

Web and Mobile Examination Results Dissemination and Verification System Using Encryption and Cryptographic Hash Functions: A Case of TEVETA

Lister Mseteka, Jackson Phiri, and Simon Tembo

Abstract—The enormous impact of erroneous student examination results due to wrongly computed results, erring user authentication and loss of data integrity demands meticulous student result computation, secure storage and secure transmission of examination results. This paper describes our attempt to improve the integrity of students' examination results during transmission and storage through the use of encryption and cryptographic hash functions to provide information security objectives of confidentiality, integrity and authenticity assurances on data. The study was guided by three (3) objectives. A baseline study was conducted to determine the challenges faced by Zambia's Technical Education Vocational and Entrepreneurship Training Authority (TEVETA) and students regarding dissemination of students' examination results in order to address objective number one. The results from the study indicate that the current TEVETA examination process cycle and business processes have a number of irregularities. These include storage, dissemination and how students access the examination results. The results from the baseline study were used to come up with the model which was then used to develop the proposed prototype in order to address the second and third objective. The developed prototype from our model shows that our system provides secure storage and transmission of examination results. This is largely because of the encryption and hashing introduced during storage and dissemination of the results.

Index Terms—Encryption, examination dissemination system, integrity, hash function.

I. INTRODUCTION

Most developing countries and consequently public higher learning institutions in developing countries have low levels of Information Communication Technology (ICT) [1]-[3] and hence face challenges in securing the storage, management and dissemination of examination results. The conventional system of storing student examination results on paper or insecure electronic records is often characterised with high fraudulent practices ranging from fake results, falsification of results due to unauthorised amendments to results and unauthorised disclosure. Currently, educational institutions have become heavily reliant on ICT for delivering educational services such as,

examination results, study schedules, lectures and other information institutions wish to communicate to stakeholders [4]. Consequently, there has been a recent increase in the use of web and mobile applications in educational institutions for dissemination of students' examination results. However, the use of web and mobile application for 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. This is because web and mobile applications are susceptible to cyber attacks [5]-[8] which can comprise the confidentiality, integrity and authenticity of data. In this study, we propose a web and mobile prototype for dissemination of examination results for TEVETA using encryption and cryptographic hash functions to simultaneously provide confidentiality, integrity and authenticity of data [9]. A baseline study was conducted to establish the challenges faced by TEVETA and students regarding dissemination of examination results. The results obtained from the baseline study reveal that the current examination process cycle has a number of irregularities in terms of storage, dissemination and how students access the results. The business processes identified formed the basis of the developed web and mobile prototype for dissemination of results.

II. LITERATURE REVIEW

There has been an exponential increase in the number educational institutions disseminating examination results through mobile and web applications [6], [10]-[12]. Although educational institutions benefit from using web and mobile applications for dissemination of examination results, they are subject to cyber attacks [4]-[7] which can comprise the confidentiality, integrity and authenticity of academic records.

III. RELATED WORKS

Various studies have been conducted aimed at improving the security of web and mobile information systems for dissemination of examination results. Authors in Nigeria developed a Short Message Service (SMS) application that enables university students to access both current and old examination results by sending an SMS along with a password [10]. However, the SMS propagates between the sender and the receiver in unencrypted form, hence is subject to cyber attacks. Another system 'Results Alert through SMS and Email' was implemented in Nigeria that

Manuscript received September 30, 2018; revised February 12, 2019.

Lister Mseteka is with School of Engineering, Department of Electrical and Electronic Engineering, University of Zambia, Lusaka, Zambia (e-mail: lismseteka@gmail.com).

Jackson Phiri is with School of Natural Sciences, Department of Computer Science, University of Zambia, Lusaka, Zambia.

Simon Tembo is with School of Engineering, Department of Electrical and Electronic Engineering, University of Zambia, Lusaka, Zambia.

provides examination results through email and SMS [13]. However, results are transmitted and stored in the database in plain text without encryption, hence can be viewed or modified by anyone who has access to the database. It was observed by [4] that despite numerous vendor results computation systems on the market, many universities in Nigeria still engage in manual processing of students results due to high cost of software acquisition/licences, maintenance, infrastructure, support and security treats. The author proposed the design of a result computation system as a cloud service to eliminate the aforementioned factors. In addition, the author proposed securing computed results data using encrypting during transmission and before storage in the database using Advanced Encryption Standard (AES). However, encryption alone does not protect the data from modification or tampering as some cyber attacks are directed to cipher text [9]. In Palestine, an author developed an application that enable, supports students to access academic services such as assessment performance, study schedules and institution's provision of information to students irrespective of their geographic location [14]. The security incorporated was sending a SMS in a defined format along with a one-time password (Roll number password keyword semester). However, the study by [14] addressed only security issues in SMS and not web based applications.

In Zambia, a system was implemented for Examinations Council of Zambia (ECZ) that enables students to access them as soon as they are available using a mobile phone [11]. However, examination results are stored in plain text without encryption. In another research, authors in Zambia developed a web based candidate registration system based on the cloud model to reduce cycle time for registration and cost for IT infrastructure [15]. In Malaysia, authors developed an '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. However, the main emphasis on security is user and administrative access to the database and not security on examination results [12]. Authors in [16] designed and implemented 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. In [14], authors 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. In Tanzania, authors 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 [6]. However, encryption of communication channel proposed in [6] only provides confidentiality of examinations results during transmission but results are

stored in plain text in the database. In India, authors proposed an innovative method of authenticating digital mark sheets of students' results using Quick Response (QR) code [17]. However, digital records of students' results are stored in plain text meaning that can be viewed by unauthorised personnel.

IV. METHODOLOGY

A. Baseline Study

A mixed methods was used in this study. For quantitative data, questionnaires were administered to a total of 514 students from 12 institutions of higher learning in Zambia, 36 members of staff from various institutions of learning and TEVETA. The sample size had a total of 558 respondents consisting of students, members of staff in-charge of examinations from various institutions and TEVETA IT staff. For Qualitative data, interviews were conducted with IT staff at TEVETA.

TEVETA has a total of 304 registered institutions country wide [18] and a total of 25,650 students as at 31st December 2016 [19]. As at 31st December 2016, TEVETA developed, reviewed and approved a total of 247 curricula at diploma, advanced certificate, certificate, trade test and skill award levels. Out of the 247 revised curricula, 53 were at diploma level, 22 advanced certificate, 57 certificate, 89 trade test and 41 at skills awards [18], [19].

Institutions were purposely selected such that some are located in urban areas while others are in rural areas. Further, some institutions are private while others are public institutions. Students as well as members of staff that handle examinations from various institutions from various institutions were purposively selected to participate in the study. IT staff from TEVETA that handle examinations were purposively selected too.

B. System Automation and Software Development Methodology

The results of the baseline study were used to design a model from the current business processes benchmarked with ISO 27001 security standard and a prototype developed. Object oriented software development methodology was used in conjunction with iterative to allow new components to be added in an iterative and incremental manner.

C. System Modelling and Design

Object Oriented Design (OOD) was used to analyse the existing system and design the system modules. Unified Modelling Language was used in this study as it the de facto standard for object oriented systems [20]. UML diagrams are categorized in two, namely: behavioral and structural diagrams. Behavioral diagrams depict the dynamic behavior while structural diagrams depict the static behavior of the software system. In this study, Class diagrams and were used to capture the static behavior of the software system while use case and activity diagrams were used to capture the dynamic behaviors of the software system.

Fig. 1 is a Use Case diagram depicting the functionality of the system from the user's perspective. Fig. 2 is a class

diagram depicting static relationships that represent the fundamental architecture of the system. Fig.3 is an activity diagram showing the result computation process. The process of computing student results is performed by three roles which begins with the Data Entry personnel who enters the score of the students. The results are queued waiting for authorisation by the Data Manager which is the first level of authorisation. The Manager Qualifications performs the second level of authorisation. In the event that authorisation is denied at any level, results are removed for and sent to relevant personnel for reconsideration. Otherwise, the Data Manager can generate results for consideration by Senate or committee responsible for results. Upon approval by Senate or committee, manager qualifications or any personnel charged with the responsibility can publish results for students and other stake holders to view.

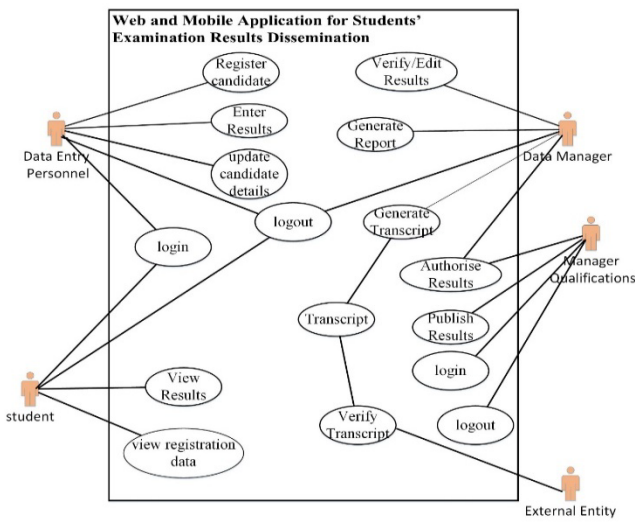


Fig. 1. System use case diagram.

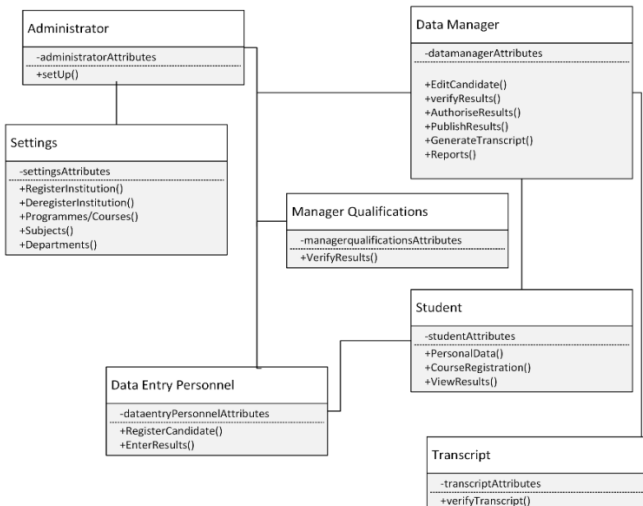


Fig. 2. Class diagram for examination results.

D. Entity Relationship Diagram

Entity relationship model describes data as entities, attributes and relationships. Fig.4 shows the entity relationship diagram drawn from requirements through interviews and documents such as student registration and examination entry forms.

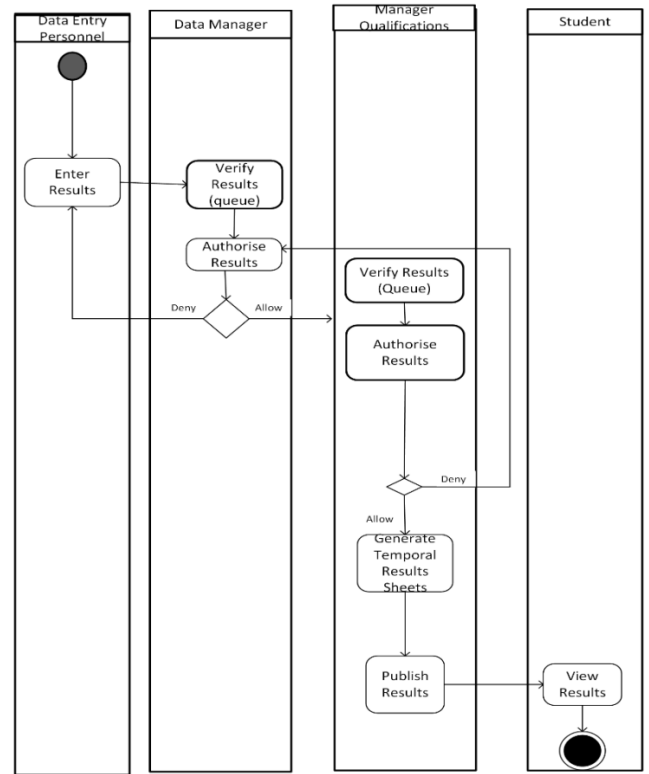


Fig. 3. Activity diagram for results computation process.

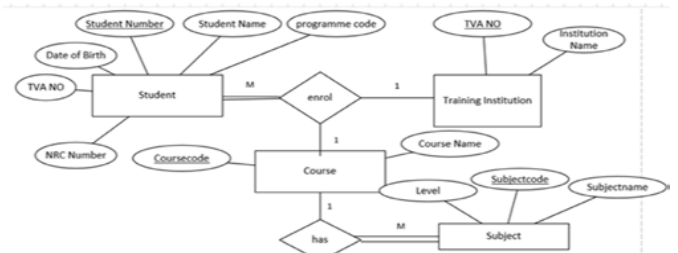


Fig. 4. Entity relationship diagram.

E. Business Process Mapping

The proposed secure model in Fig.5 is derived from the current transaction processes for candidate enrolment, examination entry and publishing of results. Automating the manual based phase of disseminating results through the mobile phone and web, use of encryption Advanced Encryption Standard (AES) algorithm and cryptographic hash function Secure Hash Algorithm (SHA3-224) are the changes proposed. In 2000, the National Institute of Standards and Technology (NIST) announced that Data Encryption Standards (DES) had been replaced by AES. In that same year, the United States mandated encrypting all sensitive but unclassified data using AES [21]. It is noted by [22] that AES is most widely used and secure encryption algorithm available today and preferred in banks, governments and high security systems around the world. In [23][23], a performance evaluation of four popular and commonly used encryption algorithms: Rivest-Shamir-Adleman (RSA), Data Encryption Standard (DES), Triple Data Encryption Standard (3DES), and Advanced Encryption Standard (AES) were carried out based on the encryption time, memory usage, output byte, power consumption rate, flexibility and security. Experimental results from the study show that AES consumes least encryption time and has least memory usage. A study in

[24] provided an analytical study on various symmetric encryption algorithms such as DES, 3DES, CAST-128, AES, RC6 and asymmetric RSA algorithm based on architecture of algorithms, security and limitations they have and it was established that AES is an effective encryption algorithm among all the encryption algorithms.

F. 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 figure derived from the current business process. The registration involves capturing of candidate information by TEVETA so that a student can be assigned an examination number which is used for examination enrolment at a later stage. All details pertaining to registration are stored in the database. After a candidate sits for examinations, marks are entered. 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. Hashed marks and encrypted marks are stored in different databases for the purpose of adding another layer of defence on 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.

Fig. 5 shows a secure architecture for examination results entry, storage and dissemination of examination results.

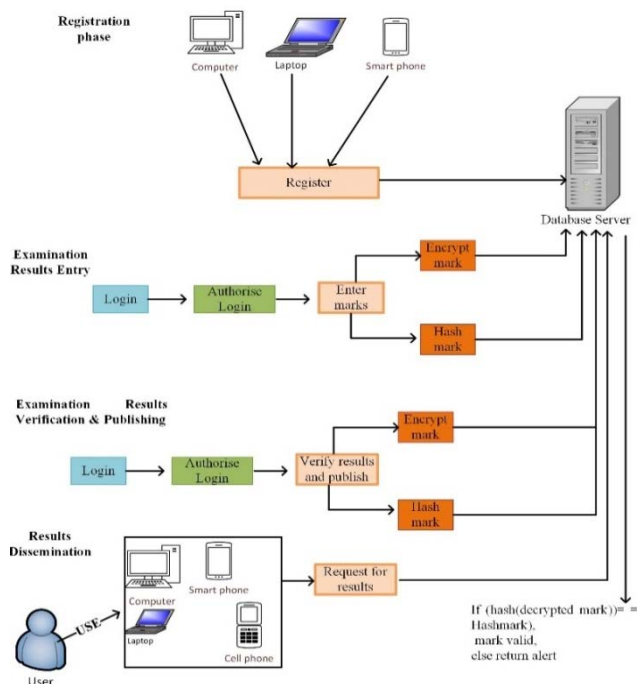


Fig. 5. Secure architecture for insertion, storage and dissemination of examination results.

V. SECURE MODELS FOR EXAMINATION RESULTS ENTRY AND RETRIEVAL OF RESULTS DEFINITION

Cryptographic hash functions provides the assurance of data integrity by engraving a fingerprint on source data, such that any alteration in transit or on the database will no longer guarantee the integrity of data.

Common hashing algorithms include Message Digest 2 (MD2), Message Digest 4 (MD4), Message Digest 5 (MD5) and Secure Hash Algorithm (SHA). However, MD2, MD4 and MD5 algorithms are no longer accepted as suitable hashing functions [21]. Several mathematicians have published articles documenting flaws in these algorithms. Recent cryptanalytic attacks demonstrated that there are weaknesses in the SHA-1 algorithm that led to the creation of SHA-2, which has four variants: SHA-224, SHA-256, SHA-384, and SHA-512 [21] [21]. A 2011 attacks breaks pre-image resistance for 57 and 80 rounds of SHA-512, and 52 out of 64 rounds for SHA-256 [25]. SHA-256 and SHA-512 are also prone to length extension attacks; by guessing the hidden part of the state, length attacks on SHA-224 and SHA-384 are possible. SHA-3 (Secure Hash Algorithm 3) is the latest member of the Secure Hash Algorithm released by NIST in 2015 [26]-[28]. 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. Authors in [29] proposed an efficient method to conquer SHA-3 family of hash algorithms using Differential Fault Analysis (DFA). DFA is a powerful and efficient attack method that has been used to break various cryptographic algorithms. The findings of the research shows that DFA on SHA3-224 and SHA3-256 are more difficult than SHA3-384 and SHA3-512, while SHA3-224 is more difficult to conquer than SHA3-256. Therefore, SHA3-224 was used to hash marks to provide integrity checks before decrypting and displaying examination results.

Let hash be the hash function and mark the mark obtained by a student, then the corresponding fingerprint or message digest is defined as:

$$x = \text{hash}(\text{mark}) \quad (1)$$

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:

$$x' = \text{hash}(\text{mark}') \quad (3)$$

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.

Fig. 6 shows the architecture for secure examination results entry while Fig.7 shows the diagrammatic flow of

results integrity check during retrieval of examination results.

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.

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

Start:

Retrieve mark 1 and mark 2 from the database tables

Mark1 -----> (encrypted mark)

Mark2 -----> (hashed mark)

Mark3 = AES_DECRYPT(mark1, key)

hashedmark = SHA3-224(mark3)

Compare mark2 with hashedmark,

If hashedmark == mark2

Decrypt (mark1)

Else return alert

Stop.

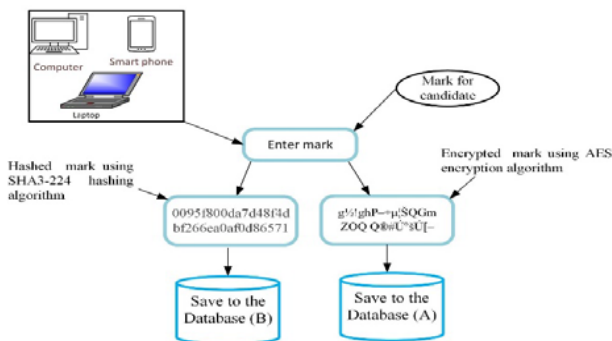


Fig. 6. Secure architecture for insertion of student results.

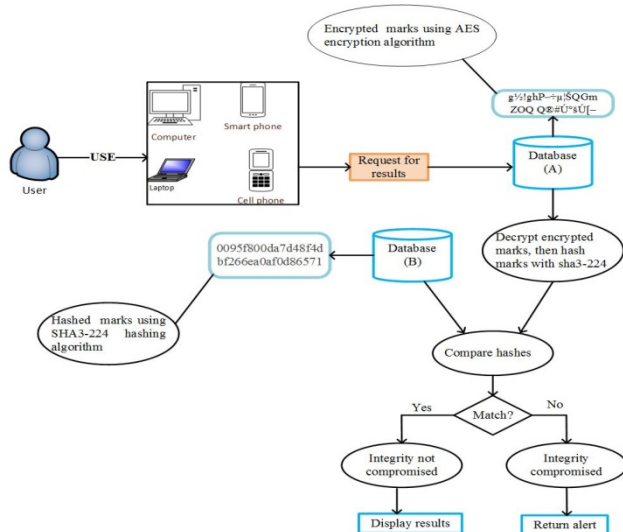


Fig. 7. Secure architecture for retrieval of examination results.

VI. FINDINGS

A. Results from the Baseline Study

A baseline study was conducted to establish the challenges faced by TEVETA, students and members of

staff from institutions of learning that handle candidate registration and examination related issues. The results of the study revealed that apart from specific factors that delay the release of examination results, a number of factors during candidate registration for examination also contribute. After establishing the challenges, respondents were asked to recommend solutions to resolve the mentioned challenges.

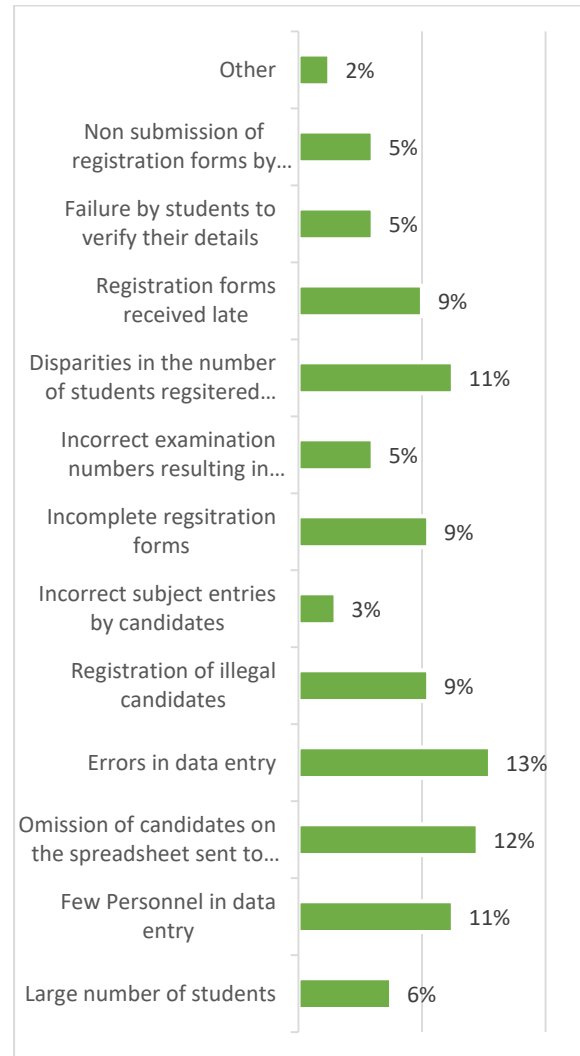


Fig. 8. Challenges faced by TEVETA Data Entry staff in Candidate registration for examinations.

The results of the baseline study in Fig.9 further show that factors that delay the release of examination results by TEVETA are long and tedious administrative procedure before release of examination results at 33%, large number of students at 25%, few personnel in data entry at 34% while late submission of continuous assessment results by institutions accounted for 8%.

Results from the baseline study in Fig. 10 show that out of 514 students who participated in the study, 76% think that a mobile application would improve access to examination results, 21% 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 percent do not have according to Fig.11. This means that more students have mobile phones which they can use to access examination results through a mobile application.

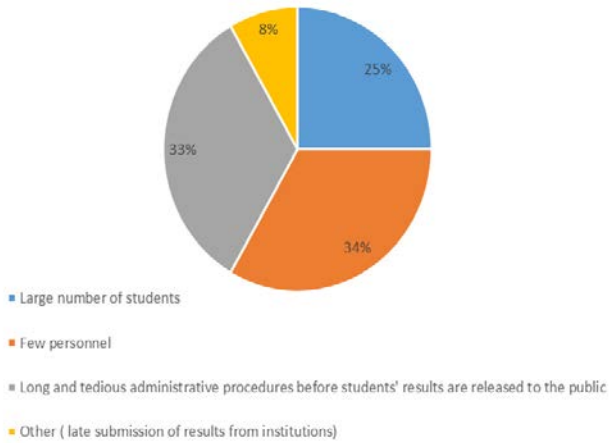


Fig. 9. Factors that delay the release of examination results.

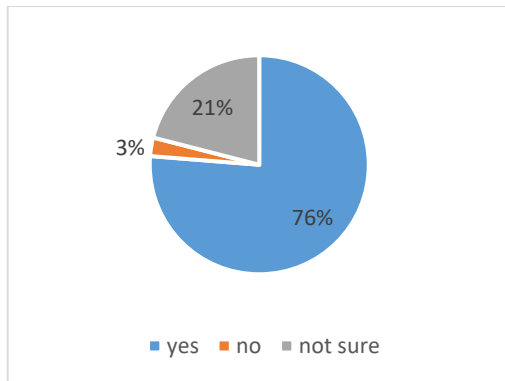


Fig. 10. Whether a mobile application would improve access to results.

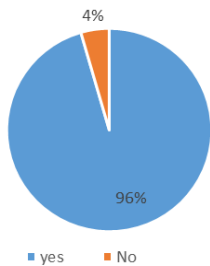


Fig. 11. Students with mobile phones.

When asked if a web based application would improve access to examination results, 71 percent agreed, 3 percent disagreed while 26 percent said they were not sure according to Fig. 12.

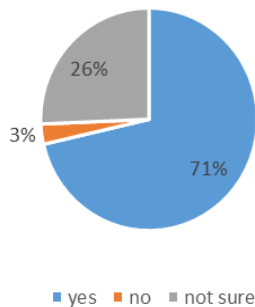


Fig. 12. Whether a web application would improve access to examination result.

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 according to Fig.13.

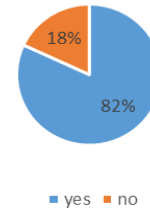


Fig. 13. Students' access to internet.

Results of the baseline study from TEVETA data entry personnel indicate that a mobile and web based application would improve dissemination of results. TEVETA data entry staff recommended features they want in a mobile and web application as shown in Fig. 14 and Fig.15 respectively.

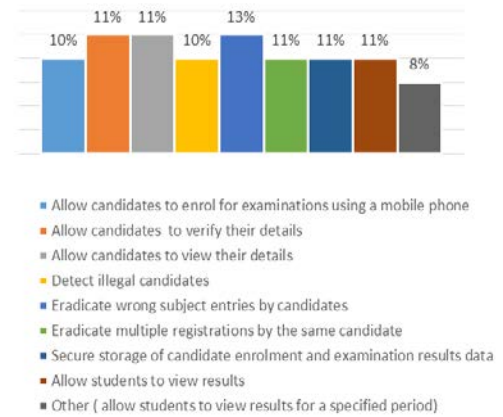


Fig. 14. Features recommended in a mobile application.

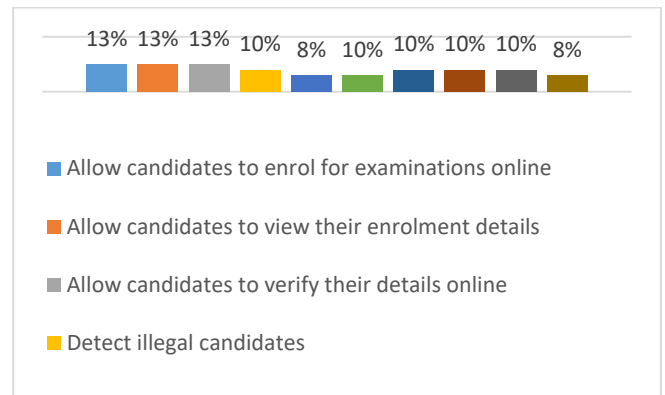


Fig. 15. Features recommended in a web application.

B. System Implementation

The proposed system has two components; web and USSD/SMS application. The web component was developed using Hypertext Preprocessor (PHP) and Hypertext Markup Language (HTML). The web application runs on Apache web server and uses MYSQL database engine to store information. The web application allows users to use computer or smart phones with internet connection to send requests to the database in order to retrieve both examination enrolment details and examination results. The USSD/SMS mobile application was developed using Java programming language. 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 individual or organisation needs to subscribe with mobile service


provider to use their gateway and it was expensive for the researcher. A USSD simulator was developed that allows students to send requests to the database in order to retrieve both examination enrolment details and examination results using a mobile phone. Fig. 16 and Fig. 17 show encrypted marks and hashed marks in the database tables.

studentnumber	coursecode	mark
5040	CS1	žRŦŦe(‘æŦŦ°ŠÇé
5040	CS2	çUÇÄimL'ÿ^ŦŦfÜ
5040	CS3	ˆ^UŦŦ°½8l<f³ÊÇ
5040	CS4	žRŦŦe(‘æŦŦ°ŠÇé
5040	CS5	þSñGUŦ5_E«u7Kø
5040	CS6	ˆ^UŦŦ°½8l<f³ÊÇ
5040	CS7	i-âÔq_°4ÄN

Fig. 16. Encrypted student marks in the database table.

studentnumber	coursecode	hmark
5040	CS7	270e03682fb47296e1bf6aa0ef2600ed908f4dbfe384e9e855...
5040	CS5	92b065a98f6209c6037b825c811f9176f66e542bf34e1293c...
5040	CS4	65a63788ac31cbb11efdb36acce7371f9b1032b71da2364240...
5040	CS3	9826417aebb868fd3963a393d570aa78d5476086766857d052...
5040	CS2	629fbfe8a30cb576c956bf22d3a75c213682e70e0ed8873462...
5040	CS1	65a63788ac31cbb11efdb36acce7371f9b1032b71da2364240...
5040	CS6	9826417aebb868fd3963a393d570aa78d5476086766857d052...

Fig. 17. Hashed marks in the database table.



Statement of Results

STUDENT 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. 18. Screen showing results of a student on a web page.

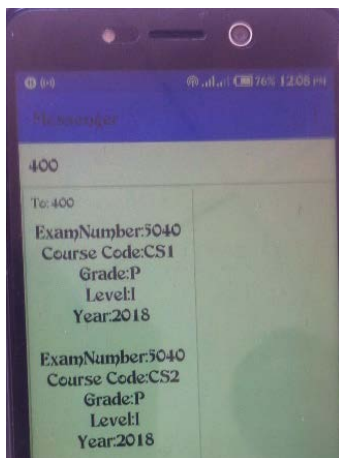


Fig. 19. Screen showing results on a mobile phone.

Fig. 18 shows the screen for examination results on the web and Fig.19 shows examination results on the mobile phone. If encrypted marks are not altered after authorisation

by the Senate or committee in charge of examination results and subsequent publishing of examination results, a student or stakeholder can view results on the web or mobile phone. However, if results of a student are altered by unauthorised personnel after publishing, the application program detects and display an alert that results could not be retrieved. This is because the hashes of the altered marks are different from the hashes of the marks originally stored in the database, meaning that the integrity of results no longer holds.

VII. DISCUSSION AND CONCLUSION

The results of this research show that the current examination results business processes has a number of irregularities. These irregularities include the current examination cycle business processes, storage, dissemination and how students access examination results. Further, the study revealed that all TEVETA IT staff that participated in the study think that a mobile and web application would improve dissemination of results. Out of 514 students who participated in this study, 76% think a mobile application can improve access to examination results, 21% are not sure while 3% disagree. The study further revealed that 71% of students think a web application can improve access to examination results, 26% are not sure while 3% disagree.

A prototype has been developed that allows students and other stakeholder to access students' results through mobile phones and the web. The web component has been implemented in PHP and the mobile component in Java. 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.

VIII. FUTURE WORKS

A number of business processes have been identified in this research study, however, some functionalities have not been implemented. The following are future research recommendation:

- Integrate the TEVETA application with Examinations Council of Zambia (ECZ) that stores national results for Grade 12 school leavers in Zambia so as to perform online verification of grades before a student is enrolled in a programme of study.
- Multifactor authentication to capture the true identity of students and TEVETA staff in charge of examinations
- Extend to other security services such as non-repudiation, entity authentication and data origin authentication

REFERENCES

- [1] P. Wallet, Paper Commissioned for the Global Education Monitoring Report 2016, Education for People and Planet: Creating Sustainable Futures for All, 2016.
- [2] K. Akarowhe, "Information communication technology (ICT) in the educational system of the third world countries as a pivotal to meet

- global best practice in teaching and development,” *American Journal of Computer Science and Information Technology*, vol. 5, no. 2, pp. 1-5, 2017.
- [3] T. Fredriksson, C. Barayre, P. Fajarnes, S. Fondeur, S. Lelmoli, D. Korka, S. Lakhe, M. P. Cuso, and M. Pletosu, The Information Economy Report 2017, United Nations Publications, 2017.
- [4] O. A. Ise, “A Novel Framework for Student Result Computation as a Cloud Computing Service,” *American Journal of Systems and Software*, vol. 3, no. 1, pp. 13-19, 2015.
- [5] S. Rico, S. Sembhi, and R. Singh-Latulipe, “Web application security: Sustainability business and risk considerations,” *ISACA Journal*, vol. 1, pp. 1-28, 2011.
- [6] M. Mshangi, E. N. Nfuka, and C. Sanga, “Designing secure web and mobile-based information system for dissemination of students' results: The suitability of soft design science methodology,” *International Journal of Computing and ICT Research*, vol. 10, no. 2, pp. 10-40, 2016.
- [7] D. Stafford and M. Pionto, *The Wep Application's Handbook: Finding and Exploiting Flaws*, 2nd ed., UK: Wiley Publishing Inc., 2011.
- [8] N. E. Nfuka, C. Sanga, and M. Mshangi, “The rapid growth of cybercrimes affecting information systems in the global: Is this a myth or reality in Tanzania?” *International Journal of Computer Science and Network Security*, vol. 9, no. 8, pp. 200-208, 2014.
- [9] K. Martin, *Everyday Cryptography: Fundamental Principles and Applications*, New York: Oxford University Press, 2012.
- [10] E. R. Adagunodo, O. Awodele, and S. Idowu, “SMS user interface result checking system,” *Issues in Informing Science and Technology*, vol. 6, pp. 101-112, 2009.
- [11] J. Zabangwa, “Online and SMS results dissemination system (ORDS),” thesis, University of Zambia, Zambia, 2013.
- [12] I. A. Muhamadi, A. A. Zaidan, M. A. Zaidan, C. Mapundu, B. B. Zaidan, and R. S. Raja, “Auto notification service for the student record retrieval system using short message service (SMS),” *International Journal of Computer Science and Network Security*, vol. 9, no. 8, pp. 200-208, 2009.
- [13] O. O. Olusanya and O. Ogaba, “Result alert system through SMS and email,” *IOSR Journal of Moble Computing & Computing*, vol. 2, no. 2, pp. 41-45, 2015.
- [14] M. I. Al Sheikh Eid, “An improved SMS user interface system to support university services: A case study on Islamic University of Gaza,” thesis, Islamic University of Gaza, Palestine, 2011.
- [15] B. Milumbe, J. Phiri, and M. M. Kalumbilo, “Automation of the candidate registration for school examinations in Zambia using the cloud model,” in *Proc. of IEEE International Conference in Information and Communications Technologies (ICICT)*, 2017.
- [16] L. Solomom and J. Phiri, “Enhancing the administration of national examinations using mobile cloud technologies: A case of Malawi National Examinations Board,” *International Journal of Advanced Computer Science and Applications*, vol. 9, no. 8, 2017.
- [17] P. K. Chavan, P. R. Kamble, P. P. Meshram, and K. K. Doke, “QR coded based digitized marksheet system,” *International Journal of Engineering Research and Advanced Technology*, vol. 3, no. 2, pp. 128-133, 2016.
- [18] TEVET Newswriter, *A Publication of the Technical Education, Vocational and Entrepreneurship Training Authority*, no. 2, April-June 2017.
- [19] TEVET Newswriter, *A Publication of the Technical Education, Vocational and Entrepreneurship Training Authority*, no. 3, July-September 2017.
- [20] X. Jia, *Object-Oriented Software Development Using Java*, 2nd ed., Pearson Education Inc., 2003.
- [21] *Certified Information Systems Security Professional*, UK: Wiley Publishing, 2008.
- [22] Boxcryptor. (July 2018). AES and RSA Encryption. [Online]. Available: <https://www.boxcryptor.com/en/encryption>
- [23] O. A. Afolabi and O. G. Atanda, “Comparative analysis of some selected cryptographic algorithms,” *Computing, Information Systems, Development Informatics & Allied Research Journal*, vol. 7, no. 2, pp. 41-52, 2016.
- [24] Z. Hercigonja, D. Gimnazija, and V. Croatia, “Comparative analysis of cryptographic algorithms,” *International Journal of Digital technology & Economy*, vol. 1, no. 2, pp. 127-134, 2016.
- [25] D. Khovratovich, C. Rechberger, and A. Savelieva. (July 2015). Bicliques for preimages: Attacks on Skein-512 and the SHA-2 family. [Online]. Available: <https://eprint.iacr.org/2011/286.pdf>
- [26] P. Hernandez. (August 2015). NIST releases SHA-3 cryptographic hash standard. [Online]. Available: <https://www.nist.gov/news-events/news/2015/08/nist-releases-sha-3-cryptographic-hash-standard>
- [27] M. J. Dworkin. (August 2015). SHA-3 standard: Permutation-based hash and extendable-output functions. [Online]. Available: https://www.nist.gov/publications/sha-3-standard-permutation-based-hash-and-extendable-output-functions?pub_id=919061
- [28] National Institute of Standards and Technology, *SHA-3 standard: Permutation-based hash and extendable-output functions*, Federal Information Processing Standards Publication, 2015.
- [29] P. Luo, Y. Fei, L. Zhang, and A. A. Ding, “Differential fault analysis of SHA3-224 and SHA3-256,” in *Proc. of 2016 Workshop on Fault Diagnosis and Tolerance in Cryptography (FDTC)*, 2016.

Lister Mseteka received her Bachelor of Science Degree from the University of Greenwich and a Master of Engineering in Information and Communication Technology Security from the University of Zambia. She is currently working as a lecturer at Evelyn Hone College. Her current research interest is information security and advanced database security.

Jackson Phiri is a lecturer at the University of Zambia. He received his Bachelor of Computer Science at the University of Zambia and an MSc in Computer Science at the University of the Western Cape. He received his PhD at Harbin Institute of Technology. His current research interest include information security, spatial databases, cloud computing and sensor networks.

Simon Tembo is a lecturer and current Head of Department for Electrical and Electronic Engineering at the University of Zambia. He received his Bachelor of Engineering Degree at the University of Zambia and a Master of Engineering degree at University of Electro-communications, Japan. He received his Doctor of Engineering Degree at Akita University, Japan. His current research areas include Next-Generation High-performance and robust networks, wireless sensor networks, multi-path routing for Optical Technologies, Information and Communication Technologies in Modern Societies and routing algorithms for flexible bus systems.