IJARIIT INTERNATIONAL JOURNAL OF ADVANCE RESEARCH, IDEAS AND INNOVATIONS IN TECHNOLOGY

ISSN: 2454-132X
Impact Factor: 6.078
(Volume 7, Issue 6 - V7I6-1229)
Available online at: https://www.ijariit.com

Secure result processing system amid COVID-19 and beyond using digital signature

Ome Uchenna Kenneth
uchenna.ome@unn.edu.ng
University of Nigeria, Nsukka, Nigeria

Ugwu Celestine Ikechukwu
celestine.ugwu@unn.edu.ng
University of Nigeria, Nsukka, Nigeria

Ezenna Charles
charlesezenna@gmail.com
University of Nigeria, Nsukka, Nigeria

ABSTRACT

Digital workflow of results from the department where results are generated, to the processing unit and finally to the students or any other units where results are needed is highly recommended more especially in this era of technological revolution and COVID-19 epidemics. Besides, couple of drawbacks is usually associated with paper based result processing. These drawbacks included but not limited to high overhead cost, high fraud risk, document misplacement, degradation of document after multiple printing and delay in result processing. However, online result processing cannot be exonerated from fraud such as cyber related frauds. Cybercrimes are increasing on daily basis with more concern in developing countries and as such, every online business or transaction should be defended against malicious attacks and unnecessary alterations. Considering the critical and confidential nature of result vis-à-vis the menace associated with cybercrime , this paper suggest the application of digital signature in online result processing to ensure authentication of the sender, integrity of data and non-repudiation. The use of digital signature technique as a security measure in online result processing will promote trust and acceptability of result and other related information. This paper carried out an overview of cybercrime, introduced the concept, framework and application of digital signature in online result processing.

Keywords: *Result Processing, Cyber Attack, COVID-19, Digital Workflow and Digital Signature*

1. INTRODUCTION

An attempt to solve the problem facing students' result computations in various universities in Nigeria has made bare some irregularities associated with manual method of result computation. It was equally found out that only few universities have started making use of the automated result processing and systems adopted by some of these institutions lack those security tools needed to combat the ongoing fraud in both the manual and the existing computerized result processing system. More so, with the report of the first case of COVID-19 in Africa in February, 2020 and continuous spread of the disease, governments across the continent closed down educational institutions [1]. This scenario has brought serious challenges to the conventional means of teaching and learning via classroom. The announcement of temporary close down of schools in Nigeria by the ministry of education in response to the pandemic has made, educators, founders and policymakers to start rethinking on the ideal means of delivering and accessing education in the country[2]. There is no doubt that CONVID-19 pandemic is revolutionizing digital and online education globally, which will promote secure online result processing.

Several successful researches have made several attempts to automate academic result processing systems. Solutions developed through these researches join an avalanche of other applications deployed on the wild internet and as a result, they are exposed to cyber attacks. In the same vein, academic results are very sensitive piece of data, consequently systems developed to process them requires critical attention to data security details.

Researches and industry products have demonstrated that digital signature can be used to secure database and distributed applications. In this paper, we provide an additional security layer for a result processing system. The paper leveraged upon the Java Cryptographic Architecture (JCA) to digitally sign input (results). A test application for result processing was developed and then using JCA, we provide an additional security layer. Unit and behavioral tests were written to guarantee the effectiveness and accuracy of the system. By implication, the successful implementation of digital signature eliminates the fears of non-repudiation, integrity, and authenticity associated with online result processing systems.

1.1 Research Motivation

The revolution of digital and online education globally because of CONVID-19 pandemic motivated the authors of this paper into this research direction. At present, many universities in Nigeria have not adopted the use of online result processing system rather they only have portals for students' course registration. Even those that have adopted online and computerized result processing system lack a secure means of protecting the information against malicious attack.

In such situation, some personnel in charge of result processing like departmental examination officers in the universities and those staff working under exams and record unit may connive to alter students' grades in a particular course(s) without the knowledge of the lecturer(s) that taught the course. Even an intruder can hijack and alter the result without the knowledge of those concerned.

Hence, the need to encourage the use of robust computerized online result processing system backed up with digital signature technique for a secure result processing. With this, when the lecturer sends results to the module used as raw data for result processing, no other person will have access to edit the input before sending it for processing.

1.2 Research Aim

To develop additional security layers to database application/distributed system in academic result processing software using digital signature.

1.3 Research Objectives

Below are the objectives of this research:

- To review cyber-attacks possible within the database application /distributed system sphere.
- Enforce a system that would automatically pool fail courses into the student's registration portal and ensure they are registered before registering new courses.
- Set up a unified database system that coordinates course registration and result processing.
- Provide a means of transmitting secured examination results to all the appropriate units such as department, exams and record units.
- To enforce secured implementation for database application and distributed system using academic result processing as a case study.
- Implement digital signature to secure academic result processing application.

2. LITERATURE REVIEW

There have been several studies on online course registration, computerized result processing as well as transcript generation, some of which were reviewed in this paper.

Authors in [3] designed a software application for the processing of students' results. The system was developed using water fall software cycle model. It is a web-based application that runs on a network. The tools used in developing the system include MySQL relational database, Dream weaver integrated development Environment, PHP and JavaScript.

The application software was successfully developed, tested, and found to be working as expected. It is well-designed software that is capable of storing and processing students' results with high speed and accuracy. It has adequate security that enforces data integrity. It is elegant, convenient, and easy to use due to the use of a GUI rather than command-line approach. It also has a large database that can automatically increase in size. With this application, the processing of students' results can be automated to a large extent, thereby reducing processing time and increasing accuracy. But, this system lack the ability to encrypt result for transmission, not capable of monitoring activities going on in the system and also does not have the capacity to work offline.

In [4], the developed result processing system considered the following: user validation, students' registration, course registration, grade computation, grade point average and cumulative grade point average computation. The report of the system showed that it was successfully developed, tested and found to have achieved the author's aim. Though the system was working, it still has some errors as the data entry is done manually and there were no multilayered backup in case of server failure. The system do not have audit trail to monitor the activities of the user on the application and the time it took place.

According to [5], the use of computers for information processing made the following possible:
Calculate the total score, grade a course given the required parameters which are the continuous assessment score and exam score, allows the lecturers to work on students' results offline, prohibiting any upload of any file which is not an MS-Excel 2007, uploading the concerned file to the server, generation of students' transcript up to the present level, which is also done at the point of transcript download, monitor the roles handled by different levels of admin, traced the activities of the system administrator(s), implementation of single login, generation of important reports such as students' details, lecturers' details, class lists, course lists, result sheets and transcripts and messaging system

To achieve these, the author employed the following: architectural design, UML Class diagram, database design and human interface design. The author equally made use of these tools PHP, MYSQL, JavaScript, CSS, HTML, Ajax, JQuery and Excel [6]. The system developed here virtually solved most of the problem facing result processing in the university, but the aspect of system that needed an improvement is the security of the result that will transmitted from the lecturer to the destinations where results are using internet.

Web based application to facilitate online processing of result was developed in [7].The system was developed using HTML, CSS#, JavaScript, PHP and MYSQLi as the relational database software. The application was developed, tested and was found working as expected. The system was able to handle the following:

- Storing and retrieving academic records with high speed and accuracy, and presenting useful information to its users.
- Reduction in the cost of processing student's results and also the time spent in the computation of student's grades and the elimination of duplication of resources in terms of manpower and infrastructure.
- Enforces data integrity through the use of a relational database management system to an extent, it also minimizes data redundancy and it is user-friendly

Though, the system was working as expected, there is still need for an improvement. There is a need to add audit trial, multilayered backup and security on the result to be transmitted.

In summary, the major feature that is lacking based on this review is that of security of the result to be transmitted. If a result as sensitive information in the universities is allowed to be transmitted via internet lacks the strong security measure it requires; then such result is made porous for an intruder to hijack, alter and allow transmission to continue to the destination.

Thus, a Secure Result Processing System was designed and developed to address the shortcomings inherent in manual processing as well as some of the weaknesses of the very numerous systems developed for result processing. Digital signature approach was used to enforce security in our developed system.

3. COVID-19: A CALL TO REVAMP TEACHING AND LEARNING IN NIGERIA

The outbreak of COVID-19 issued a urgent call to revamp teaching and learning in Nigeria by the stakeholders. With what was experienced in the educational sector in Nigeria due to CONVID-19 pandemic, it has become imperative for a drastic improvement in the sector in readiness for digitalized and online teaching and learning. The report of cases of coronavirus disease in Nigeria brought about a total closure of all educational institutions for a period not less than seven months. Within this period, both teachers and students were made to remain at home bringing all educational activities to almost a standstill. This situation ushered in the following questions: [2]

i. Do schools in Nigeria have the required technology to take care of students in the country?
ii. Do households have the needed facilities that will enable students engage in distance learning?
iii. Do teachers have the resources and technical know-how to deliver lessons online?

There was no clear-cut policy to mitigate disruption of teaching and learning imposed by the pandemic.

Distance learning support announced by Italian government in March, 2020 include providing schools with digital platform and tools for distance learning, assist the less privileged with digital devices and organizing training for staff on the required technique and methodologies for distance learning [8].

Therefore, if Nigeria values the education of her youths, the government should be thinking at direction of providing the required infrastructures, technologies, training and retraining of teachers and students for an online learning. To ensure an effective online learning in Nigeria, teachers and students should have the needed skills, access to computers, software, and among others, there should be an existence of internet connectivity and reliable power supply. A proactive measure should be taken by Nigerian government to ensure that students continue to learn even when school is closed down amid and even beyond COVID-19. When learning becomes online based, online result processing becomes inevitable. Hence, there is need for proper security against data to prevent data from being compromised by attackers.

4. APPLICATION OF DIGITAL SIGNATURE IN RESULT PROCESSING

The global cyber security space is constantly evolving with an increasing attack vectors and zero-day payloads which paved way to cyber espionages dealing heavy blows on companies, organization and institutions across the globe. This cyber security threat cuts virtually in every spheres of the software industry and poses a question on the reliability of the data we access.

It is now obvious that developing systems with access and privilege restrictions does not necessarily guarantee that such system will be hack proof as attackers have established various sophisticated techniques to compromise application regardless of the application architecture and platform. Several notable attempts have been made to help protect users and their data, but attacker are constantly developing sophisticated tools that can bypass anti-viruses and firewalls without been detected. In the light of the foregoing and for the need to safely transmit sensitive academic result data within a university community, the following questions being raised:

- Integrity: has the message been altered in transit?
- Authenticity: Is the author of the message the person he really claims to be?
- Non-repudiation: can the author of the message later deny being the source? These questions are particularly important where there is need for speed, reliability and efficiency in academic result processing.

Several successful attempts have been made to efficiently compute/process academic results with emphasis on reducing the inherent computational errors, however there have been no guarantees that what is eventually transmitted after computation reflects exactly what the student have earned. There are possibilities of alteration in the cause of data transmission. One of such possibilities is the Advanced Persistent Threats (APTs) which are highly sophisticated, target specific and operate in a stealthy mode till the target is compromised. Authors in [9] explore the intention of the APTs so as to deploy target specific automated malwares in a host or network to initiate an on-demand attack based on continuous monitoring. Man in the middle attacks are also possible in distributed systems when a hacker inserts himself between the communications of a client and a server. A hacker can achieve this by hijacking a session, IP spoofing, replay, phishing, spear phishing attacks etc. In [10], an explanation of how digital signature implementation can militate against these cyber-attacks. Based on Cryptography, an aged long cipher technique that successfully transcend into Information Technology, Digital Signature answers the questions posed on integrity, authenticity & non-repudiation as seen in fig1.

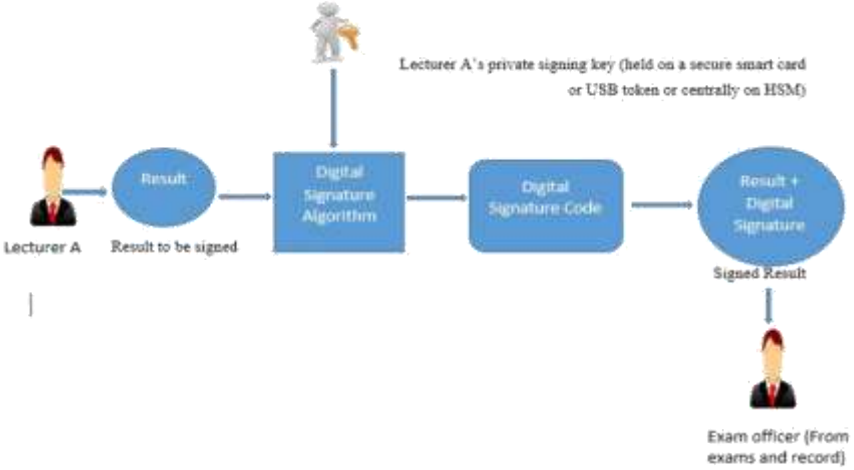

Lecturer A's private signing key (held on a secure smart card
or USB token or centrally on HSM)
Lecturer A
Result
Result to be signed
Digital Signature Algorithm
Digital Signature Code
Result + Digital Signature
Signed Result
Exam officer (From exams and record)

Fig-1: Transmission of Digitally Signed Result

The proposed result processing system with digital signature security back up was designed and implemented using java. There are a number of programming languages and Relational Database Management Systems (RDBMS) that can be used to accomplish these tasks. We selected Java programming language for its comparative edge over most traditional programming language. With a great team at Oracle behind its maintenance, Java has implemented a lot of useful classes and libraries (including JCA) and has many endearing features. Amongst many of Java's features include:
It is object oriented language: this means we can organize and plan our software in reusable modules which makes development easier and debugging faster.

Java is platform independence: with the Java Virtual Machine (JVM), the java platform makes it possible for us to write programs that can be compiled into byte code once and deploy anywhere.

The test application was built using Java's Spring 5 framework which provides a comprehensive programming and configuration model for modern Java-based enterprise applications on any kind of deployment platform. The Spring 5 framework has great support for testing, data access; system integration, Dependency Injection DI, Aspect Oriented Programming etc. and all of these are tools which will be needed in the course of this research. We will use hibernate, an Object Relational Mapping (ORM) tool to interface with H2 Database which is an in-memory database for development. With an ORM tool like hibernate, our application can be deployed on any RDBMS for production without any changes to the data layer of our application. System design deals with the coordination of activities, processes and the use of equipment in order to achieve the objectives of the research.
However, in any system design, the output is considered first because it is the desired output that will determine both the input and the procedure**.** All the modules of the program were integrated together to become a single program and then test run as shown in fig-2 and fig-3. Figure-2 shows a flowchart of how digital signed result can be accessed while fig-3 shows a flowchart of result uploading process.

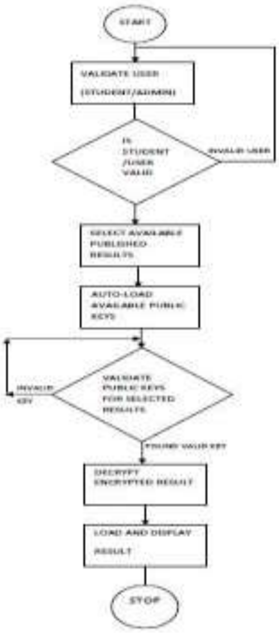

START
VALIDATE USER (STUDENT/ADMIN)
IS STUDENT /USER VALID
INVALID USER
SELECT AVAILABLE PUBLISHED RESULTS
AUTO-LOAD AVAILABLE PUBLIC KEYS
VALIDATE PUBLIC KEYS FOR SELECTED RESULTS
INVALID KEY
FOUND VALID KEY
DECRYPT ENCRYPTED RESULT
LOAD AND DISPLAY RESULT
STOP

Fig-2: Accessing digitally signed result

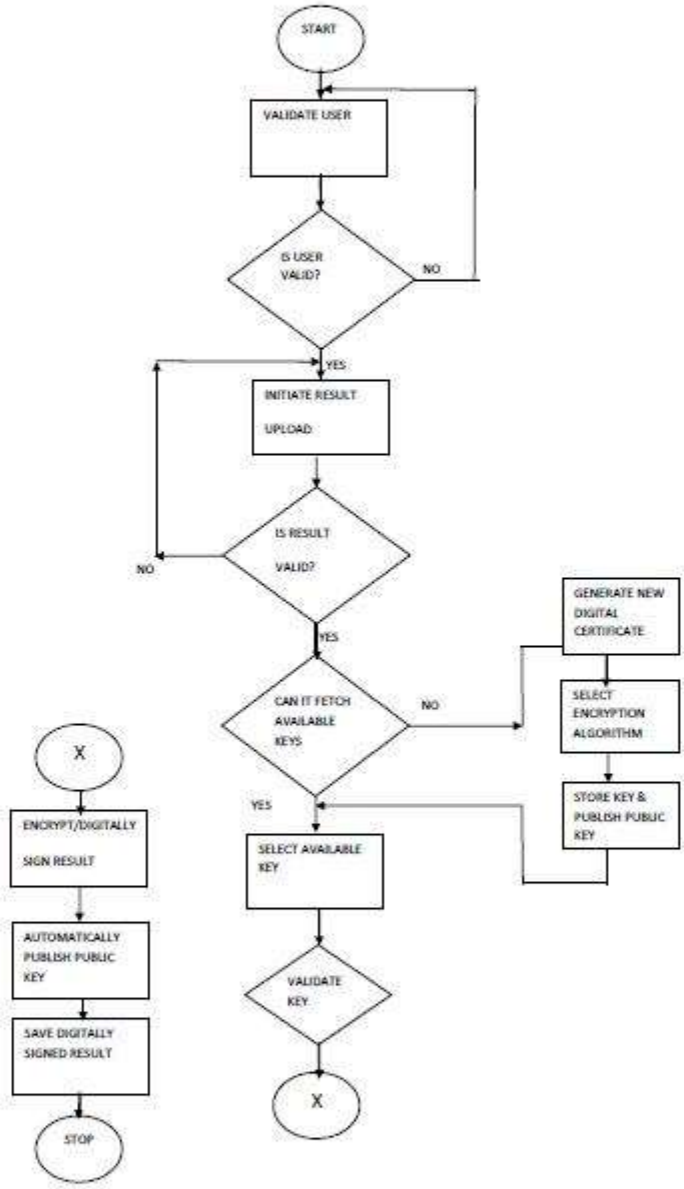

START
VALIDATE USER
IS USER VALID?
NO
YES
INITIATE RESULT UPLOAD
IS RESULT VALID?
NO
YES
CAN IT FETCH AVAILABLE KEYS
NO
GENERATE NEW DIGITAL CERTIFICATE
SELECT ENCRYPTION ALGORITHM
STORE KEY & PUBLISH PUBLIC KEY
YES
SELECT AVAILABLE KEY
VALIDATE KEY
X
X
ENCRYPT/DIGITALLY SIGN RESULT
AUTOMATICALLY PUBLISH PUBLIC KEY
SAVE DIGITALLY SIGNED RESULT
STOP

Fig-3: Result uploading process

5. DATABASE DESIGN

The proposed system database design shown in fig-4 below describes how data is represented and used. This application has one database called digital_signature_result with twelve (12) relational tables hosted on MS-SQL Server 2008. The relationships among the tables are shown below.

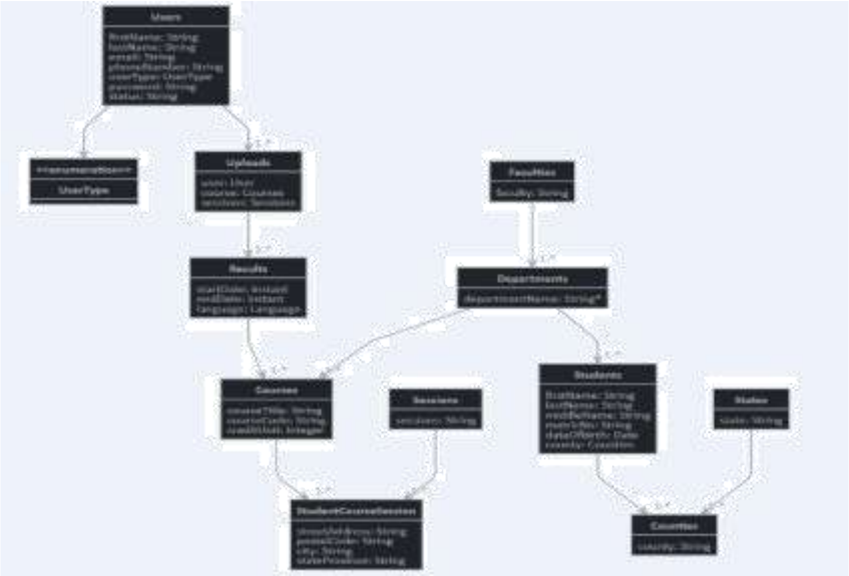
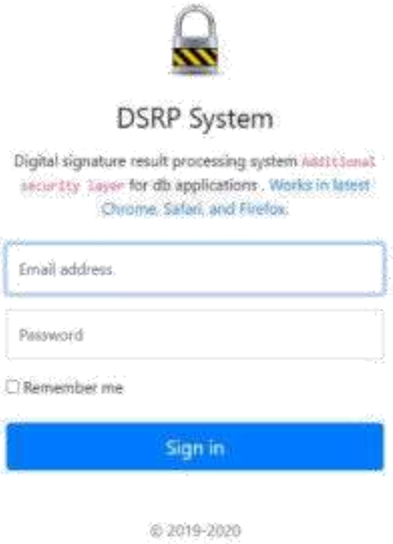


Fig-4: Database design (screenshot the pdf format of the schema)

6. RESULTS AND DISCUSSION

The developed software application was tested and found to operate as expected. The computer software application is required to be independent of any platform. Figure-4 below shows the login page when the program is started.



DSRP System

Digital signature result processing system Additional security layer for db applications . Works in latest Chrome, Safari, and Firefox.

Email address

Password

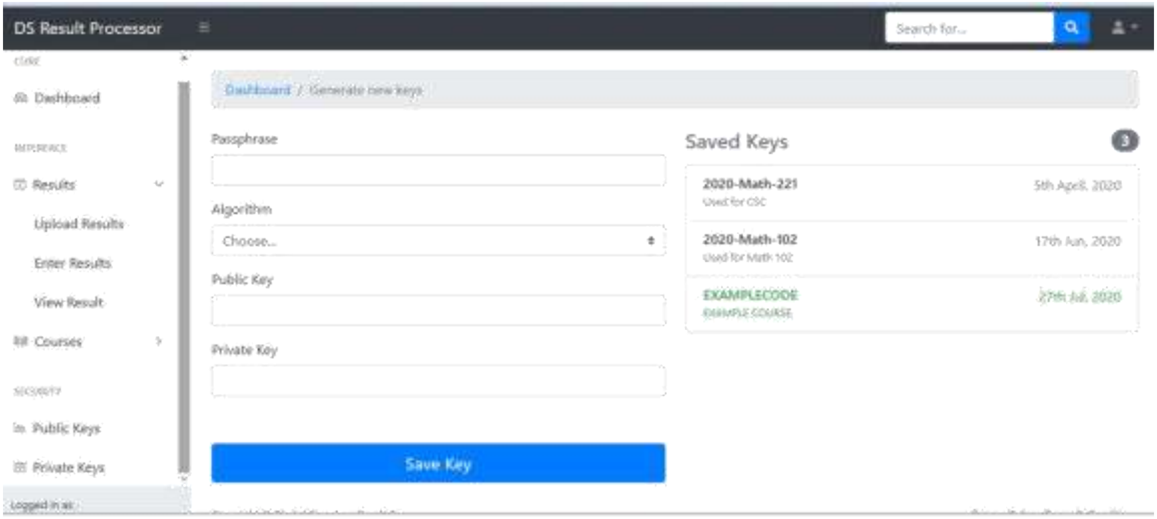
□ Remember me

Sign in

© 2019-2020

Fig-5: Screenshot showing login page

For user to have access to the package, the user needs to supply the email address and password. Different privileges are given automatically to different types of users by the system. If the user has not been registered, the user will click on apply for digital certificate and a form will appear demanding for the users details. When the user has supplied the needed information, it will take the user to the passphrase where a key will be generated as shown fig-5.



Passphrase

Algorithm

Choose...

Public Key

Private Key

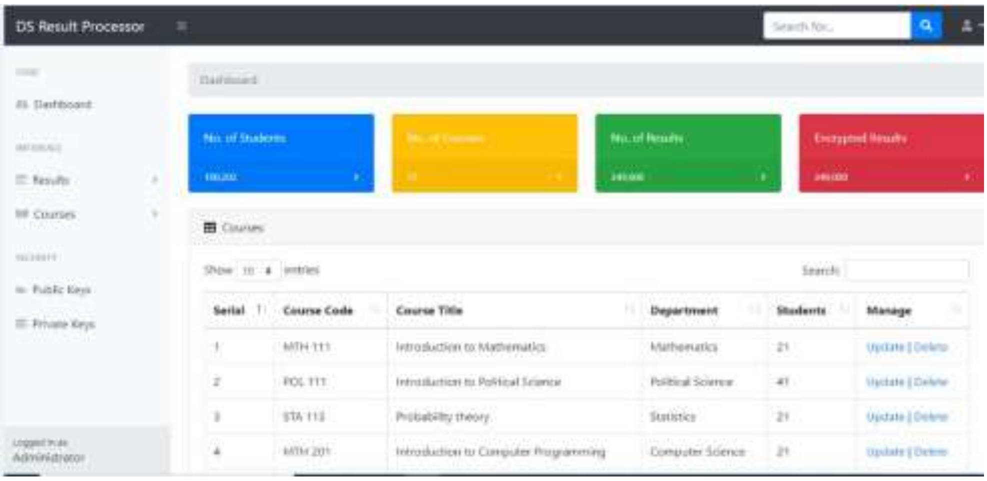
Save Key

Saved Keys 3

2020-Math-221 Used for CSC	5th April, 2020
2020-Math-102 Used for Math 102	17th Jun, 2020
EXAMPLECODE EXAMPLE COURSE	27th Jul, 2020

Fig-6: Screenshot of key generator

After a successful login, a home page or dashboard will appear as shown in fig-7 below.

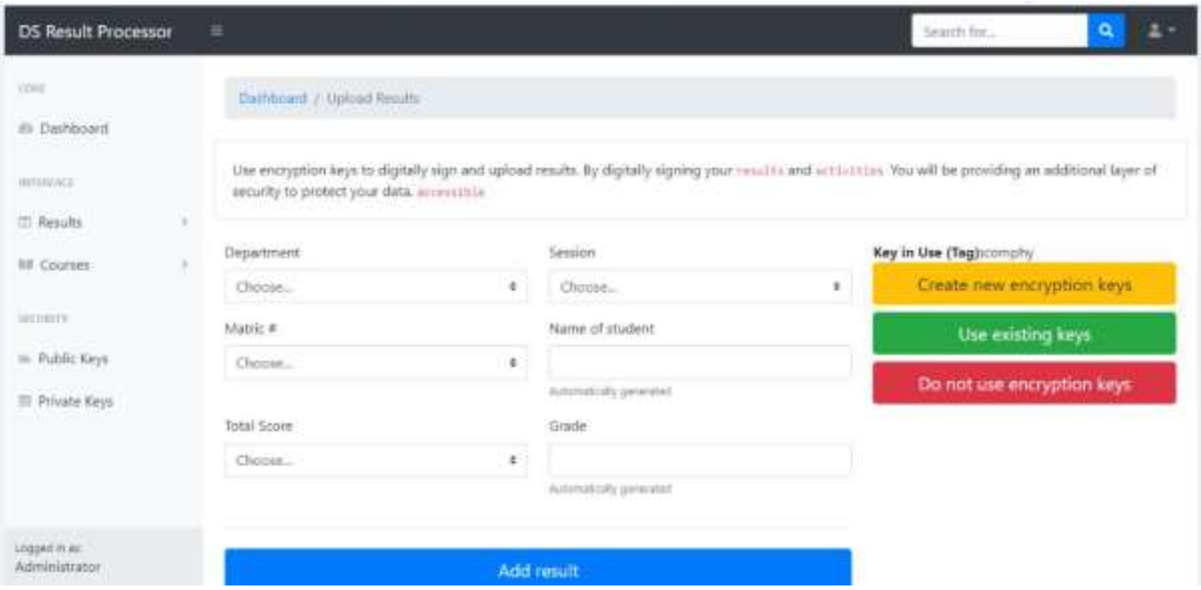


Show 10 entries Search:

Serial	Course Code	Course Title	Department	Students	Manage
1	MTH 111	Introduction to Mathematics	Mathematics	21	Update | Delete
2	POL 111	Introduction to Political Science	Political Science	41	Update | Delete
3	STA 112	Probability theory	Statistics	21	Update | Delete
4	MTH 201	Introduction to Computer Programming	Computer Science	21	Update | Delete

Fig-7: Screenshot of the dashboard

Figure-8 represents the section for uploading of result in our system; fig-9 presents a view of semester result in our proposed system and fig-10 presents statement of academic transcript.



Use encryption keys to digitally sign and upload results. By digitally signing your `results` and `activities` You will be providing an additional layer of security to protect your data. `accessible`

Department: Choose...

Session: Choose...

Key in Use (Tag): comphy

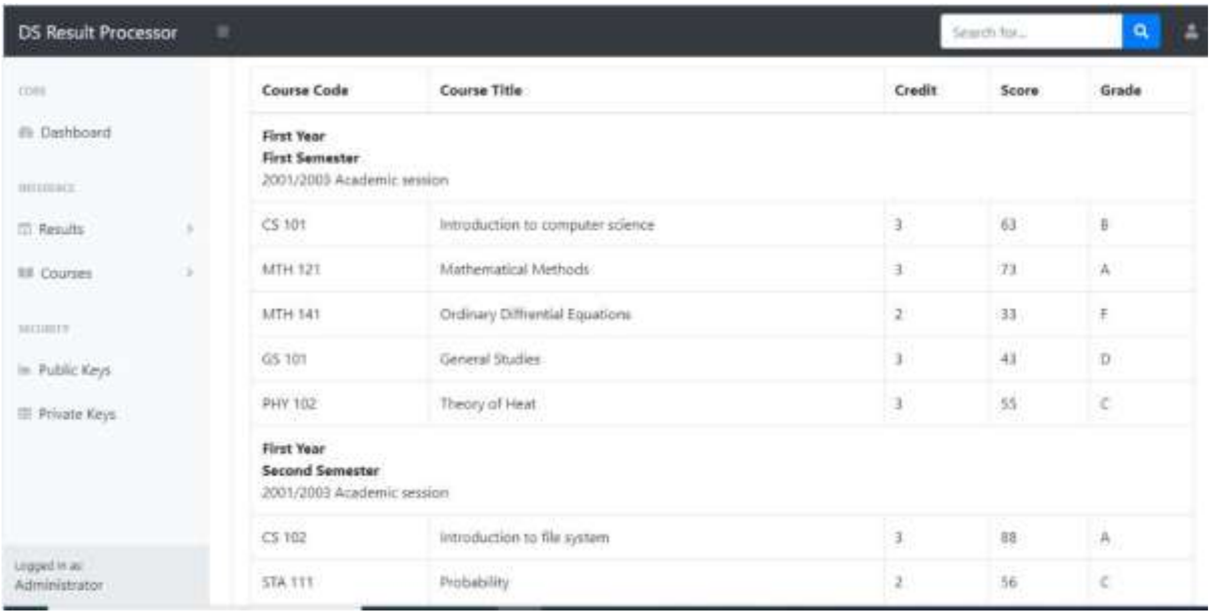
Matric #: Choose...

Name of student: Automatically generated

Total Score: Choose...

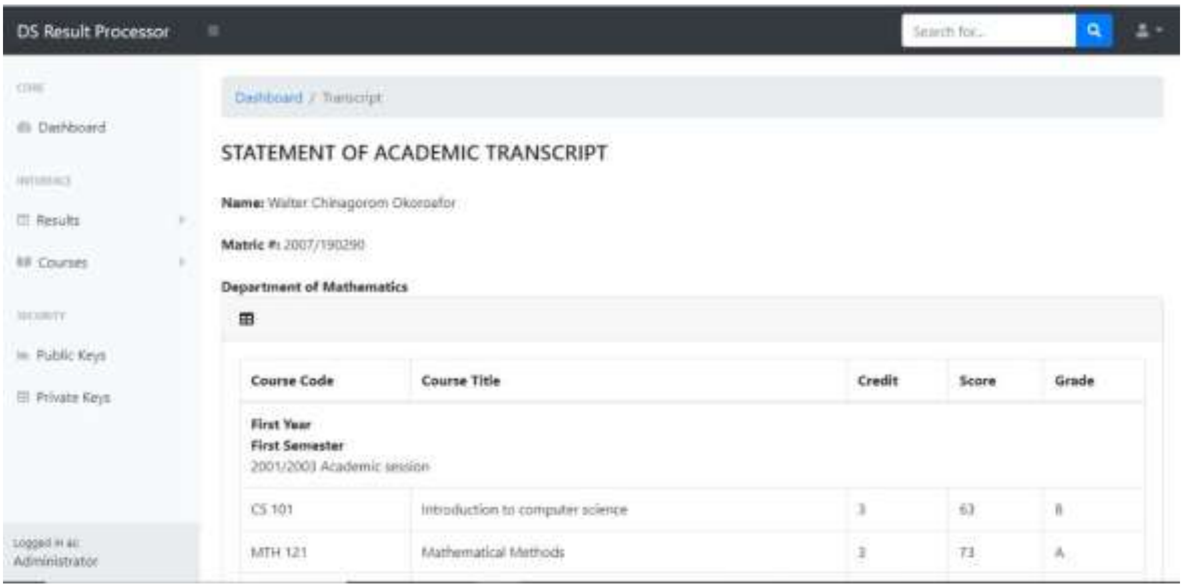
Grade: Automatically generated

Fig-8: Screenshot of Result uploads



Course Code	Course Title	Credit	Score	Grade
First Year **First Semester** 2001/2003 Academic session				
CS 101	Introduction to computer science	3	63	B
MTH 121	Mathematical Methods	3	73	A
MTH 141	Ordinary Differential Equations	2	33	F
GS 101	General Studies	3	43	D
PHY 102	Theory of Heat	3	55	C
First Year **Second Semester** 2001/2003 Academic session				
CS 102	Introduction to file system	3	88	A
STA 111	Probability	2	56	C

Fig-9: Screenshot of Semester Result



STATEMENT OF ACADEMIC TRANSCRIPT

Name: Walter Chinagorom Okoroafor

Matric #: 2007/190290

Department of Mathematics

Course Code	Course Title	Credit	Score	Grade
First Year **First Semester** 2001/2003 Academic session				
CS 101	Introduction to computer science	3	63	B
MTH 121	Mathematical Methods	3	73	A

Fig-10: Statement of academic transcript

7. CONCLUSION

A secure result processing system using digital signature makes information management much more convenient and efficient. This application is meant to facilitate the processing of students' results in tertiary institutions. The system will be capable of storing and retrieving academic records with high speed and accuracy, and presenting useful information to its handlers. Its merits are the reduction in the cost of processing students results, reduction in the time spent in the computation of student's grades and the elimination of duplication of resources in terms of manpower and infrastructure.

The system provides an efficient means of processing, preserving and displaying students' results, academic records and other relevant notices to students. As part of its benefits, it is stress-free and speed-up the processing of students' examination results. Finally, the system is flexible and runs on a web browser. It is reasonably secure, enforces data integrity from the use of a relational database management system, it also minimizes data redundancy and it is user-friendly. With this application, the processing of students' results is automated, thereby reducing processing time and increasing accuracy.

8. REFERENCES

[1] EdTech Hub,. "The Effect of Covid-19 on Education in Africa and its Implications for the Use of Technology", eLearning Africa, Pp. 1-68, 2020. DOI 10.5281/zenodo.4018774

[2] World literacy foundation, "Education and Covid-19 in Nigeria", 2021. https://worldliteracyfoundation.org

[3] E.O. Ukem and E.O Onoyom-Ita, "A software Application for the processing of students' Results", Global Journal of Pure and Applied Science, Vol.17, No.4, pp.487-497, 2011.

[4] Ukem, E and Ofoegbu, "*A Software Application for University Students Results Processing,"* Journal of Theoretical and Applied Information Technology Vol.35, No.1, pp.34-43, 2012. www.jatit.org

[5] U.C. Nnabuko, I.O. Iroegbu, C.I. Ugwuoke, I.E. Eteng, M.C. Okoronkwo, **"**An object based result processing system, International Journal of Natural and Applied Sciences", Vol.8, pp.27-34, 2013.

[6] D.O. Matemilayo, A.K. Raji, F. Oyedepo, "An Online Result Processing and Transcript Generation System: A Case Study of Kwara State Polytechnic", Journal of Research and Development Studies, Vol. 5, No.1, Pp. 1-13, 2017.

[7] A. Schleicher (2020)." The Impact of Covid-19 on Education: Insights from Education at a Glance," pp. 1-31. https://www.oecd-library.org/education

[8] https://searchsecurity.techtarget.com/definition/digital-signature

[9] https://oa.mo.gov/sites/default/files/CC-DigitalSignatures.pdf