot* parameters, the system is able to return the high level details (parcel owner) without exposing the all complex computations performed.

Separation of Duty: The UgNLIS applies RBAC as a way to allow authorization of resources to subjects. It is vivid that mutually exclusive roles can be invoked just in-case there is need to complete a specific Land transaction. Secondly, all no user (subject) is granted access to carry-out a transaction from beginning to end that is to say (Intake to registration). Each user on the UgNLIS has a specific role to play on a transaction therefore no single user of the system can be judged or executed in case of a fraudulent transaction. The main goal of SoD is to minimize risks of loss thus increasing confidentiality, integrity and availability of transactions in the UgNLIS.

5.0 CONCLUSION

The use of cloud computing has been widely adopted by many organizations since it provides many benefits like high computation power, scalability of applications, access to information from different locations and lower cost operation and maintenance by the user. However, security and privacy aspects have to be clearly defined and implemented to prevent data loss and breaches.

The UgNLIS typically runs on a RBAC mechanism that is centralized and to migrate LIS operations to cloud there is need to adopt a tailored access control mechanism to tape into the many benefits of the cloud. Nevertheless, cloud vendors have constantly innovated cloud services to tackle the privacy concerns relating to how data is accessed, managed and stored.

REFERENCES

- [1] B. Mireille, Z. Jaap and K. A. Berhanu, "Good Practices in Updating Land Information System that Used Unconventional Approaches in Systematic Land Registration," *MDPI Land* 2021, vol. 10, p. 437, 2021.
- [2] J. R. Oput, "Implementation of the National Land Information System (NLIS) in Uganda: Strengthening land governance," in *Annual World Bank Conference on Land and Poverty*, Washington, DC, 2018.
- [3] W. Yong, W. Jinpeng and V. Karthink, "Bring Your Own Device Security Issues and Challenges," *The 11th Annual IEEE CCNC-Mobile Device, Platform and Communication*, pp. 80-85, 2014.
- [4] Flexera, "Cloud Computing Trends: Flexera 2022 State of the Cloud Report," *CLOUD MANAGEMENT*, 2021.
- [5] T. Maria and T. Francis, *Service Availability: Principles and Practices*, Canada: John Wiley & Sons, 2012.
- [6] E. T. Patricia, R. Moises, G. E. Glauco, K. Judith and S. H. Djamel, "High availability in clouds: systematic review and research challenges," *Journal of Cloud Computing: Advances, Systems and Applications*, pp. 5-16, 2016.
- [7] S. Brett, R. Jordan, G. Robert, D. Vijay and A. Mansoor, "Evaluation and design of highly reliable and highly utilized cloud computing systems," *Journal of Cloud Computing*, pp. 11-13, 2015.
- [8] C. Eric, M. Seth and F. Joshua, *CISSP Study Guide*, Syngress, 2012.
- [9] G. Adam, *The Official (ISC)2 Guide to the CCSP CBK*, Sybex, 2016.
- [10] C. Eric, F. Joshua and M. Seith, *Domain 5: Identity and Access Management (Controlling Access and Managing Identity)*, Elsevier Inc, 2016, pp. 293-327.
- [11] W. Craig, "How to Survive Information Systems Audit and Assessments," in *The IT Regulatory and Standards Compliance Handbook*, Elsevier Inc, 2008, pp. 73-114.

- [12] R. Derrick, "Chapter 2 - What Is Federated Identity?," in *Federated Identity Primer*, Elsevier Inc., 2013, pp. 13-36.
- [13] A. Jason, "Understanding the Fundamentals of Infosec in Theory and Practice," in *The Basics of Information Security (Second Edition)*, Elsevier Inc, 2014, pp. 39-56.
- [14] M. Kubbo, J. Manoj and R. E. Muhammad, "Privacy and Security Challenges Towards Cloud Based Access Control in Electronic Health Records," *Asian Journal of Information Technology*, pp. 274 - 281, 2017.
- [15] D. N. Carlos, M. C. Paulo and S. Adenilso, "Similarity testing for role-based access control systems," *Journal of Software Engineering Research Development*, p. 6:1, 2018.
- [16] S. S. Ravi, C. J. Edward, F. L. Hal and Y. E. Charles, "Role-Based Access Control Models," *IEEE Computer*, pp. 38-47, 1996.
- [17] H. C. Vincent, F. David, K. Rick, S. Adam, S. Kenneth, M. Robert and S. Karen, "Guide to Attribute Based Access Control (RBAC) Definition and Consideration," *National Institute of Standards and Technology*, 2014.

BIOGRAPHICAL NOTES

The authors' of this document have worked in the Land Sector for over 10 years with major specialties in the Land Administration and Management Sub Sector. Most of them are members of the respective Survey, ICT and Management Memberships in the Country. One of their key achievements is the transformation Land Administration in Uganda, from establishing a functional National Land Information Systems to Systematic Land Adjudication and Registration.

CONTACTS

Name: Jimmy Alani
Organisation: Ministry of Lands, Housing and Urban Development, Uganda
Address: P. O Box 7096, Kampala
City: Kampala
Country: Uganda
Tel.: +256772449748
Email: alanjim@gmail.com
Web site: <https://mlhud.go.ug>