Journal of Computer Science

Original Research Paper

A Secure Model for Storage and Dissemination of Examination Results: A Case Study of Zambia Technical Education Vocational and Entrepreneurship Training Authority

[1]Lister Mseteka and [2]Jackson Phiri

[1]School of Engineering, Department of Electrical and Electronic Engineering, University of Zambia, Lusaka, Zambia
[2]School of Natural Sciences, Department of Computer Science, University of Zambia, Lusaka, Zambia

Article history
Received: 23-10-2018
Revised: 04-01-2019
Accepted: 31-01-2019

Corresponding Author:
Lister Mseteka
School of Engineering,
Department of Electrical and Electronic Engineering,
University of Zambia, Lusaka,
Zambia
Email: lismseteka@gmail.com

Abstract: Most developing countries and public higher institutions of learning have low levels of Information and Communication Technology (ICT) and hence face challenges in securing information and information systems. Therefore, dissemination of examination results through web and mobile applications usually raise security concerns on how to ensure the confidentiality, integrity and authenticity of students' examination results due to susceptibility of web and mobile applications. In this study, we are proposing a secure model for storage and dissemination of students' examination results using encryption and cryptographic hash functions to simultaneously provide confidentiality, integrity and authenticity assurances of students' examination results. The study is based on Technical Education, Vocational and Entrepreneurship Training Authority (TEVETA), an examination body in Zambia. A baseline study was conducted to determine the challenges faced by TEVETA and students regarding dissemination of students' examination results. Data was collected from 558 respondents consisting of 514 students, 36 members of staff in-charge of examinations in TEVETA registered institutions and 8 TEVETA ICT staff. The results from the study indicate that the current TEVETA examination cycle business processes have a number of irregularities. These include candidate registration, storage of students' examination results and dissemination of students' examination results. The results from the baseline study were used to come up with the model which was then used to develop a prototype. The results obtained from the test and evaluation of the developed prototype based on the model shows that the system provides an avenue to ensure the confidentiality of students' results through encryption as well of integrity and authenticity of students' examination results through detection of altered students' examination results during transmission and storage through cryptographic hash function.

Keywords: Authenticated Encryption, Integrity, Hash Function, Web, Dissemination System

Introduction

The trend of educational institutions offering services such as dissemination of examination results through web and mobile applications has raised security concerns on how to ensure the confidentiality, integrity and authenticity of students' examination results due to susceptibility of web and mobile applications to cyber attacks (Rico *et al*., 2011; Nfuka *et al*., 2014; Stufford and Pionto, 2011; Mshangi *et al*., 2016). In this study, we have designed a model for improved security levels of students' examination results during transmission and storage through the use of encryption and cryptographic hash function to provide information

security objectives of confidentiality, integrity and authenticity assurances on students' examination results. Integrating encryption and cryptographic hash function ensure not only confidentiality, but also integrity and authenticity of data (Martin, 2012).

The research objectives that constituted this study are:

(i) To conduct a baseline study to establish the challenges faced by TEVETA and students regarding dissemination of students' examination results
(ii) To design a model based on TEVETA business processes and ISO 27001 information security standard
(iii) To develop a secure web and mobile prototype for storage and dissemination of students' examination results based on the model in (ii)

Background

Educational institutions are expected to manage and preserve students' academic data. This data includes general information as well as examination results which must be properly calculated, preserved and released on time. However, educational institutions of higher learning with many students face challenges in handling and releasing examination results leading to high cost and delay accessibility by students (Fue *et al*., 2014). Several researches have since been conducted to disseminate results through web and mobile applications. However, mobile and web applications are susceptible to cyber attacks (Rico *et al*., 2011; Nfuka *et al*., 2014; Stufford and Pionto, 2011; Mshangi *et al*., 2016; Mshangi *et al*., 2015). This study will aim at designing and implementing a web and mobile based examination results dissemination system using encryption and cryptographic hash function for secure storage and dissemination of students' examination results.

Related Works

Institutions of higher learning retain sensitive data making them highly attractive targets for cybercrime (Verizon, 2017). Security risks on information systems in higher learning institutions are not theoretical, as some incidents have revealed; ranging from theft of information, unauthorised disclosure, unauthorised alteration of information, corruption of data or damage to networks (Verizon, 2017; Okibo and Ochibe, 2014; Ndolo *et al*., 2018; Juma, 2011; Capital Campus, 2015; Mugyenyi, 2017; BBC, 2018; Perlroth, 2012). In Kenya, a catholic university of Eastern Africa system was hacked by some students and this resulted into alteration of grades, registration for courses not yet covered and grading them, clearance/alteration of their financial balances (Okibo and Ochibe, 2014). In 2011, a report was circulated by the Permanent Secretary, Ministry of Higher Education, Science and Technology to all Vice Chancellors of Jomo Kenyatta University of Agriculture and Technology, the Catholic University of Eastern Africa, Daystar University and Maseno University about a group of university students that compromised academic and financial systems' integrity by altering grades and fee balances (Ndolo *et al*., 2018). In another incident, employees and students of Kenyatta University hacked into the university's database and altered examination results (Juma, 2011). According to the Cyberoams's report released during the education Cyber Security Symposium, Kenyan students are fourth in Africa after Egypt, Morocco and South Africa in terms of hacking school systems to manipulate grades and fees (Capital Campus, 2015). In Uganda, a number of incidences occurred at Makerere University due to poor information systems security resulting to a number of ghost students appearing on graduation list and leaving out genuine students who had successfully graduated (Mugyenyi, 2017). In 2018, the University of Greenwich in the United Kingdom was fined £120,000 ($160,000) by the Information Commissioner as fine for a security breach in which 19,500 students' records were placed online (BBC, 2018). The data included names, addresses, dates of birth, phone numbers, signatures and - in some – cases – physical and mental health problems. Perlroth (2012) highlighted that 53 universities, including Harvard, Stanford, Cornell Princeton, Johns Hopkins, the University of Zurich and other universities around the world were hacked and 36,000 email addresses and thousands of names, usernames, passwords, addresses and phone numbers of students, faculty and staff were published to the web site Pastebin.com. A cyber security survey in 2017 by Verizon reveals that there were 455 cyber security incidents in the educational sector and that 73 of them resulted in data breaches (Verizon, 2017).

A number of studies related to improving the security of students' examination results exist. The study by (Zabangwa, 2013) designed and implemented a system to enable easy and convenient access to examination results for Examinations Council of Zambia (ECZ) as soon as they are available using a mobile phone. The security of the system is on administrative and user access to the database. Adagunodo *et al*. (2009), designed and implemented a system 'SMS User Interface and Result Checking System' that enables students to request for university examination results using a mobile phone. The system sends a Short Message Service (SMS) along with the password to a designated number. Muhamadi *et al*. (2009), proposed a system architecture 'Auto Notification Service for the Student Record Retrieval System Using Short Message

Service (SMS)' that automatically sends an SMS to each student once a Lecturer submits a mark to their records. The main emphasis on security is on administrative and user access to the database. Solomom and Phiri (2017), proposed an SMS/USSD mobile application using mobile cloud technologies to enhance candidate registration for examinations and dissemination of examination results for Malawi National Examinations Board. The main emphasis on security is on administrative and user access to the database but students' marks are stored in plain text. Mshangi *et al*. (2015), presented the design and implementation of a 'Results Alert System through Email and SMS' that conveniently sends examination results to students with the use of SMS and Email technologies via their mobile phones. Their work majored on security measures such as administrative and user access to the database. Mshangi *et al*. (2016), proposed a secure architecture of Web and Mobile-Based information system for dissemination of students' examination results using a soft science design science methodology in Systems development Life Cycle (SDLC) that embraces secure coding practices, security awareness training and education. However, encryption of communication channel proposed by (Mshangi *et al*., 2016) only provides confidentiality of examinations results during transmission but results are stored in plain text in the database. Milumbe *et al*. (2017), developed a web based candidate registration system based on the cloud model. Their work majored on improving efficiency and reducing the cycle time in the candidate registration process for examinations. Chavan *et al*. (2016), proposed an innovative method of authenticating digital mark sheets of students' results using Quick Response (QR) code. The findings of the research are that QR codes save a lot digital space and also provide an innovative way to authenticate digital documents. However, no security was enforced on the digital records of students' results which means results can still be modified or viewed by unauthorised personnel. Ise (2015), designed and implemented a student result computation application as a cloud computing service. The findings are that Universities can use a student result computation application as a cloud service to eliminate high cost of acquisition, infrastructure, licenses, support and maintenance. Computed examination result data are encrypted during transmission and before storage in the database. However, the system has no mechanism to check the validity of encrypted data in case of cipher text attacks. Onuiri *et al*. (2015) designed and implemented a biometric student management system that enable prompt checking of grades, track progress and efficiently record each student's attendance through a biometric device. The findings revealed that the system provides lecturers with an efficient means of calculating students' grade scores and recording attendance. The security of the system is on administrative and user access to the system but student academic records such as examination results are stored in plain text without encryption.

Materials and Methods

The purpose of this study was to establish the challenges faced by TEVETA and students regarding dissemination of students' examination results and then develop a model based on current TEVETA business processes and ISO 27001 information security standard for access control. Further, a mobile and web prototype for dissemination of students' examination results using Advanced Encryption Standard (AES) encryption algorithm and SHA3-224 cryptographic hash function based on the model was developed.

Baseline Study

The purpose of the baseline study was to establish the challenges faced by TEVETA and students regarding dissemination of examination results. To address this objective, mixed methods research methodology was used. For quantitative data, questionnaires were administered to a total of 558 respondents consisting of 514 students, 36 members of staff in charge of candidate registration for examinations from 12 TEVETA registered institutions and 8 TEVETA ICT staff. For qualitative data, interviews with selected ICT staff were conducted. Purposive sampling was used to facilitate inclusion of the best candidates for the study based on the objectives of the study. TEVETA registered institutions were purposively sampled. The results from our baseline study indicate that the current TEVETA business processes for candidate registration and dissemination of examination results have a number of irregularities that consequently lead to delay in the release of students' examination results. Further, an ICT staff at TEVETA said that students' examination results are stored in plain text in the database without encryption. The storage of students' examination results without encryption gives room for possibility of unauthorised disclosure, results alteration and identity theft.

System Automation

The results from the baseline study were used to come up with the model which was then used to develop the prototype.

Requirements Specification

Data from questionnaires and interviews with TEVETA ICT staff provided qualitative data used to come up with requirements and design a model of the system in the study.

System Design

Interviews conducted with some TEVETA ICT staff helped to understand how registration for examinations and dissemination of results are done and design a model for the proposed system. Questionnaires were administered to TEVETA data entry personnel to understand the challenges in candidate registration for examinations and dissemination of examination results.

Data Design

For data design, use case diagrams and entity relationship modelling were used.

Use Case Diagrams

Use case diagrams describe the functionality of the system from the user's perspective. Figure 1 show the use case diagram between the system and external entities.

Entity Relationship Diagram

Entity relationship model describes data as entities, attributes and relationships. Figure 2 shows the entity relationship diagram drawn from requirements through interviews and documents such as student registration and examination entry forms.

Business Process Mapping

The proposed secure model in Fig. 3 is derived from the current business processes for candidate registration, examination results entry, verification, publishing and dissemination of results. Automating the dissemination of students' examination results through the mobile application and web application instead of using hard copies, encryption and hashing of marks or grades during storage and dissemination of students' examination results are the changes proposed.

Encryption of students' marks or grades provides assurance of confidentiality of students' marks or grades and hashing of students' marks or grades provides assurance of integrity and authenticity through detection of altered marks or grades during transmission and storage.

There are two types of encryption algorithms used today; symmetric encryption and asymmetric encryption. Symmetric key algorithms rely on a shared secret key that is distributed to all members who participate in the communication for encryption and decryption of messages. Popular examples of symmetric key cryptosystems are: the Data Encryption Standard (DES), Triple DES (3DES), International Data Encryption Standard (IDEA), Blowfish, Skipjack and the AES.

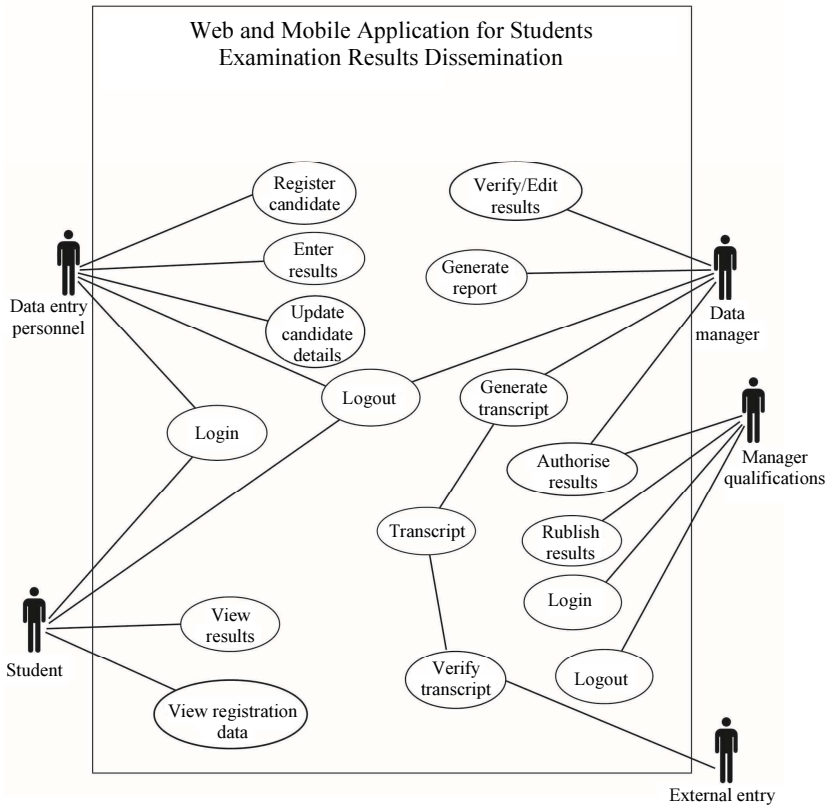

Fig. 1: System use case diagram

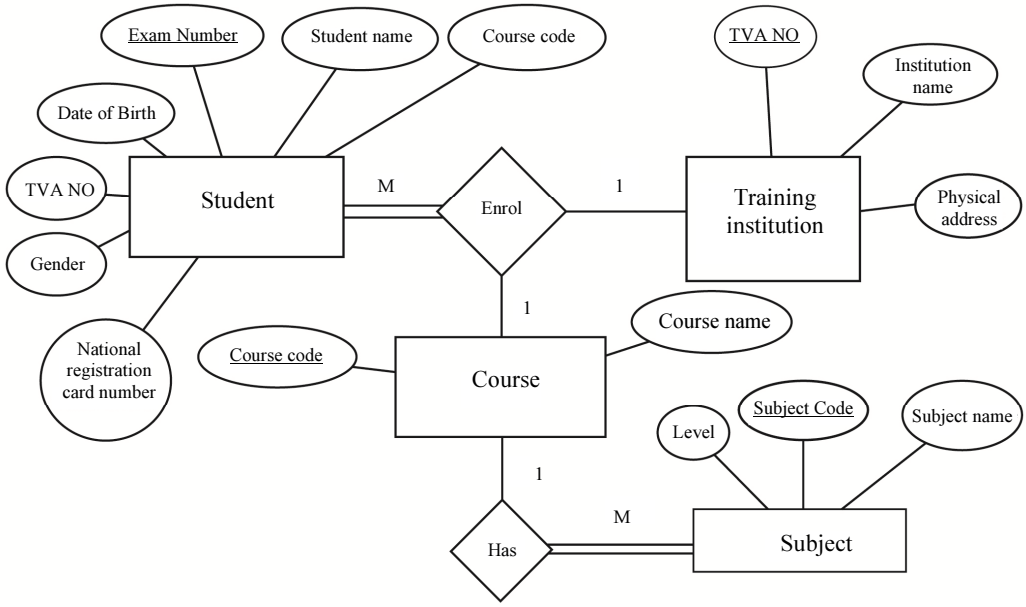

Fig. 2: Entity relationship diagram

Asymmetric algorithms (also called Public-key algorithms) are designed so that the key used for encryption is different from the key used for decryption. The three common public key cryptosystems in use today are: Rivest-Shamir-Adleman (RSA), El Gamal and Elliptic Curve cryptosystem (Martin, 2012).

A study by (Singhal and Singhal, 2016) compared AES and RSA encryption algorithms. The results of the study reveal that encryption and decryption takes more time in RSA algorithm than AES. (Mahajan and Sachdeva, 2013) measured the performance of encryption algorithms; AES, DES and RSA algorithms. Based on the text files and the experimental results, it was established that AES algorithm consumes least encryption and decryption time than RSA. From the simulation results, it was observed that AES is better that DES and RSA algorithm. A performance evaluation of four encryption algorithms: RSA, DES, 3DES and AES based on encryption time, memory usage, output byte, power consumption rate, flexibility and security show that AES consumes least encryption time and has least memory usage (Afolabi and Atanda, 2016). A study by (Hercigonja *et al*., 2016) on symmetric encryption algorithms such as DES, 3DES, CAST-128, AES, RC6 and asymmetric RSA algorithm based on architecture, security and limitations of algorithms reveal that AES is an effective encryption algorithm among all the encryption algorithms. A study by (Mushtaque, 2014), presents the complete analysis of various symmetric key encryption algorithms (DES, 3DES, Blowfish, CAST-128, MARS, IDEA, AES and RC6) based on different parameters such as: architecture, scalability, security, flexibility and limitations. After the comparison, it was established that AES is secure, fast, better and effective encryption algorithm among all the encryption algorithms and has least memory usage, high encryption performance, without any weakness and limitations while other algorithms have some weakness and differences in performance and storage space. (Boxcrptor, 2018) noted that AES is the most widely used and secure encryption algorithm preferred in banks, governments and high security systems around the world.

The major weakness of public key cryptography (asymmetric encryption) is its slow speed operation. Because of this reason, many applications that require secure transmission of large amounts of data use a public key to establish a connection and then exchange a symmetric secret key and encryption and decryption of data is through symmetric encryption algorithm (Vacca, 2009; Stallings, 2014). Therefore, AES algorithm will be used for encryption and decryption of students' marks or grades as it has been established by many researchers as the most secure and efficient algorithm among symmetric algorithms and more efficient than the popular asymmetric encryption algorithm such as RSA.

Cryptographic hash functions provides the assurance of data integrity with notion of imprintingon fingerprint of source data, that any alteration in transit or on the database no longer guarantee the integrity of data (Martin, 2012).

Let h be the hash function and m the mark, then the corresponding fingerprint or message digest is defined as:

$$x = h(m) \quad (1)$$

if x is stored in a secure place, then:

$$y = x \quad (2)$$

If the source data, m is changed in transit or on the database, it becomes *m*', then the corresponding message digest in (1) will change from x to x' as:

$$x' = h(m') \quad (3)$$

If marks are altered in transit or on the database, then by comparing Equation (2) and (3) it can be deduced that:

$$y \neq y' \quad (4)$$

verifying that the integrity of the marks have been compromised.

Common hashing algorithms in use today include Message Digest 5 (MD5) and Secure Hash Algorithm (SHA). However, MD5 algorithm is no longer accepted as a suitable hashing function (CISSP, 2008). Cryptanalytic attacks on SHA-1 algorithm demonstrated weaknesses in SHA-1 algorithm that led to the creation of SHA-2, which has four variants: SHA-224, SHA-256, SHA-384 and SHA-512 (CISSP, 2008). Recent cryptanalytic attacks breaks pre-image resistance for SHA-512 in 57 and 80 rounds and 52 out of 64 rounds for SHA-256 (Khovratovich *et al*., 2011). 256 SHA-256, SHA-512, SHA-224 and SHA-384 are also prone to length extension attacks. SHA-3 is the latest member of the SHA algorithm released by NIST in 2015 (Hernandez, 2018; Dworkin, 2015; NIST, 2015). The SHA-3 family consists of SHA3-224, SHA3-256, SHA3-384 and SHA3-512 and two Extendable-Output Functions (XOFs), called SHAKE128 and SHAKE256. Luo *et al*. (2016) proposed an efficient and powerful method to conquer the SHA-3 family of hash algorithms using Differential Fault Analysis (DFA). The findings from the study show that DFA on SHA3-224 and SHA3-256 are more difficult than on SHA3-384 and SHA3-512, while SHA3-224 is more difficult to conquer than SHA3-256. Therefore, SHA3-224 will be used to hash marks to provide integrity checks before displaying examination results.

Architecture of Secured Model for Examination Results Entry, Storage and Dissemination

The system architecture consists of three sub sections: The registration phase, entering of grades, verification of grades shown in Fig. 3 derived from the current business process.

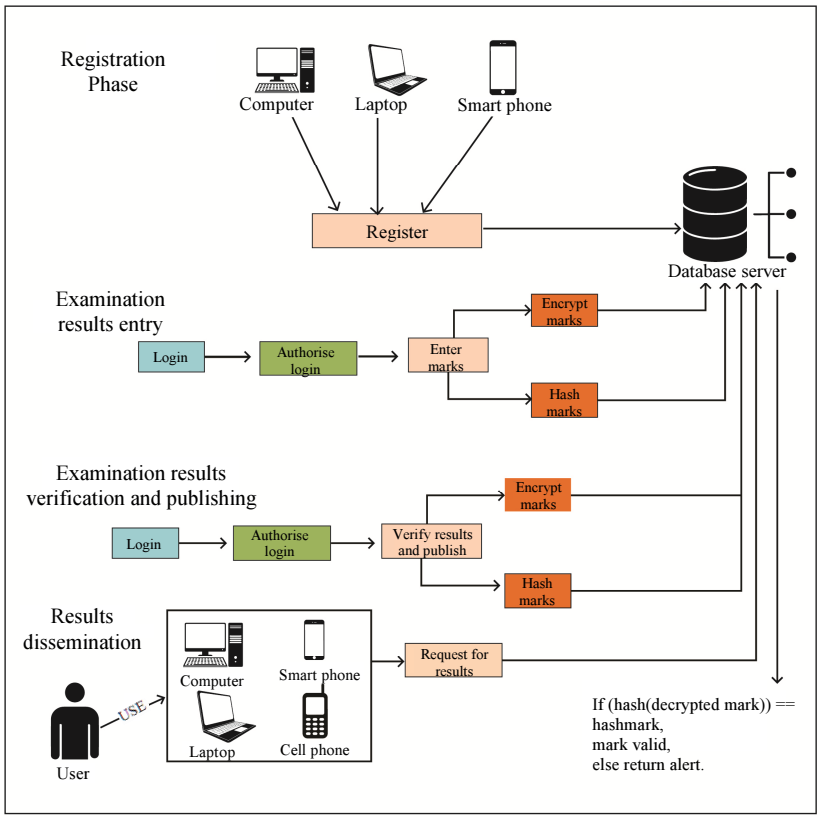

Fig. 3: Secure architecture for insertion, storage and dissemination of examination results

Algorithm for Secure Insertion and Storage of Marks

During examination results entry, plain text marks are encrypted with AES encryption algorithm. Plain text marks are also hashed with SHA3-224 hashing algorithm so that the final encoded mark consists of two parts; an encrypted mark and a hashed mark. Figure 4 shows the secure architecture for insertion of examination marks.

The algorithm for secure insertion of examination results using AES encryption and SHA3-224 works as follows:

start:
mark1 = AES_ENCRYPT(mark, key)
mark2 = sha3-224(mark)
populate table in database (A) and table in database (B) with mark1 and mark2 respectively
stop.

Algorithm for Secure Retrieval of Examination Results

During retrieval of student marks, SHA3-224 is used to check the integrity of each stored encrypted mark in case of alteration in transit or in the database. The process involves decrypting each mark with AES encryption algorithm, then hashing each mark with SHA3-224 hashing algorithm. The hashed mark is compared with the hashed mark originally stored in the database. If the hashes of marks match, the AES algorithm proceed to display the examination results, otherwise it will not display the examination results as it is an indication that marks were altered while in transit or on the database and therefore are not authentic. Figure 5 shows the secure architecture for retrieval of examination results.

During retrieval of results, the SHA3-224 works as follows:

Start:
Retrieve mark 1 and mark 2 from database (A) and database (B) respectively
mark1 -----> (encrypted mark)
mark2 ------> (hashed mark)
mark3 = AES_DECRYPT (mark1, key)
hashedmark = SHA3-224(mark3)
Compare mark2 with hashedmark,
If hashedmark equals mark2
display grades
else return alert.

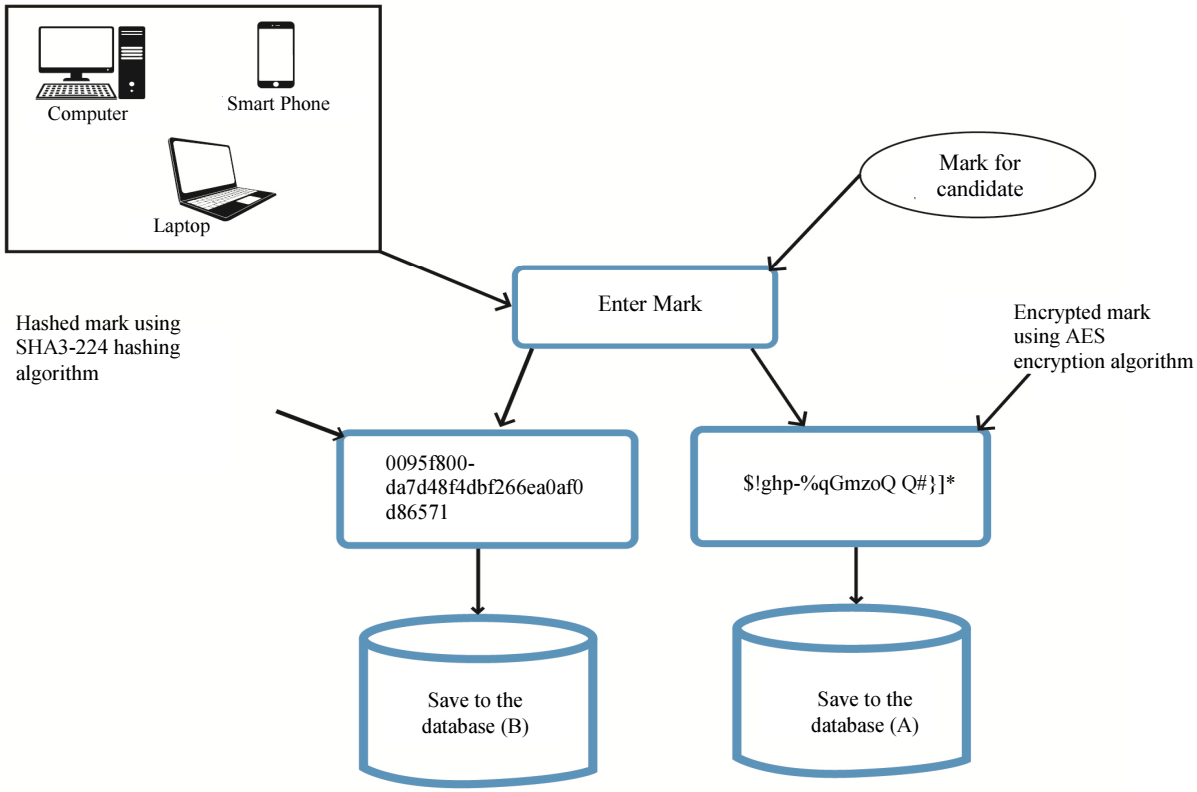

Fig. 4: Architecture for secure insertion of examination results

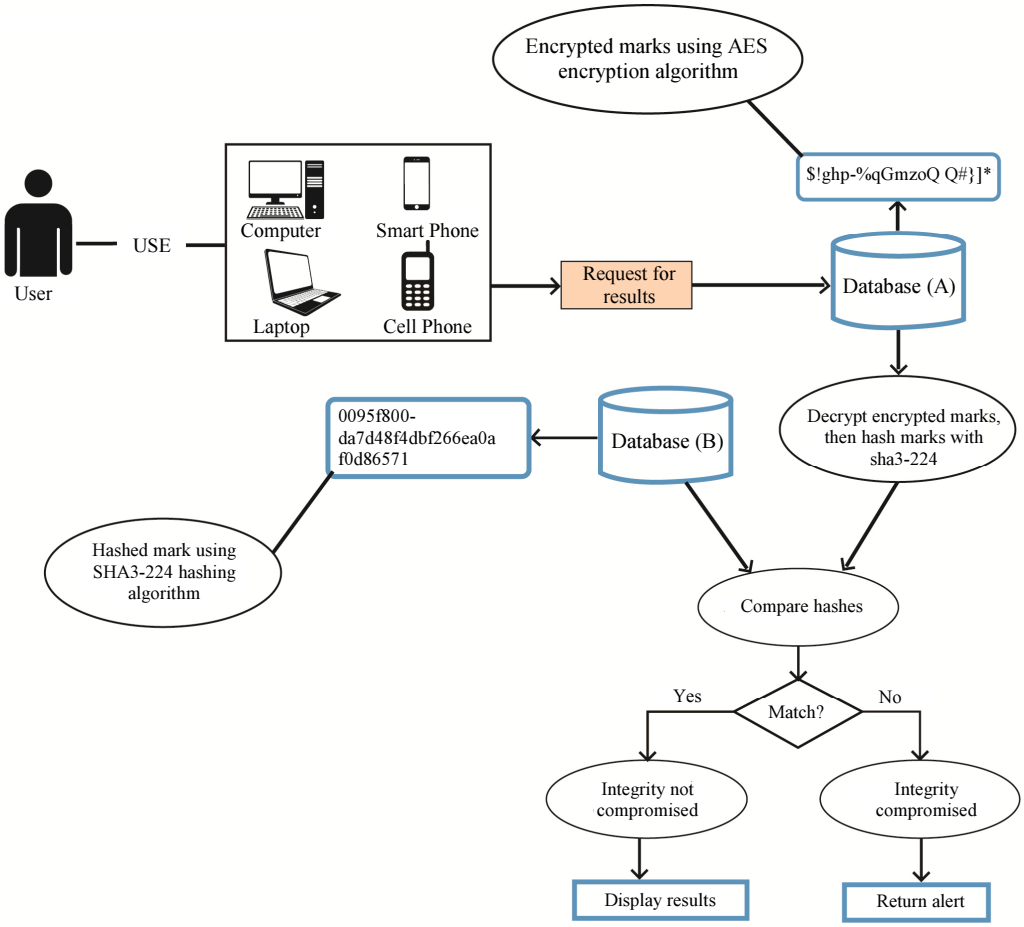

Fig. 5: Architecture for secure retrieval of examination results

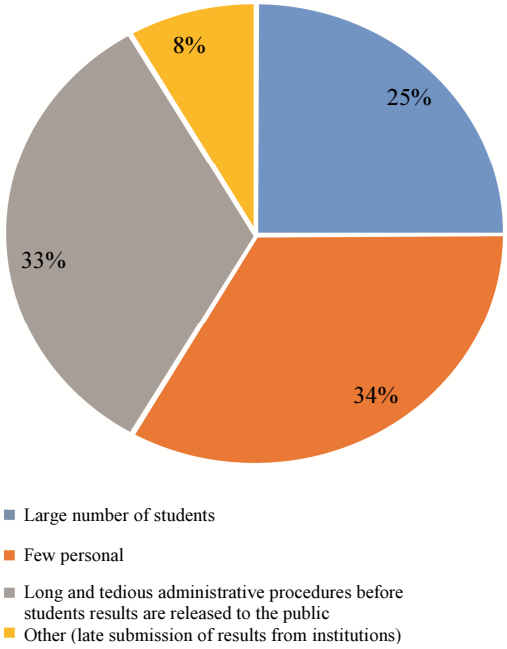

Fig. 6: Examination results release challenges

Findings

The results of the baseline study were analysed and it was found that challenges exist that delay the release of examination results. As indicated in Fig.6, respondents mentioned challenges such as long and tedious administrative procedure before the release of examination results which accounted for 33%, large number of students accounted for 25%, few personnel in data entry accounted for 34%, late submission of continuous assessment results by institutions of study accounted for 8%.

The research findings from TEVETA examined students confirm the delay in the release of examination results. Figure 7 show that results are released after three months which accounted for 48%, 32% of students said results are released after two months while 20% of students said it varies. Having established the challenges, respondents from TEVETA, members of staff and TEVETA examined students from various institutions of study were asked to recommend solutions that would help in reducing or eradicating some of the challenges. They all recommended a mobile and web based application for registration and dissemination of examination results.

When students were asked if a web based application would improve access to examination results. The results in Fig. 8 show that 71% agreed, 3% disagreed while 26% said they were not sure.

Students were asked if they have access to the internet and 82% have access to internet while 18% do not have access to the internet as shown in Fig. 9.

The chart in Fig. 10 show that 76% of TEVETA examined students think that a mobile application would improve access to examination results, 21% said that they are not sure while 3% said a mobile application cannot improve access to results. Furthermore the study revealed that 96% of students have mobile phones while 4% do not have as shown in Fig. 11.

System Implementation

A prototype was developed that allows students and other stakeholder to access students' results through mobile phones and the web. The web component was developed using Hypertext Preprocessor (PHP) and Hypertext Markup Language (HTML). The USSD/SMS mobile application requires a gateway which allows a mobile phone to send or receive requests to and from the mobile service provider. An organisation or individual must subscribe to a mobile service provider in order to use their gateway. However, a USSD/SMS simulator was developed using Java programming language that enables a stakeholder to send requests for both examination enrolment details and examination results using a mobile phone as connecting a mobile application to a gateway was expensive to the researcher.

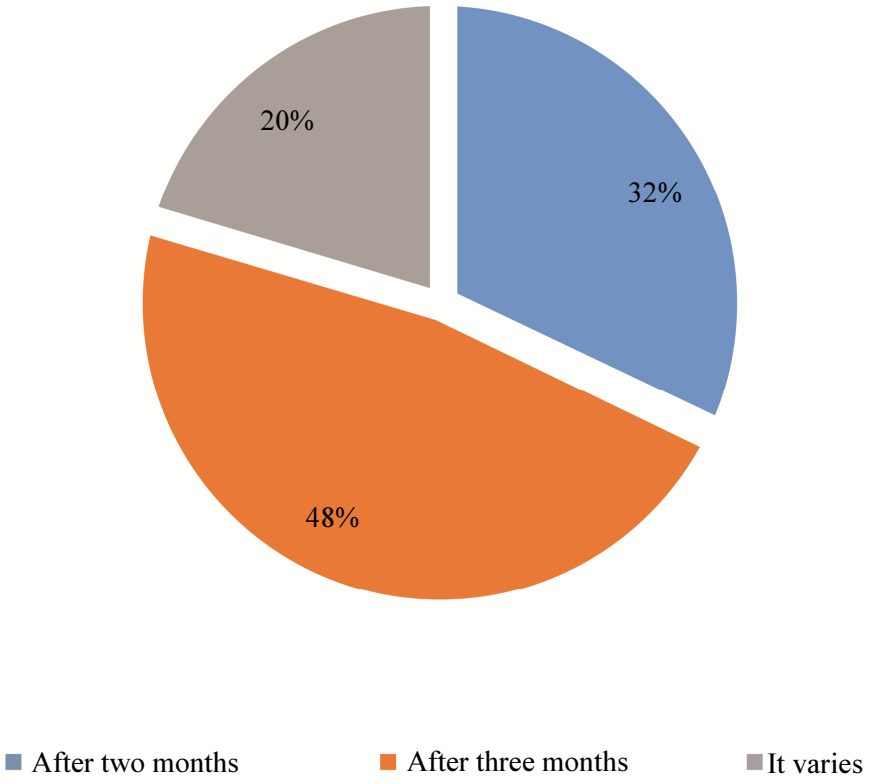

Fig. 7: How long it takes for TEVETA to release examination results

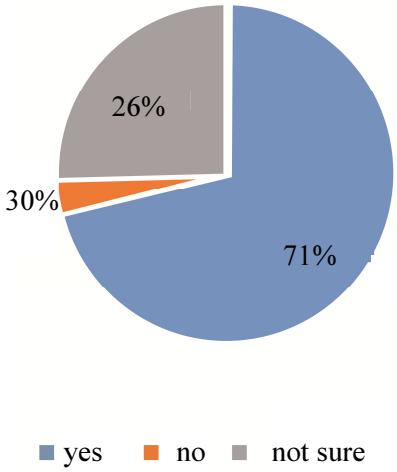

Fig. 8: Whether a web application would improve access to examination results

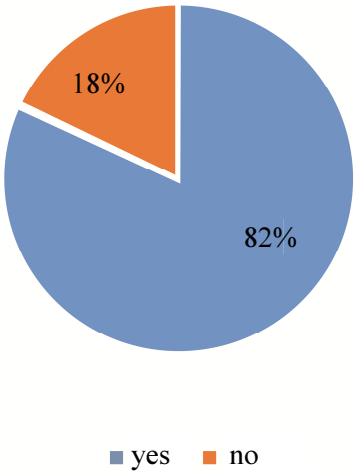

Fig. 9: Student access to internet

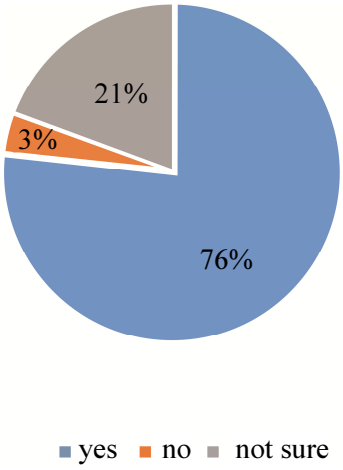

Fig. 10: Whether a mobile application would improve access to examination results

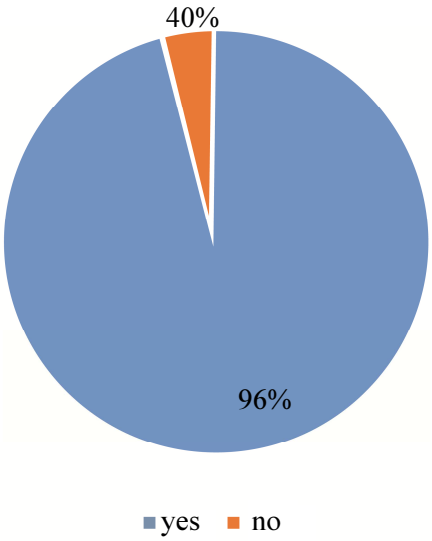

Fig. 11: Students with mobile phones

TEVETA
Technical Education, Vocational and Entrepreneurship Training Authority

Statement of Results

Statement Number	Course Code	Grade	Level	Year
5040	CS1	P	1	2018
5040	CS2	P	1	2018
5040	CS3	C	1	2018
5040	CS4	F	1	2018
5040	CS5	F	1	2018
5040	CS6	F	1	2018
5040	CS7	F	1	2018

Fig. 12: Screen showing results of a student on a web Page

Both applications have used AES encryption algorithm integrated with SHA3-224 cryptographic hash function to provide cyber security objectives of confidentiality, integrity and authenticity assurances on examination results. The developed prototype from our model shows that our system provides secure storage and transmission of examination results. If encrypted marks are not altered after publishing by the Senate or committee in charge of examination results, a student or stakeholder can view results on the web or mobile phone. Figure 12 and 13 shows the web and mobile screen for examination results respectively. However, if results are altered by unauthorised personnel after publishing, the application program will detect and display an alert that results could not be retrieved or accessed. This is because the hashes of the altered marks will be different from the hashes of the marks originally stored in the database, meaning that the integrity of the examination results no longer holds. Figure 14 and 15 shows the web and mobile screen when examination results are illegally altered respectively.

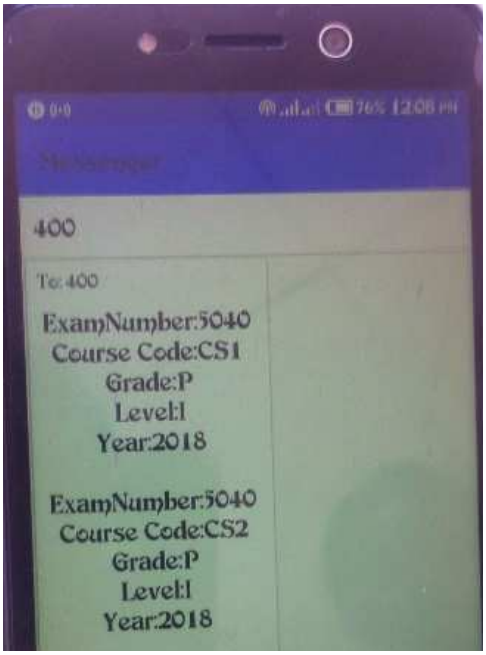

Fig. 13: Screen showing results on a mobile phone

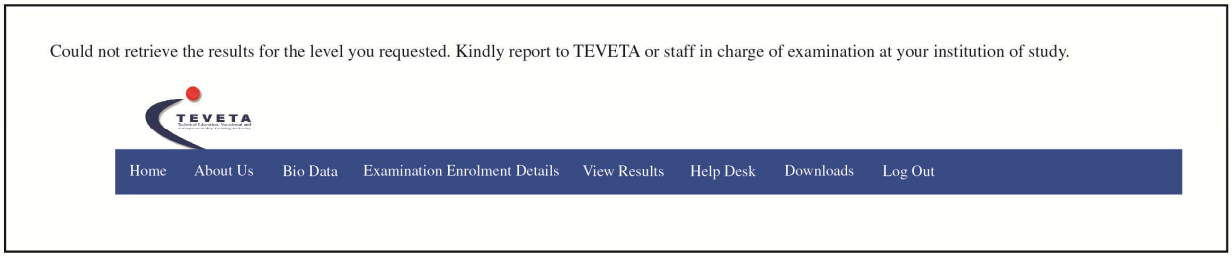

Fig. 14: Web screen displayed when results have been altered

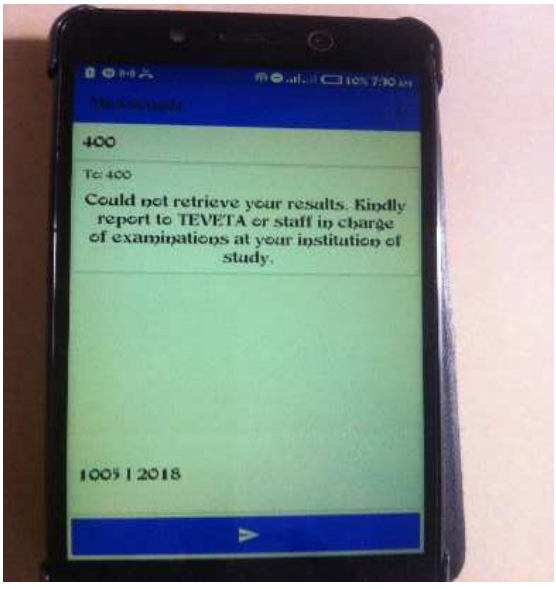

Fig. 15: Mobile screen displayed when results have been altered

Discussion

The study was conducted to establish the challenges faced by TEVETA and students regarding dissemination of examination results. The challenges were established through a baseline study that was undertaken with 8 TEVETA ICT staff, 514 students and 36 members of staff in selected TEVETA registered institutions. The analytical results of the baseline study reveal that the current TEVETA business processes for candidate registration and dissemination of examination results have a number of irregularities. These irregularities include candidate registration, storage of students' examination and dissemination of students' examination results. This paper recommends a mobile and web application to curb delays in the release of students' examination results. Literature reviewed during the study show that similar challenges are also faced in other countries especially in Africa. Literature reviewed also show that cyber attacks on examination results system have occurred ranging from theft of information,

unauthorised disclosure, unauthorised alteration of information and corruption of information. The results from the baseline study were used to develop a model based on current TEVETA business processes and ISO 27001 information security standard for access control. Further, a mobile and web prototype for dissemination of students' examination results based on the model was developed. The web and mobile application for dissemination of students' examination results were developed using PHP and Java programming languages respectively. Both applications used AES encryption algorithm integrated with SHA3-224 cryptographic hash function to provide information security objectives of confidentiality, integrity and authenticity assurances on students' examination results. The developed prototype from our model shows that the system provides confidentiality of results through encryption and secure storage and transmission of students' examination results through detection of altered students' examination results during transmission and storage through cryptographic hash function.

Conclusion

TEVETA should strive to use modern technologies such as web and mobile applications in order to enhance the administration of national examinations more especially management of candidate registration and examination results information. In this study, a baseline study was conducted to establish the challenges faced by TEVETA and students regarding dissemination of examination results. Challenges have been identified and literature reviewed during the study show that similar challenges are also faced in other countries especially in Africa. Literature reviewed also show that cyber attacks on examination results system have occurred compromising the confidentiality, integrity and authenticity of students' examination results. The results from the baseline study and literature reviewed were used to develop a model based on TEVETA business processes for candidate registration, examination results entry, verification, publishing and dissemination of results. A web and mobile prototype utilizing encryption and cryptographic hash function was then developed based on model to provide information security objectives of confidentiality, integrity and encryption respectively. The developed prototype was tested and proved to be more secure because of encryption that provides confidentiality of examination results and hashing which provides a mechanism to detect altered students' examination results during transmission and storage. This paper recommends a mobile and web students' examination results dissemination system using encryption and cryptographic hash functions to provide information security objectives of confidentiality, integrity and authenticity of students' examination results in an examination body but can be generalized to universities or colleges to enhance secure storage and dissemination of examination results.

Acknowledgement

Authors would like to thank staff at TEVETA, students and staff from TEVETA registered for their cooperation and support during the research study, for without them this research would not have been completed.

Author's Contributions

All the authors contributed to the final version of the manuscript.

Ethics

The corresponding author testify on behalf of the co-author that this article is original and has not been published elsewhere, and that ethics were considered for this research.

References

Adagunodo, E.R., O. Awodele and S. Idowu, 2009. SMS user interface result checking system. Issues Informing Science Technol., 6: 101-112.

Afolabi, O.A. and O.G. Atanda, 2016. Comparative analysis of some selected cryptographic algorithms. Computing, Information Systems, Development Informatics Allied Research J., 7: 41-52.

BBC, 2018. Greenwich University fined £120,000 for data breach. https://www.bbc.com/news/technology-44197118

Boxcrptor, 2018. AES and RSA Encryption. https://www.boxcryptor.com/en/encryption

Capital Campus, 2015. KU, JKUAT top list of students hacking systems to change grades, fees. https://www.capitalfm.co.ke/campus/ku-jkuat-top-list-of-students-hacking-systems-to-change-grade-fees

Chavan, P.K., P.R. Kamble, P.P. Meshram and K.K. Doke, 2016. QR coded based digitized Marksheet system. Int. J. Engineering Research Advanced Technology, 3: 128-133.

CISSP, 2008. Certified Information Systems Security Professional, Wiley Publishing.

Dworkin, M.J., 2015. SHA-3 standard: Permutation-based hash and extendable-output functions.

Fue, K.G., M.P. Mahenge and L.S. Busagala, 2014. Web-based examination results release information system for cost effective strategies in academic institutions. In. J. Technology Enhancements Emerging Engineering Res.

Hercigonja, Z., D. Gimnazija and V. Croatia, 2016. Comparative analysis of cryptographic algorithms. Int. J. Digital Technology Economy, 1: 127-134.

Hernandez, P., 2018. NIST Releases SHA-3 cryptographic hash standard.

Ise, O.A., 2015. A novel framework for student result computation as a cloud computing service. Am. J. Syst. Software, 3: 13-19.

Juma, P., 2011. Hackers blamed in KU exam row.

Khovratovich, D., C. Rechberger and A. Savelieva, 2011. https://eprint.iacr.org/2011/286.pdf

Luo, P., Y. Fei, L. Zhang and A.A. Ding, 2016. Differential Fault Analysis of SHA3-224 and SHA3-256.

Mahajan, P. and A. Sachdeva, 2013. A study of enryption algorithms AES, DES and RSA for security. Global J. Science Technology Network, Web Security.

Martin, K., 2012. Everyday cryptography: Fundamental principles and applications, New York: Oxford University Press.

Milumbe, B., J. Phiri and M.M. Kalumbilo, 2017. Automating of the Candidate registration for school examinations in Zambia using the cloud model. Proceedings of the IEEE International Conference in Information and Communication Technologies (ICICT), Lusaka, pp: 108-115.

Mshangi, M., E.N. Nfuka and C. Sanga, 2015. Using soft systems methodology and activity theory to exploit security of web applaications against heartbleed vulnerability. Int. J. Computing ICT Res., 8: 32-52.

Mshangi, M., E.N. Nfuka and C. Sanga, 2016. Designing secure web and mobile-based information system for dissemination of students' results: The suitability of soft design science methodology. Int. J. Computing ICT Research, 10: 10-40.

Mugyenyi, R., 2017. Analysing information systems security in higher learning institutions of Uganda. Int. J. Scientific Technology Res., 10: 385-392.

Muhamadi, I.A., A.A. Zaidan, M.A. Zaidan, C. Mapundu and B.B. Zaidan *et al*., 2009. Auto notification service for the student record retrieval system using Short Message Service (SMS). Int. J. Computer Science Network Security, 9: 200-208.

Mushtaque, M.A., 2014. Comparison analysis on different parameters of encryption algorithms for information security. Int. J. Computer Sciences Engineering, 2: 76-82.

Ndolo, A., S. Ogara and S. Liyala, 2018. Model for information security government prediction in public Universities in Kenya. Int. J. Computer Applications Technology Res., 7: 63-77.

Nfuka, N.E., C. Sanga and M. Mshangi, 2014. The rapid growth of cybercrimes affecting inofrmation systems in the global: Is this a Myth or reality in Tanzania? Int. J. Computer Science Network Security, 9: 200-208.

NIST, 2015. SHA-3 Standard. Federal Information Processing Standards Publication.

Okibo, B.W. and O.B. Ochibe, 2014. Challenges facing information systems security management in higher learning institutions: A case study of the Catholic University of Eastern Africa-Kenya. Int. J. Management Excellence, 3: 336-349.

Onuiri, E.E., A. Oludele, O. Ibukum, C. Yadi and O. Etuk, 2015. Biometric student record management system. Int. J. Computer Science Information Security, 13: 51-61.

Perlroth, N., 2012. Hackers Breach 53 Universities and Dump Thousands of Personal Records Online.

Rico, S., S. Sembhi and R. Singh-Latulipe, 2011. Web apllication security: Sustainability business and risk considerations. ISACA J., 1: 1-28.

Singhal, N. and S. Singhal, 2016. A comparative analysis of AES and RSA algorithm. Int. J. Scientific Eng. Res., 7: 149-151.

Solomom, L. and J. Phiri, 2017. Enhancing the administration of national examinations using mobile cloud technologies: A case of Malawi National Examinations Board. Int. J. Advanced Computer Science Applications, 8: 294-305. DOI: 10.14569/IJACSA.2017.080942

Stallings, W., 2014. Cryptography and Network Security: Principles and Practice, 6th Edn., PHI.

Stufford, D. and M. Pionto, 2011. The Wep Application's Handbook: Finding and Exploiting Flaws, 2nd Edn., Wiley Publishing, Inc.

Vacca, J.R., 2009. Computer and Information Security Handbook, 1st Edn., Morgan Kaufmann Publishers.

Verizon, 2017. Data Breach Invesitigation Report.

Zabangwa, J., 2013. Online and SMS Results Dissemination System (ORDS), University of Zambia.