International Journal of Computer (IJC)

ISSN 2307-4523 (Print & Online)

© Global Society of Scientific Research and Researchers

http://ijcjournal.org/

A Secure Application for Information Sharing in Organizations: A Case Study of Kabale District Local Government

Ivan Niyonzima[a*], Godfrey Omoda-Onyait[b]

[a]Faculty of Science, Department of Information and Communication Technology Kabale University, P.O.Box 317, Kabale.

[b]National Council for Higher Education.

[a]Email: nidkmax@gmail.com/iniyonzima@kab.ac.ug

[b]Email:gonyait@gmail.com

Abstract

Information shared is exposed to threats of confidentiality, integrity and availability needed for decision making in organizations. A case study was carried out at Kabale District local Government where interviews and questionnaires were administered to purposively selected elements of the study. The findings revealed that the information shared within the organization is exposed to potential threats that can put the organization's information at a risk of being accessed by unauthorized users. The following factors for securing information were identified and used in the development of a secure application for information sharing in organizations. These factors include; denying unauthorized staff and other individuals from gaining access to personal data, passwords to be treated as private to the individual, secure disposal of information, paper files to store in secure locations and only accessed by those who need to use them. In this application, the information is encoded using crypto-graphical methods that cannot be easily intercepted, such that only the intended recipient is able to receive it in its original format for decoding. This makes information shared secure. The application was tested and validated by a range of stakeholders and it was found secure. For the future work, a survey will be carried out in a range of organizations in order to develop an improved application for information sharing.

Keywords: A secure Application; Information Sharing; organizations; Crypto-graphical Methods.

----

* Corresponding author.

1. Introduction

The central goal of secure information sharing is to "share but protect" where the motivation to "protect" is to safeguard the sensitive content from unauthorized disclosure [1]. This elusive goal has been a major driver for information security for over three decades. In Uganda, the need for secure information sharing has dramatically increased with the explosion of the Internet and the convergence of outsourcing, off-shoring and collaboration in the commercial arena and the real-world demonstration of the tragic consequences of lack of information sharing in the national security arena. As technology has made the aspect of sharing easier, so has it increased the difficulty of enforcing the aspect of protecting information in other areas of the country.

As technology has made the aspect of sharing information easier, so has it increased the difficulty of enforcing the aspect of protecting information in other areas of the country. Therefore, coming up with an application for information sharing in organizations particularly Kabale District Local Government is the solution to Information sharing challenges that are existing currently and leading to the leakage, tampering and denying its correctness to the intended users in the institution.

As organizations increasingly access the benefits offered by the inexpensive computer and communications technology, the problems and concerns that accompany the benefits become more apparent. The application of computer technology offers possibilities of collecting a considerable amount of data and put it into managerial information to be shared within the local governments. Due to lack of standard methods for information sharing in government, the information sharing environment is not constantly assured to be risk free from the risks that might grip illegal access, malicious alteration and destruction of information [2]. Guaranteeing security for its Information Systems, together with computers and networks is a fundamental need for a digital government function to the hope and provision of service to its people.

2.1 Theoretical Framework

Figure 1 is the theoretical framework to explain how an application for information sharing works in an organization.

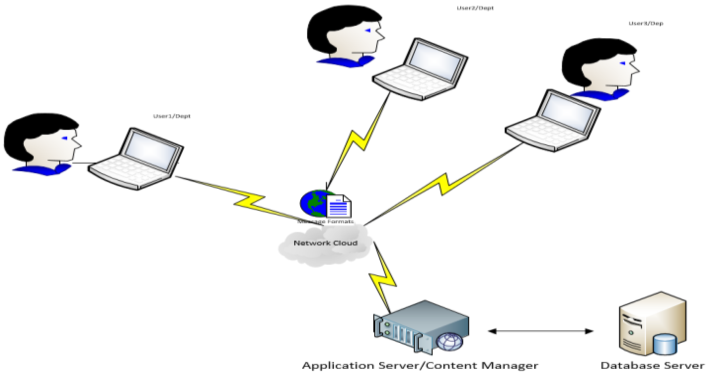


Figure 1. 1: Theoretical framework

Figure 1.1 represents the theoretical framework of the study. All departments within the organization will share the information via the organization's central Application server which encrypts information for storage purposes. The application server manages permissions of the files uploaded on the database to control accessibility by unauthorized parties in the organization. When a user request for information from the file server, the application server manages the decryption of information and sends it back to intended recipient. This helps the organization for easy decision making since the application is secure and can minimize the challenges involved in information sharing by denying intruders to access the information being shared.

2. Related Works

Researchers have presented approaches towards Secure Information Sharing between communicating parties as shown by the related reviews.

2.1 The Current Information Sharing Technologies

Reference [3] observed that information sharing is a key ingredient for organizations seeking to remain competitive. The understanding and practice of information sharing is becoming increasingly essential for organizations to stay competitive and boost portability. Research on supply chain management suggests that the key to the portability of an organization lies in the seamless supply chain.

Secure information sharing among multiple agencies does not only provide basic support for classifying information, encrypting data, ensure interoperability, but also address the controlling access to resources to multiple agencies and adapting to different user profiles and interface. Information sharing and security in dynamic coalitions is a complex task, which manifests itself throughout the lifetime of the coalition. Reference [4] identifies the critical issues that arise during a coalition's formation, and in support of its day-to-day management and usage.

Research on information sharing and social networks demonstrates that if information sharing is encouraged between and among organizational members, it is likely to lead to reduced product development cycle times and customer service response times, which could result in increased organizational productivity [5]. Sharing information using databases is often viewed as mediated sharing, since the database acts as a medium from which people later retrieve information. This requires organization members to exhibit responsible behavior in all their communications in order to contribute to the information exchange process. Organizational social structure is very important to information sharing among organization members. Users of information also need motivation to initiate a database search [5,6].

Reference [7] established a distributed information sharing model as well as investigated the technique standard support of the model. It was deduced that the expenditure of dealing with government information exchange and cooperation between agencies will be minimized by a raise in the potential and efficiency of agencies' collaboration due to the secure e-government information sharing elucidations.

Reference [8] examined the demands in integration, aggregation and secure sharing information to facilitate situation consciousness and response at the strategic level. On extraction of data from various independent systems, the system filters, integrates, and proficiently envisages information indispensable to obtain a general operational picture, by utilizing context-sensitive parameters. One considerable demand was to assist secure information sharing. Sharing of information prolongs to be a major complexity due to the data privacy and ownership concerns as well as owing to a widespread range of security policies followed inside various government agencies.

Reference [1] presented a way to share secure information easily through modern Trusted Computing (TC) technologies which is not available with pre-TC technology. They have configured the PEI framework of policy, enforcement and implementation models, and demonstrated its applicability in inspecting the issue and generating solutions for it. The framework enables the deep investigation of potential TC applications for secure information sharing in the upcoming work. TC applications excluding information sharing as well are expected to be scrutinized.

2.2 Online Secure Information Sharing Applications as a Solution

Online secure information sharing can be one of the solutions to reduce the information sharing challenges in the country. It can be used to acquire new clients from previously District Local Government segments especially those who are willing to embrace new technologies which meet their real needs.

Online information sharing can be used for information transfer in between organization departments and archiving of old documents. Clients are therefore in control of their files and also make sure that a file is only accessible by the assigned staff in the organization at all times.

Reference [9] noted that the use of online information sharing applications can help to cut down the costs of coordination, communication and information processing and enable service provision at a lower cost. Online information sharing can promote the dual objective of district local government institutions which is the sustainability and outreach to the poor people. This can help Local government to reduce the corruption tendencies, expand their community outreach activities and provide affordable and flexible services to clients than the current queue mechanisms currently at districts.

3. Methodology

This section focuses on the steps and procedures taken in order to accomplish the project. It comprises of techniques and data structures that were employed in the research study, data collection, analysis design, implementation testing and validation. It includes the technologies used in implementing the prototype, and validation/testing of the developed application.

3.1 Systems Analysis

A number of research tools were used to determine requirements for a secure file sharing solution for KDLG in Uganda and they included; interviews, observation, questionnaires and review the existing literature with the view of identifying requirements for the proposed application.

3.2 Interviews

Interviews were conducted with key staff of the KDLG to gain an insight about the operations and challenges of district and to also find out their views about the introduction of online file sharing application for the institution. Interviews were conducted by the researcher and 46 interviewees were interviewed. They included; all the11 heads of departments. Because of the few heads of departments, purposive sampling was carried out and 35 employees who were randomly selected and interviewed. The selected interviewees were interviewed because they had relevant knowledge about the existing ways of information shared within the organization.

3.3 Observation

Observation technique was used to physically observe the bureaucratic processes in place, stationery consumed, time spent to respond to client requests for local government information, and the time it takes to process such records. The number of clients served compared to the number of waiting clients was also observed. Through this technique the researcher gained insight on how the lag will be minimized with the introduction of a secure file sharing application system for KDLG services.

3.4 Questionnaires

A questionnaire was developed and issued to selected respondents mainly KDLG clients and staff whose responses were analyzed to determine requirements for the prototype. The questionnaire had a Likert Scale format which included a five point format for the respondent to choose from. The tick-able agreement options consisted of “strongly agree”, “agree”, “neutral or no option”, “disagree” and “strongly disagree’ respectively. SPSS as an analysis software tool was used for presentation and analysis of the respondents’ data. The questionnaire technique was used to assess the client’s technology acceptance of the proposed file sharing application.

3.5 Application Design

The design addressed the functional and non-functional requirements that provided guidance on describing the data and process for an information sharing application for institutions.

3.5.1 Database Design

Microsoft Office Visio was used to draw Dataflow diagrams (DFD) to model requirements and give a clear understanding of the information sharing system for KDLG. Entity Relationship Diagrams (ERDs) were used to identify relationships between various entities in the system and associating these entities with attributes and attribute domains.

The database was designed using conceptual logical ERDs. MySQL database was used to store the information from user interaction through the system interface and also as a relational database management information system.

MySQL database was used to store file meta data, such as file names, location on server, access permission and security details as well as content. On the retrieval instance, SQL queries were used to create sets from the database in order to display information to authorize after comparing their details with those in the database and processes from different district departments and other related entities.

Data Flow Diagram

Data flow diagrams show the flow of information in and out of the information sharing Application.

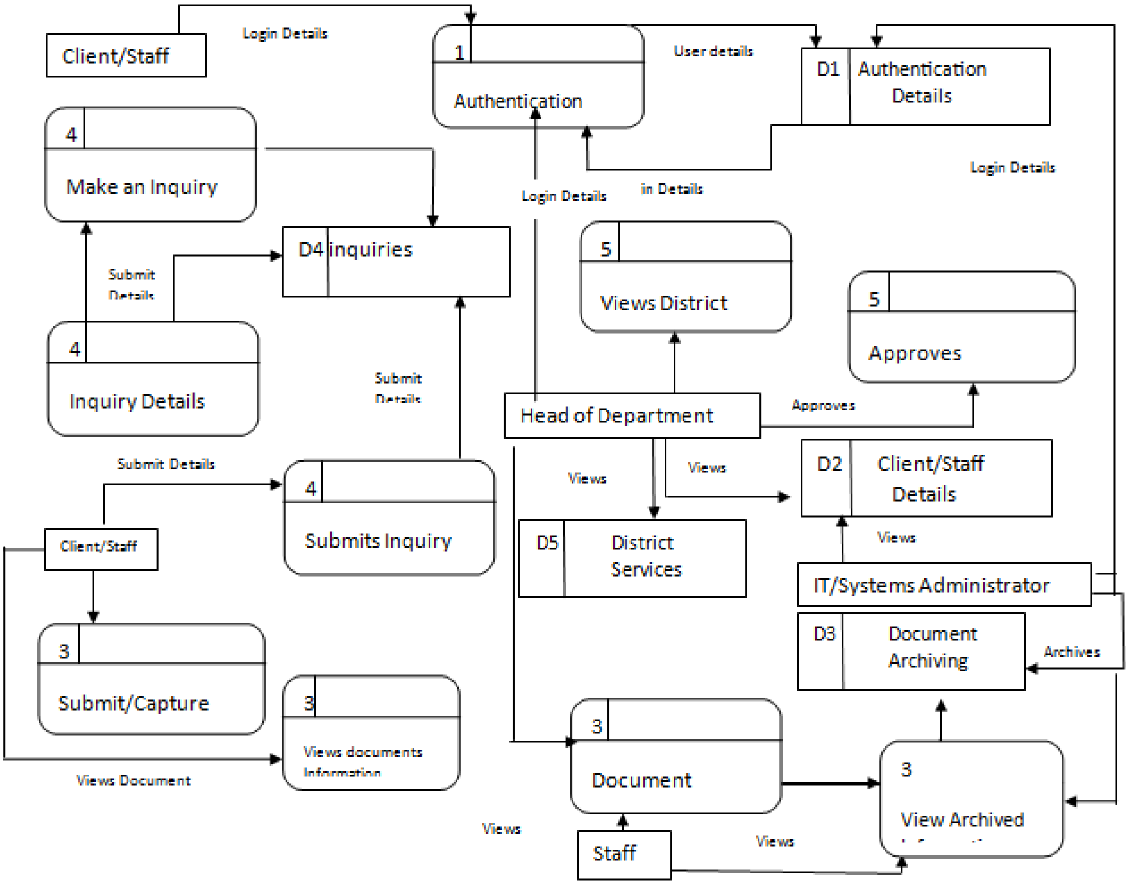


Figure2: Data flow diagram for the application for information sharing

Figure 2 shows the various processes used by the Application users. It shows the information accessed by the users and the process that takes place which includes, input, process and output.

3.5.2 Security

Being an information sharing application, the researcher took a deeper insight in user security, data security and interface standard as indicated below:

i). *User Security*

User access security is by User IDs and passwords. User IDs and Passwords are entered at the time of accounts application (sign up) by the client. To enhance security, the researcher used challenged response where a client must answer several personal questions correctly, according to his /her answers at the time he signed up.

ii). *Data Security*

This was mainly on the encryption provided by user's browsers, with the added security of requiring up-to-date versions with encryption.

3.6 Tools used for Implementation

Different tools were used in the implementation of the application. These tools included

(i) MySQL which is one of the world's most widely used relational database management system (RDBMS) was used for the database implementations needed for this project research. It is an open source RDBMS that runs as a server providing multi-user access to databases. Being open source software makes it cheap to use. It also has widely spread documentation making it easy for developers to work with.

(ii) HTML, which stands for Hypertext Markup Language, was used to design the interface pages for the application to be achieved. It provided a means to create structured documents by denoting structural semantics for text such as headings, paragraphs, lists, links, quotes and other items. It allowed images and objects to be embedded and used to create interactive forms.

(iii) PHP is the server side language that was used to connect the client language HTML and the database management system, MySQL. It was used mainly because it is an open source language and compatible with most of the database management systems as compared to other languages.

PHP script can be embedded straight into the heart of html code.

(iv) JavaScript is considered to be one of the most famous scripting languages. The main usage of JavaScript is to add various Web functionalities, Web form validations, browser detections and creation of cookies. JavaScript is one of the most popular scripting languages and that is why it is supported by almost all web browsers available today like Firefox and Google chrome.

(v) Cascading style sheets (CSS) were used to format the layout of Web pages. The basic purpose of CSS is to separate the content of a web document (written in any markup language) from its presentation (that is written using Cascading Style Sheets). There are lots of benefits that one can extract through CSS like improved content accessibility and better flexibility.

3.7 Application Testing and Validation

The application was run to identify errors for correction and the validation was done based on users opinion using the validations and testing questionnaire to ensure that the goals and the objectives of the project were achieved. The users were selected based on their experience in information techniques. They were asked to rate the extent to which the system met the expectations of the information sharing application for Kabale District Local Government (KDLG). Routine system testing and validation of the prototype system was done throughout the development process to ensure that quality and integrity were maintained.

4. Presentation of the results

Interviews, observations and questionnaires were used to gather user requirements for the system. Multiple questions were used and the users were able to give views on how the online an Application for Information Sharing Management system should function. There were two categories of users interviewed which included; the heads of department and employees/staff. The researcher used a Likert Scale format which uses 5-tickable option for agreeing with the question. The five options include “Strongly Agree”, “Agree”, “Undecided” and “Disagree” and “Strongly Disagree”. The researcher used SPSS to capture, compile and analyze data from questionnaires so as to determine the requirements for the system. The interview questions were given to different respondents in different offices as illustrated in table 1

Table 1: Sharing of Information

Is there any information sharing within the Organization	Frequency	Percentage (%)
Yes	84	91.3
No	8	8.7
Total	**92`**	**100**

Table 1 above shows that 91.3% of the respondents indicated that there is some form of information sharing within the organization whereas 8.7% of the respondents said that there is no information shared with the organization.

Information about the existing ways of securing information shared in organizations at Kabale District local government headquarters in Kabale District are presented in this section.

Figure 3 shows; the majority of respondents (68%) reported that one of the existing ways of securing information in the organization is through restricting access to the organization’s data and information, 19% of the respondents reported the use of strong passwords and 13.0% of the respondents reported backing up data frequently as one of the ways they have been using while sharing the information within the organizations.

There is Information sharing challenges that respondents reported. These included loss of information, tampering with information, blocking of information, leakage of information, guaranteeing of information and privacy as illustrated in figure 4.

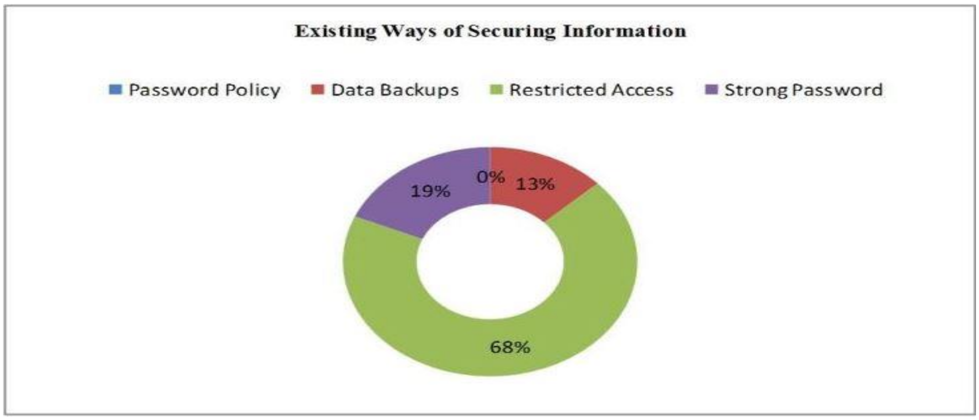


Figure 3: Existing Ways of Securing Information

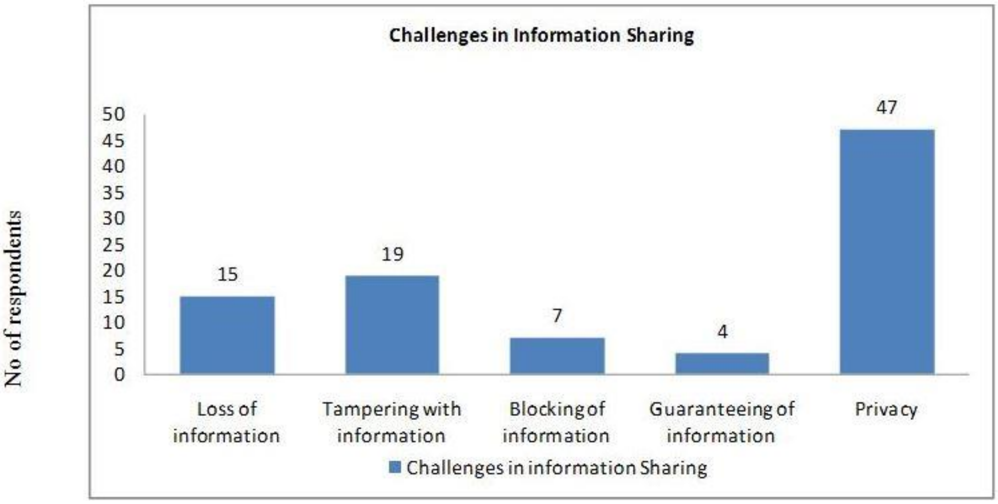


Figure 4: Challenges in information Sharing

Figure 4 shows the challenges in information sharing. The majority of the respondents 47 (51.1%) indicate that privacy during information sharing within organizations is the major security challenge that most employees' face. 19 (20.7%) of the respondents reported tampering with the information, 15 (16.3%) of the respondents reported loss of their information during the process of sharing information within organizations, while blocking and guaranteeing of information registered the lowest number of respondents 7 (7.6%) and 4 (4.3%) respectively.

The results from the respondents on the measures to be put in place for the security of information shared, protection of information shared, physical security at the premises of the organization, and levels of access control as shown in the tables below;

Table 2 shows the security measures. From the responses obtained, a number of employees at Kabale district local government headquarters were asked the measures they think would be put in place for the security of information shared within the organizations. Most of the respondents (employees) 27.2% said that if it's to be electronically shared, the computers within the organizations containing personal and organizations' data should be password protected.

Table 2: Security Measures

Measure	Number of respondents	%age
Ensure that unauthorized staff and other individuals are prevented from gaining access to personal data.	16	17.4
Ensure visitors are received and supervised at all times in areas where personal data is stored.	04	4.3
Ensure computer systems containing personal and organization's data are password protected.	25	27.2
Passwords must be treated as private to the individual and must not be disclosed to others	13	14.2
Ensure the secure disposal of information (electronic and on paper).	08	8.7
Check that the intended recipients of faxes, emails and letters containing personal data are aware the information is being sent and can ensure security on delivery.	04	4.3
Ensure your paper files are stored in secure locations and only accessed by those who need to use them.	22	23.9
Total	**92**	**100**

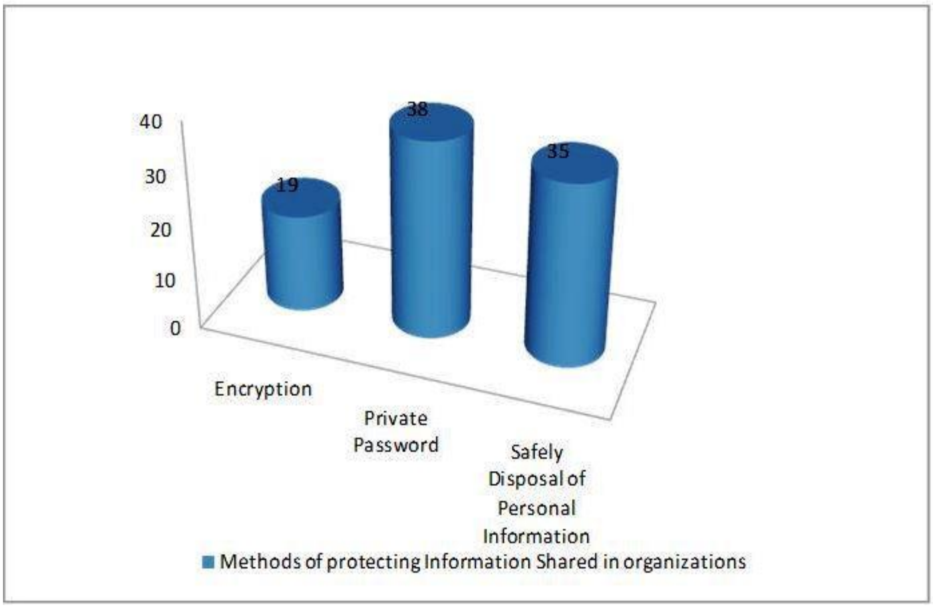


Figure 5: Methods of Protecting Information shared in organizations

Figure 5 shows the methods of protecting information shared in organizations. From the findings a large number of the respondents 38 (41.3%) agreed that keeping passwords private is one of the most methods to protect information shared within organizations, 35 (38%) of the respondents said that safely disposal of personal information would also be another method of protecting information shared within organizations while 19 (20.7%) of the respondents said that information shared within organizations can be protected through the use of encryption.

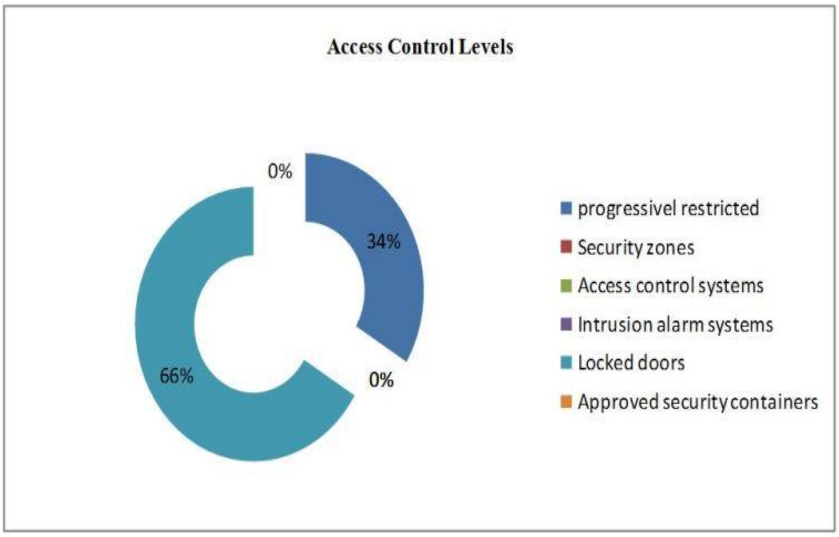


Figure 6: Access Control Levels

Figure 6 shows access control levels. In the figure, different access control levels within the organization were looked at, and a large number of respondents (66%) said they would prefer locked doors to other methods of control access, 34% of the respondents said, they would prefer progressively restricted areas no respondent preferred security zones, access control systems, intrusion alarm systems and approved security containers.

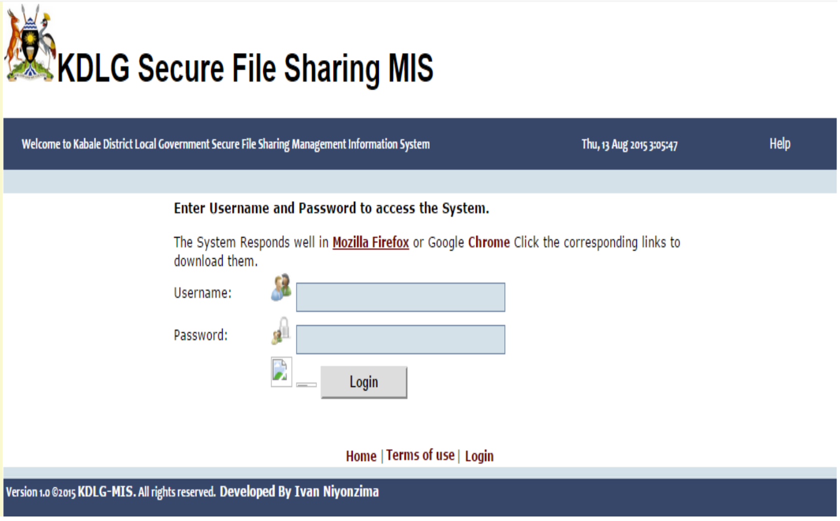
4.1 Application for Information Sharing

The Application was implemented using a WAMP server with Apache, MySQL and PHP as the principal components. The web solution was achieved through use of PHP as a tool whereas the interface pages for the application were achieved through HTML, and Cascading style sheets, JavaScript and Ajax framework for data validation for the data interchange. Microsoft word was used for the typing text and Microsoft Visio was used to achieve the flow charts and documenting data flow diagrams.

Once the application is started, it opens the homepage which is shown in figure below. At the home page the client, staff r super administrator can login given the correct authentication. Once the application opens, the super administrator can perform all the administrative roles including, adding and deleting of anything within the system. The client on the other hand only enters records into the application. Upon completion the users log out of the application.

(i) Application Login page

When a user accesses the secure application for information sharing online on the link shared above, below is the interface that appears on the home page. This interface (figure 7) is the point at which the client, staff or super administrator views the available services that are provided by the district as well as the secure application for information sharing. The interface of the application was designed using HTML. This interface is the point at which the client, staff and administrator gain access.



KDLG Secure File Sharing MIS

Welcome to Kabale District Local Government Secure File Sharing Management Information System Thu, 13 Aug 2015 3:05:47 Help

Enter Username and Password to access the System.

The System Responds well in Mozilla Firefox or Google Chrome Click the corresponding links to download them.

Username:

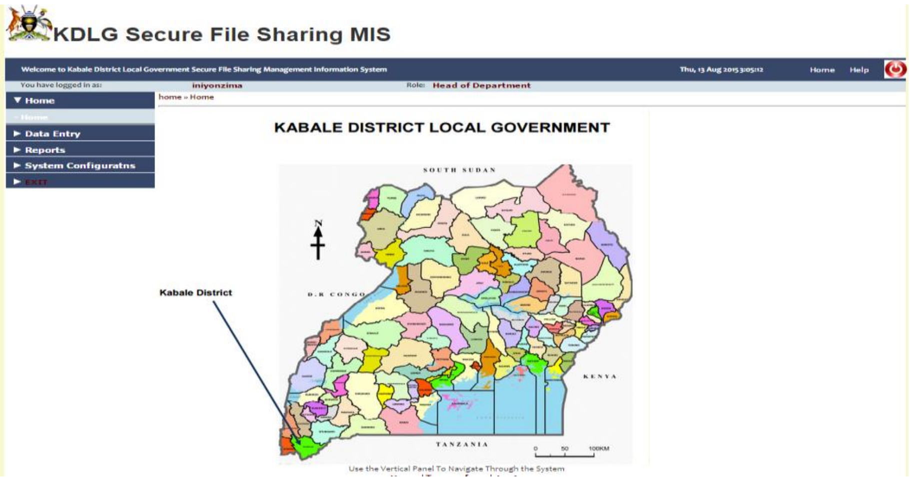
Password:

Version 1.0 ©2015 KDLG-MIS. All rights reserved. Developed By Ivan Niyonzima

Figure 7: Login for an Application for Information sharing

(ii) Application Home page

When a user accesses the secure application information for shared online on the link shared above, below is the interface that appears on the home page. This interface (figure 8) is the point at which the client, staff or super administrator views the available services that are provided by the district as well as the secure application for information sharing. The interface of the application was designed using HTML. This interface is the point at which the client, staff and administrator gain access.



KDLG Secure File Sharing MIS

Welcome to Kabale District Local Government Secure File Sharing Management Information System Thu, 13 Aug 2015 3:05:12 Home Help

You have logged in as: iniyonzima Role: Head of Department

KABALE DISTRICT LOCAL GOVERNMENT

Use the Vertical Panel To Navigate Through the System

Figure 8: Application for Information Sharing. Home page interface

Table 3: Application Validation results

	Rating Scale	**1**	**2**	**3**	**4**	**5**
1	This information system is easy to understand	0	0	1	8	1
2	This information system is easy to implement	0	0	4	3	3
3	This information system is easy to use	0	0	2	5	3
4	The system is fast and secure in managing and retrieving data	0	1	3	3	3
5	I will be willing to use the information system to get secure service delivery information	0	0	1	7	2
6	I would recommend this system to be used by various Local Government stakeholders to disseminate information	0	0	2	2	6
7	This information system addresses the need for an online secure system for information dissemination for organization service delivery	0	0	2	6	2
8	This information system meets our requirement for online secure information sharing.	0	0	4	5	1

5. Conclusion and Future Work

5.1 Conclusions

Information shared which is needed for decision making in organizations has become more a challenging issue in that it is accessed by both the authorized and unauthorized users which put the organizations on a competitive disadvantage. The aim of this research was to develop an application for information sharing and it was achieved through the development of the application. A case study was carried out at Kabale District Local government, and different research tools were employed in the collection of data, they included; questionnaires, interview guides and observation. These research methods were used because they were convenient for the researcher in carrying out the investigation in the field of information sharing within organizations. The application development was done using different technologies which included Data flow diagram, entity relation, security model in the design and Wamp server, JavaScript, PHP, html Ajax and MySQL in the implementation stages.

The researcher developed an application for information sharing in organizations. The Information sharing application developed provides many benefits to government and non-government organizations in that records and administrative works can be managed effectively and efficiently. The application enables information sharing among related departments and government providers. The results of the study will help to identify new requirements of how information sharing can be secured and be able to overcome current issues related to the security of information shared in organizations.

5.2 Future Work

Since the study was carried out in a shorter period, all the fields that were necessary in developing the application for information sharing were not exploited. Therefore, a survey could be carried out in a range of organizations in order to develop an improved application for information sharing.

References

[1] S. Ravi, R. Kumar and Z. Xinwen (2006.). "Secure information sharing enabled by Trusted Computing and PEI models", Proceedings of the ACM Symposium on Information, computer and communications security, 2 – 12.

[2] M. Fillia, S. Calliope, B. Beth, B., P. Grammati and M. Conalis-Kontos (2003). "A Safe Information Sharing Framework for E-Government Communication", IT white paper from Boston University.

[3] C. R. Moberg, B. D. Cutler, A.Gross, & T. W. Speh (2002). Identifying antecedents of information exchange within supply chains. International Journal of Physical Dis- tribution and Logistics Management, 32(9), 755–770

[4] E. Charles, T. Phillips, T.C. Ting and A.D. Steven. “Mobile and Cooperative Systems: Information sharing and security in dynamic coalitions,” Proceedings of the seventh ACM symposium on Access control models and technologies, Anaheim, CA, USA, June 2002, pp. 3-11.

[5] A. Barua, S. Ravindran, A.B. Whinston, (2007). Enabling information sharing within organizations. Information Technology and Management, 8(1), 31–45.

[6] S.` Li & B. Lin. (2006). Accessing information sharing and information quality in supply chain management. Decision Support Systems, 42(3), 1641−1656.

[7] L. Xin. (2007). "Distributed Secure Information Sharing Model for E- Government in China," Eighth ACIS International Conference on Software Engineering, Artificial Intelligence, Networking, and Parallel/Distributed Computing (SNPD 2007), 3, 958-962.

[8] R.A. Nabil, A. Vijay, S.A. Chun, E. John, S. Basit, V. Jaideep and X. Hui (2008). “Secure Information Sharing and Analysis for Effective Emergency Management”, Proceedings of the 9th International Conference on Digital Government Research Montreal, Canada, pp. 407-408.

[9] J. K. Ssewanyana, (2009). ICT Usage in Microfinance Institutions in Uganda. The African Journal of Information Systems (AJIS), 1(3), 5-28.