ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 12, December 2015

Secure automation of the Zambia Police Service business processes

Lyoko Gift[1], Phiri Jackson[2]

P.G. Student, Department of Electrical and Electronics Engineering, The University of Zambia, Lusaka, Zambia[1]

Head of Department, Department of Computer Science, The University of Zambia, Lusaka, Zambia[2]

ABSTRACT:A lot of developing countries don't have business process automation systemsfor security institutions. In this paper, we present a system designed for Zambia Police to automate their paper intensive processes. Beyond the automation process, some reports will be implemented for theirreporting needs. A baseline study was done to ascertain the levels of Information and Communications Technology (ICT) skills, security awareness and ICT tools utilization within Zambia Police Service. Results showed that 24% had received basic computer training, 39% use their personal email accounts for work communications and 36% use their personal devices to store work-related documents. The study also aimed to establish major business processes and identify the major security risks in the current workflows. A model was developed using the business process results. A web-based prototype that integrates fingerprint biometrics was developed using the model. The developed system showed improved business process through automation.

KEYWORDS:Information Management Systems, Security, Police, ICT, eGovernance.

I. INTRODUCTION

The growing usage of the internet brings with it various security concerns as we will show in the next section. This is amidst an environment where the various sectors of every country's economy rely heavily on the usage of Information and Communications Technology (ICT) solutions. Economic sectors such as banking [1], healthcare [2] and education [3] have benefited highly through innovative service delivery solutions. The investigative wings, in third world countries in particular, have not taken advantage of technology to make their work easier. Suffice to say that information security is very important in the security wings because of the sensitivity of the data they deal with on a daily basis.

In this research study, we propose a software prototype for the Zambia Police Service to automate their paper-intensive processes. We will review some of the most common security threats to consider when building information systems for investigative wings. We will then review some of the business processes for the Zambia Police Service from which a model will be developed. We will then discuss some of the results from a baseline study that we carried out with the aim of establishing the levels of ICT skills within the police service and to identify the points of security risks and how they can be corrected. We will then review the design for the system with the security considerations in place. Next we will present the developed prototype to date.

II. LITERATURE REVIEW

A. SECURITY CONSIDERATIONS

With the rapid increase in the number of devices on the internet, security is increasingly becoming a greater concern. Most cybersecurity experts agree that malware is a key choice of weapon for cyber-attacks [4]. Malware is usually loaded onto the host system without the owner's knowledge before running in the background. Various types of malware exist that include viruses, worms, spyware, bot executables and Trojan horses [4]. Malware exhibits different behaviour but is often intended to harm the host computer or another target machine.

The main principles of computer security are confidentiality, integrity and availability. Confidentiality assures us that the assets will only be accessed by the authorized parties. Integrity assures us that the assets can only be modified

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 12, December 2015

through authorized mechanisms by the authorized parties. Lastly, availability assures us that the assets will be accessed in a timely manner [4], [5]. When the last principle is not met, the result is a denial of service [5]. There are various mechanisms of carrying out a denial of service attack.

Due to the fact that huge amounts of information are shared on a daily basis, we will address some more aspects of security in relation to Information Security. These are authentication, access control and non-repudiation [6].

Authentication is the process of ensuring that the person sending or receiving information is who they claim to be. Access control deals with who can access information usually based on their rights. This is often implemented by using mechanisms such as usernames, passwords, biometrics and other mechanisms. Non-repudiation deals with a way of ensuring that a person cannot deny a transaction they previously performed [6]. This is especially important in electronic commerce. Various methods such as digital signatures, certificates and cryptographic technologies are employed here to ensure non-repudiation.

In addition, it is important to note that there are three main elements that affect security. These involve the people, the policies and procedures in place and the choice of technology that is used [6]. In this paper, we will concentrate on the technological aspects of security. There are a number of various threats that arise from the use of the internet. The threats can be loosely placed into three categories. These are hardware, software and network attacks [4].

Hardware attacks are those that are targeted at the hardware that hosts an asset of interest. The hardware attacks are comprised of hardware Trojan, illegal clones and side channel attacks. The existing mechanisms to counter these attacks include tamper-resistant hardware, trusted computing base, hardware watermarking and obfuscation [4].

Software attacks are usually targeted at software vulnerabilities within applications. Some of the most common attacks arise from software programming bugs such as poor memory management, race conditions and mismanaged user access privileges. Other attacks arise from software design bugs and deployment errors. The countermeasures against these attacks include secure coding practices such as type checking, runtime error and program transformation. The other measures are code obfuscation to prevent generation of code from installed assemblies, secure design and development and implementation of formal methods during the software life cycle.

The network threats include message privacy, spoofing, network protocol attacks and replay of messages [4], [7].

When a message is transmitted over the internet, it is possible to intercept it by a third party. Depending on the encryption method used during transmission, the messages might still be susceptible to interpretation [7] thereby exposing the privacy that the communicating parties expect. The technique where an attacker places themselves between two communicating parties is known as man-in the middle attack [8].

Message spoofing is a technique where an attacker falsifies the origin of a message and sends it to an unsuspecting entity on the same network. The attacker can wait for some time to eavesdrop on the authentication information between a legitimate entity and the service provider [7] and then use that information to masquerade as the victim.

Network protocol attacks are attacks that capitalize on the inherent vulnerabilities that exist within a protocol [4]. By exploiting a given vulnerability, an attacker can have access to all kinds of information from the victim's machine.

It is also possible to replay the authentication messages in order to impersonate a legitimate user. This attack tries to convince the server that the communication is coming from an authenticated user [7].

There are various countermeasures in existence for network attacks. One of the most common mechanisms is the use of the firewall for filtering traffic and allowing only specific kind of traffic. The traffic can be filtered out by the type of protocol, port number or content depending on the type of firewall that is in use. The second mechanism is the intrusion prevention and detection that aid in preventing or detecting a cyber-attack while it is in progress. The third mechanism is the use of a strong encryption algorithm for the communications. Lastly, another way to keep attackers away is to have managed Virtual Private networks (VPN) [4] that are not accessible on the internet.

Malware is spread to unsuspecting users using a number of methods. These include spam, phishing and drive-by downloads. Spam refers to unsolicited messages that are sent to many recipients usually with the aim of advertising. It is common for spam messages to contain links or attachments with malicious files. Phishing is a method of trying to get sensitive information such as usernames and password by masquerading as trustworthy. It is common for misspelled URLs to be included in spam emails that, when clicked, take the unsuspecting victim to the attacker's site that appears similar to the legitimate one. Lastly, drive-by downloads usually occur when a user visits a website with malicious content [4]. Sometimes even trusted sites are infected with malware thereby aiding the schemes of the attacker without realizing it.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 12, December 2015

Related Work

A lot of systems have been developed across the world for use in investigative wings. The first system we will discuss here is the Secure Real Time Platform [9]. This is shared by five countries and allows them to share biometric information for international fugitives. The five countries that use this system are Canada, United Kingdom, United States of America, New Zealand and Australia.

The government of Argentina is currently discussing with CrossMatch to deploy an Identity Management System in the country [10]. It is expected that the system will offer both fingerprint and palm print biometrics. Crossmatch support for law enforcement agencies includes civil applicant background check, criminal booking and multi-factor authentication for sensitive parts of the application.

In Canada, MorphoBIS software by Morpho is being used in two police stations for paper-less responses and real time identification. This system supports both fingerprint and palm print technologies and is expected to include iris recognition in the near future [10]. It was developed using a Service Oriented Architecture (SOA), works best with Oracle 11g database and currently interoperates with other systems like the Automated Fingerprint Identification System (AFIS).

The Federal Bureau of Investigation (FBI) replaced the older Integrated Automated Fingerprint Identification System (IAFIS) with the New Generation Identification (NGI) in 2014. NGI supports both facial recognition and rapid DNA analysis in addition to the fingerprint and palm print recognition that the old system supported [11].

A team of researchers has developed a system called FaceSketchID. The system has been developed to be able to match suspect sketches with mugshot images in a database [12], [13]. This allows for quicker identification of criminals that were previously convicted. Australia also has a system that provides the police with fingerprint data. The system is called National Automated Fingerprint Identification System (NAFIS) [14]. This system is earmarked to the replaced by another system that provides more biometric support.

Another system used by the Police in the USA is the AlaCOP portal. The portal is a state-wide umbrella application used in the state of Alabama by a group of applications running within the state [15]. The system uses a system called ADAPT to provide a single sign on for any registered officer within the state.

It is clear from some of the systems above how beneficial they are in fighting crime both collectively with other countries and also within each country's border. The second thing that stands out is that all of the above systems have been developed and deployed in the developed countries. We will now look at some systems that have been developed within Africa in similar conditions to those of Zambia – the area of study.

The first system we look at was developed at the Makerere University of Uganda under the ARMS project. The system is called the Uganda Police Force Crime Records management System (PFCR). The main purpose of this system is to improve the efficiency of crime records within the Ugandan police. Before it was implemented, there was limited capacity for tracking cases, no crime intelligence, possibilities of evidence tampering and no way of carrying out retrospective reporting. The various parts of the systems that are currently supported are the traffic department, crime intelligence and investigations and the minor contraventions unit [16].

The second system we examine was also developed in Uganda. The name of the system is the Traffic Case management System (TCRIS) [17]. As implied by the name, TCRIS focuses on the management of traffic related documents. Its main purpose is to automate the processes that have previously been handled predominantly using paper based mechanisms. The system is designed to have a centralized database that can be accessed by the Migrations department, Bank of Uganda and Uganda Revenue Authority. Technically, the system is developed using a Visual Basic front end application and a SQL Server 2005 database backend.

In Namibia, a group of researchers developed a system to help the police with automation of the paper processes. In addition to crime management and reporting, the system is also able to support crime mapping through GIS. The application supports mobile devices [18].

Having explored some of the existing similar system, we will dive into the proposed system. The remainder of this paper will highlight some business processes for the Zambia Police Service. Based on these processes, a prototype will be presented showing how security has been included in the system.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 12, December 2015

III. METHODOLOGY

A. *BASELINE STUDY*

The first component of this study was carried out using qualitative and quantitative methodologies. Some questionnaires were distributed to gather specific information from police stations. Additional information was collected using oral interviews carried out one on one with some police officers selected by their role.

The study was conducted in Zambia. The country is landlocked and shares a border with eight other countries. With an area of 752, 612 km2 [19] and a population of about 15.5million people [20]; the country has ten provinces, two of which are highly urbanized. This study was conducted in Lusaka, the capital city of Zambia. The population density of the city is 100 people per square kilometer and has a population of about 2.8million people [20].There are over twenty police stations in Lusaka. For the purpose of this study, eight police stations were chosen based on their size and location. Half of the stations were big and the other half was relatively small police posts. The rationale behind this was to capture business processes from police stations of different sizes in order to come up with a solution that optimizes the processes for both scenarios. After the data was collected, it was analyzed using Microsoft Excel.

B. *SOFTWARE DEVELOPMENT*

The method of choice for the development process was Agile Software Development Life Cycle (ASDLC). This was because of the constant interaction with the would-be users during the course of development. This certainly helped with getting feedback from the point person that we worked with thereby helping to improve the application further through the constant iterations.

C. *BUSINESS PROCESS MAPPING*

The prototype is designed to run as a three tier application comprising the user interface, the business logic and the database layers. The business processes are built into the business layer of the application.

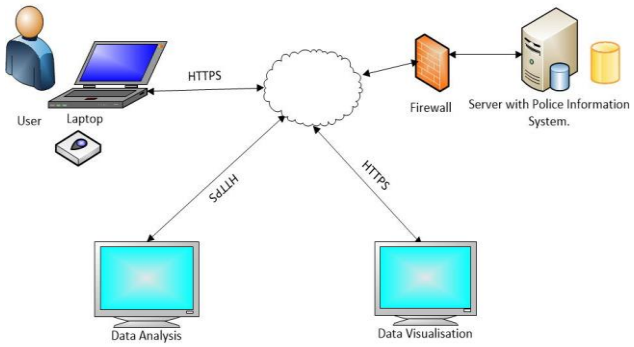

Figure 1: Context Architectural Diagram of the Proposed System

Fig. 1 above shows the context architectural diagram of the proposed prototype. The system is generally accessed via a network through the browser. In order for a user to be able to scan fingerprints, they must have a scanner connected to their device. The prototype has been tested with the DigitalPersonaU4500 running of Windows 7, 8 or 10.

In order to ensure secure access to the system, the prototype uses Secure Sockets Layer communication between the clients and the server in order to ensure encryption of the transmitted data and hence improve on privacy or confidentiality. The communication will use digital certificates for authenticating communication between the server and the clients. The management of the certificates will be handled by a Trusted Third Party. In addition to this, the proposed server implementation involves including a dedicated Firewall server to filter all data coming through to the system server.

We will now look at some of the functionality that the prototype will provide but before that, we identify the main actors. These are the Enquiries Officer, Records Officer, Criminal Investigation Detective, and the Criminal Investigation Officer. These are the individuals that will interact with the system directly.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 12, December 2015

Enquiries Officer: The Enquiries Officer (EO) sits at the enquiries point of the police station. One of the main roles of the enquiries officer is to enter complaints that are reported by the people coming to the police. A police statement is usually collected and kept for future reference. This step is crucial to the steps that follow in the investigations process of the case.

Records officer: The Records Officer (RO) sits in the registry section of the Police station. Among the responsibilities of the RO are to enter new cases into the registry. A paper form is typically filled out specifying the case details. The RO is also responsible for creating the Case Registry Number (CRN) which is generated from the register. In addition, the RO is responsible for creating the case docket to officially open a case.

*Criminal Investigation Detective:*The Criminal Investigation Detective (CID) is responsible for the assignment of cases to the Criminal Investigations Officer (CIO). A case is assigned to the appropriate CIO based on the number of cases they are currently handling. The case is worked on after the assignment process is completed.

Criminal Investigations Officer: The Criminal Investigations Officer (CIO) is responsible for the creation of the "warn and caution" statement that is issued to the person who has been reported in that specific case. After the "warn and caution" statement, the CIO officially charges the suspect with the appropriate charge based on the nature of what was reported. In addition to this, the CIO is also responsible for issuing the Police Bond to the suspect if the crime in question is eligible for one. Finally, the CIO is responsible for managing the criminal docket that contains all the details about the case from the time the Records Officer creates it. This means he will update it until the point when the docket is closed.

With regards to the security implementation, all users will be required to provide their identity before they can access the system by way of login. Once they login, they will only have access to a certain part of the system. The prototype implements Role-Based Access Control security hence only what a user is allowed to access will be visible to them.

We will now look at some of the business processes that depict the workflow in the criminal investigation assignment process as currently performed by the four identified actors.

The first process is the general criminal investigation process. The process begins with the Enquiries Officer as he enters a new complaint and takes a statement of the witness from the complainant. Thereafter, the Enquiries Officer requests the CID for permission to have the case investigated. If the CID grants this request, the Records Officer creates a new case and generates a CRN for the case. If the request is not granted, the case is not opened for investigation. He then further adds complainant's details to the docket that is opened and then returns the docket to the CID. At this point, the CID assigns the case to a CIO at which point the investigation is initiated. If there is enough evidence to make a case, the suspect is charged otherwise the charges are dropped. If the suspect is charged and the suspect is eligible for bail, a police bond is issued to the suspect.

The next process we look at is the medical examination of rape and defilement case. The business process is similar to the generalized criminal investigations process flow. Up until the assignment of the criminal case, the processes remain the same. When the case has been assigned to a CIO, a request is made for a medical examination to be carried out by a medical doctor. The paper form that is filled out at this point is the Report of Medical Examination of Rape/Defilement that is completed in triplicate. Once the medical examination has been performed, the report is added to the case docket. Based on the outcome of the medical examination, the CIO will either charge the suspect or drop the case from being investigated. Just like in the previous business case, a police bond request will be considered based on whether the user qualifies and more importantly the position of the laws of Zambia on the crime in question.

We will now look at the brought in dead business process. The process begins with the Records Officer by filling out the Brought in Dead Certificate. The certificate is supposed to contain remarks from a doctor that declared the individual dead as a legal requirement. The certificate contains bio-information about the dead individual as well as the probable cause of the death. The cause of death is classified as either a natural death or a sudden death.

The next form that is filled out by the Records Officer is the Transfer of Dead Body for Burial form. The form contains details about the informant of the death as well as details of the cause of death. The form also contains information about the person that handled and declared the body of the deceased individual free from contagious diseases. The Officer in Charge is required to sign and stamp this form. After this, the Informant signs on the form to complete the entire workflow.

The next business process is for a general affidavit.The process begins with a request from a citizen for a general affidavit. An affidavit is a sworn statement that is signed by the user in order to back some important pieces of

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 12, December 2015

information they declare to be factual. For instance, an affidavit may be used during the presentation of evidence in the court of law. Although affidavits come in different flavors, the specific type of affidavit covered in this research is the general affidavit.

After the citizen requests for an affidavit, the form is presented to him or her on behalf of the Commissioner of Oaths to fill out. Once the form is filled out, the form is signed and stamped. The form contains the full names, residential address and the postal address of the individual requesting for the affidavit. In addition, the form also contains information regarding the reasons for swearing and an oath and affirmation statement from the requesting party.

We will now discuss the design of the prototype based on the use cases and process flows outlined above. In this section, we will discuss the overall system composition.

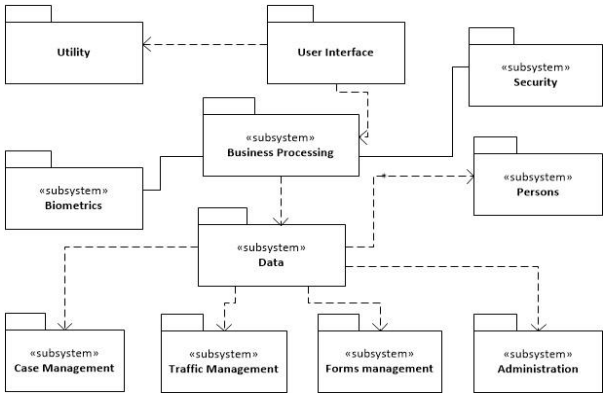

Figure 2: Prototype Architecture

Fig. 2 above shows the architectural diagram for the prototype. Some subsystems have been left out of the diagram as they are earmarked for future implementations. These include the forensics unit and the dispatch units. The user interface (UI) package represents the visible part of the application that the user is able to interact with. The UI is connected to the business processing subsystem and the utility package. The business processing subsystem handles the processing of the requests and ensures that the application conforms to the workflow of the Zambia Police Service. The Utility package provides some functions that aid in various tasks that are required on a regular basis such as system logging.

The biometrics subsystem handles the capture of fingerprint biometrics from the prototype. An example of when this subsystem is used is during the capture of criminal suspect fingerprints and during a civil job application background clearance process. The data subsystem handles the saving, retrieval and update of data for various parts of the application. The main subsystems that require data to be persisted include the forms, case and traffic management. The administration subsystem is responsible for managing the system as a whole.

The security subsystem is responsible for the management of the security related functionality of the system. Once a user is assigned a role, the user will only have access to a limited view of the application. Every role is associated with a specific set of permissions.

IV. RESULTS

A. *BASELINE STUDY*

The survey aimed to determine if an electronic system can be used in the current settings of the Zambia Police Service. Therefore, it was vital to assess the levels of ICT skills within the police workforce. Secondly, the prototype aims to aid in alleviating some security flaws within the current paper intensive workflows and hence one aspect of the survey focused on security mechanisms within the police service.

The resultsfor the access and availability of development opportunities and infrastructure respectively for the police officers shows that 24% of the respondents had formal basic computer training. 7% of the respondents had received cyber security training and 5% have access to staff development opportunities.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 12, December 2015

According to the survey, 71% of the respondents do not have a work designated email address. The results also showed that 39% of the users use their personal emails for work communications. This is a security concern when we begin to examine how sensitive the information in question is.

The results showed that 36% of the respondents use their personal devices for storing work related documents. This is with the background that 58% of the respondents say they do not have a network administrator to help configure security on these devices and 17% not being aware about the presence of a network administrator.

The study also looked into modes of sharing documents within the police. Results showed that 81% of the respondents share their documents physically, 7% use their email for sending documents, 5% use social media and 12% use a central shared directory on a network.

In this study, we also looked at the mechanisms that are currently in place to help with access to documents within the police. Due to the high rate of sharing documents physically, the physical security mechanisms are equally high at 55%. The usage of electronic media is evident despite the low numbers.

B. *Prototype Development*

The prototype has been developed using the business processes described in chapter III. The application uses MySQL for the backend and Java Server Pages for the frontend. Bootstrap has also been used in the frontend for a better look and feel of the application. After a user has logged in, they are presented with a menu from which they can choose specific tasks they wish to perform. The menu comprises of the Form, Case and Traffic management. It also has the Forensics, Dispatch, Reports and Administration menus.

Form management is the menu under which various paper forms have been placed for easy electronic access. All the forms related to the business processes identified above have been included under this menu. Case management menu has all the recording relating to maintaining criminal case records. Traffic management helps to manage traffic offense records. The administration menu is used for general management of the system.

We will look at some of the aspects of the system that have already been implemented. The form management screen has been implemented. From that screen, a user can enter a document from a list of existing forms. We will now look at some of these forms. The forms that are part of the prototype are the criminal form, civic application clearance form, statement, disposal of exhibit, police bond or recognizance, medical examination for rape/defilement, general affidavit, brought in dead and transfer of dead body for burial forms.

V. Discussion and Conclusion

The main aims of this study was to determine the business processes for the Zambia Police Service, assess the current security risks and implement a prototype to support the police in automating their processes in a secure manner.

In order for the workforce to effectively migrate to an electronic system, more work will have to be done in terms of training. From the results, only 24% of the respondents have received formal computer training. This might not be the best metric for measuring computer literacy however because some people may be computer literate but yet have not received any formal training. The access to development opportunities came at 5%. There is need for more government will to help police officers improve on their skills especially with the Zambian government's move towards e-Governance.

Lastly, there is a major security risk regarding the usage of personal emails and devices for work related communications and document storage respectively. Proper measures will need to be put in place in order to ensure confidentiality and integrity of the information that is shared so as to enjoy the resulting benefits of non-repudiation, data integrity and privacy.

Some of the obvious missing policies within the stations that were surveyed are the network policy, Bring Your Own Device (BYOD) policy and email policy. The national ICT policy provides a guide to managing ICT within the government institutions and the next steps will be for the Police to bring the policy home and customize it for the employees. In addition to that, there will be need for sensitizing the police officers about what their role will be.

Finally, a prototype was developed that implements the business processes covered in this paper. Security has been integrated into this prototype right from the design to the point of programming in order to assure secure process flows within the Zambia Police Service.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 12, December 2015

Although the work is this research is target at a Police station in the third world countries, many other institutions can benefit from this work. Sectors such as health and finance require utmost confidentiality of data and similar security mechanisms can be adapted in these sectors. We would like to recommend that the Zambian government build more capacity in the Police workforce and also enforce the National ICT policy at all levels.

VI. ACKNOWLEDGEMENT

The authors would like to thank the Zambia Police Service for allowing them to carry out this research.

REFERENCES

[1] Abubakar, A. & Tasmin, R., The impact of information and communication technology on banks' performance and customer service delivery in the banking industry. International Journal of Latest Trends Fin. Eco. Sc, Vol.2, no.1, pp.80–90, 2012.
[2] Rwashana, A.S. & Williams, D.W., Enhancing healthcare delivery through ICTs: A case study of the Ugandan immunization system. International Journal of Education and Development using Information and Communication Technology (IJEDICT), Vol.4, no.2, pp.144–158, 2008.
[3] Gülbahar, Y., ICT usage in higher education: A case study on preservice teachers and instructors. Turkish Online Journal of Educational Technology, Vol.7, no.1, pp.32–37, 2008.
[4] Julian, J.; Surya, N., " A survey of emerging threats in cybersecurity", Journal of Computer and System Sciences, vol.80, pp.973-993, 2014.
[5] Security Principle. "Security Principle", http://www.dwheeler.com/. [Online]. Available: http://www.dwheeler.com/secure-programs/Secure-Programs-HOWTO/security-principles.html [Accessed: Dec. 05, 2015].
[6] Nancylia, M.; Mudjtabar, E.K.; Sutikno, S.; Rosmansyah, Y., "The measurement design of information security management system," in Telecommunication Systems Services and Applications (TSSA), 2014 8th International Conference on, pp.1-5, 23-24 Oct. 2014.
[7] Rad, H.A.; Samsudin, K.; Ramli, A.R.B.; Tehrani, M.B.; Tavalai, M.A., "A Secure Protocol for Traffic Police Mobile Communication System," in Future Computer and Communication, 2009. ICFCC 2009. International Conference on , pp.533-539, 3-5 April 2009.
[8] Nath Nayak, G.; Samaddar, S.G., "Different flavours of Man-In-The-Middle attack, consequences and feasible solutions," in Computer Science and Information Technology (ICCSIT), 2010 3rd IEEE International Conference on , vol.5, pp.491-495, 9-11 July 2010.
[9] Global moves to extend the scope of national biometric identification systems, Biometric Technology Today, Volume 2013, Issue 1, 2013.
[10] Canadian police get real-time fingerprint and palm ID system, Biometric Technology Today, Volume 2011, Issue 6, pp.12, 2011.
[11] FBI NGI goes live with new biometric capabilities, Biometric Technology Today, Vol.2014, no.10, pp.1-2, 2014.
[12] Police forces across the globe implement biometric tech, Biometric Technology Today, Vol.2015, no. 1. Pp.1, 2015.
[13] Klum, S.J.; Hu Han; Klare, B.F.; Jain, A.K., "The FaceSketchID System: Matching Facial Composites to Mugshots," in Information Forensics and Security, IEEE Transactions on , vol.9, no.12, pp.2248-2263, Dec. 2014.
[14] Police forces extend use of biometrics across the globe, Biometric Technology Today, Vol.2014, no.9, pp.3, September 2014.
[15] Matthew, H.; Maury M.; Allen, P., "Access Control for a Federated Police Information System" in SACMAT '11 Proceedings of the 16th ACM symposium on Access control models and technologies , pp.149-150, June. 2011.
[16] Muyanja, A. et al., Requirements engineering for the Uganda police force crime records management system. 2013 21st IEEE International Requirements Engineering Conference, RE 2013 - Proceedings, pp.302–307, 2013.
[17] Mubaraka, C.M., Jirgi, I.M. & Nanyanzi, P.L.B., Integrating ICT in Traffic Police Department in Uganda : Design and Development of Traffic Case Management System (TCRIS). , Vol.4, no.5, pp.17–27, 2013.
[18] Kasper, L.J.; Hedvig N.K.I.; Michel, U.O.; Sebastian, M,, "Toward an mPolicing solution for Namibia: leveraging emerging mobile platforms and crime mapping" in SAICSIT '12 Proceedings of the South African Institute for Computer Scientists and Information Technologists Conference , pp.196-205, Oct. 2012.
[19] Zambia - Demographic and Health Survey 2013-2014. "Zambia Demographic and Health Survey 2013-14 Report", http://microdata.worldbank.org/index.php/catalog/2246. [Online]. Available: http://www.dhsprogram.com/pubs/pdf/FR304/FR304.pdf [Accessed: Dec. 04, 2015].
[20] Zambia Demographics at a Glance. "Zambia demographics at a glance", http://zambia.opendataforafrica.org. [Online]. Available: http://zambia.opendataforafrica.org/efhbnl/zambia-demographics-at-a-glance [Accessed: Dec. 05, 2015].