International Conference on Information and Communication Technology and Its Applications (ICTA 2016)
Federal University of Technology, Minna, Nigeria
November 28 – 30, 2016

Integration of Parental Alert System into Students Online Payment System

A.O. Isah[1], John K. Alhassan[2], Victor O.Waziri[3], and K.H. Lawal[4]
[1, 2, 3]Department of Cyber Security Science, Federal University of Technology, Minna, Nigeria
[4]Information Technology Services, Federal University of Technology, Minna, Nigeria
[1]ao.isah@futminna.edu.ng, [2]jkalhassan@futminna.edu.ng, [3]victor.waziri@futminna.edu.ng, [4]kenny@futminna.edu.ng

***Abstract*—The introduction of online payment systems for tuition and other fees in institutions across the globe is a great breakthrough of Information and Communication Technology. However, the attendant security risk has become a serious concern to Information Technology experts and the individual institution implementing the system. Of particular concern is the limited knowledge of parents and guardians about the status of their children or wards due to payment issues. This paper seeks to solve this problem by integrating payment transactions alert algorithm into an existing online payment algorithm in order to provide feedback information from the institution authority to parents or guardians by way of a Short Message Service for all payments made or not by their children or wards. By the codified SMS algorithm into the existing payment system, it is able to deliver feedback messages to parents.**

Keywords-online payments; parent, alert system; information security; institutions.

I. INTRODUCTION

Internet technology has rapidly made the world a global village in videos, pictures and audios communications. Exchange of ideas, goods and services are done in a matter of seconds with the application of online systems. The competitive nature of business transactions has forced any company or business outfits to embrace online transactions if a company or an organization wants to continue to be relevant in today's Information Technology world. [1]

Thus, Companies and organizations either private or government engaging in online transactions should be seriously concerned about the security implications of such transactions, security implications consist of the efficiency, confidentiality, reliability, availability. Doing business online is no longer an oddity, but the norm and companies desiring to remain competitive have to maintain some form of online presence. Doing business online is not limited to commercial businesses only, institutions across the globe today engages and rely on online systems for almost their activities including advertisements, application, registrations , academic activities and most importantly, all their payment schedules. The attendant security risk that goes along such payment has become an evolving problem to many institutions world over, it is important to ensure security of payment system in terms of reliability of hardware, software, internet network, power supplies and personnel [2]. Especially, in institution of higher learning where parents and guardians are wholly responsible for the provision of school and tuition fees of their children and wards. Feedback to such parents and guardians is very important in order to monitor the activities of their children in respect of their status since payment of prescribed fees is the first determining factor of studentship. This is the focus of this paper.

A. Essentials of Online Payment

There are some essential elements that must be in place before an online payment system can be established. These are PCI compliance, A payment gateway, A merchant account, ACH payments, and A payment processor. The payment gateway and the merchant account operators must set their operations be in total compliance with Payment Card Industry Data Security Standard (PCI DSS). This PCIDSS was established the Payment Card Industry Security Standards Council to in order to ensure that security information of the card holder is not compromise by cybercriminals. The payment gateway act as the bridge between the merchant and the payment processor and also between customer and the merchant, it ensures that the credit card information is securely passed through. The merchant account is a particular account maintained by a bank through which payments are received from a debit or credit card. The ACH is the Automated Clearing House payments are credit and debit transfers where customers pays for services from their bank accounts. Payment Processor is engaged by merchant to handle all debit and credit transactions on their behalf [3].

B. Parental right to Their Children's Information

It is the right of every parent or guardian to have adequate information about their children or wards [4] in order to have record of their academic and other activities while in the school

This means that parent should be in possession of their children information or data recorded in any medium, including but not limited to handwriting, email, print, etc. that is directly related to a student and maintained by the institution. This may be the students' grades, test scores, evaluations, courses taken, advising records, disciplinary actions, courses, exams and financial records and status.

Behavioural attitudes of students as observed by the institution authority can also form part of the information due for the parent's knowledge.

C. Information security concern

Imbibing the culture of information Security is very critical in parent and institution relationship as regards children and wards in the institution

If there exist some gaps in identifying factors that have significant influence on information security culture adoption. Current information security culture existing literatures have not agreed on principle on what factors needs to be presented to create such environment that promotes the creation of security culture. [5]

The author identifies top critical factors that are necessary for information security culture existence. These factors are: top management support for information security, establishing an effective information security policy, information security awareness, information security training, education, information security risk analysis and assessment, information security compliance, ethical conduct policies, and organization culture.

D. A case study of admission and payment fraud due to lack of parental information

Knowing the status of students in an institution cannot be overemphasized. When parents and guardians do not have adequate information of their children or wards from the institution's authority, students would have field day in all manners of deceitful acts, cheatings, truancy, absenteeism, examination malpractice and other vices on the campus that may have made them to be suspended, rusticated or outright withdrawer from school. Such students may not disclose their situation to their parents are often involved in.

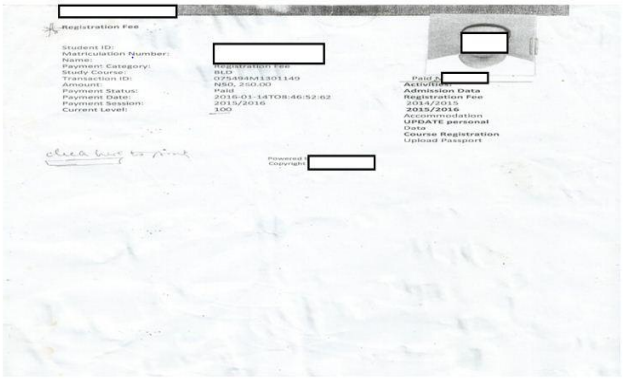

Figure 1. Fake online payment receipt with impassionate candidate (Source: Exhibit from the victim's guardian)

Figure 1 shows fake online payment information generated to defraud a prospective candidate seeking admission into a University (Anonymous) by some admission fraudsters. The candidate whose photograph appeared in figure 1 was assured that his admission was successful and therefore went ahead to release money to the fraudsters to pay the school fees. The student's Identification number that the fraudsters claimed to be for the victim belongs to a genuine and bonafide student of the university whose particulars are shown in figure 2.

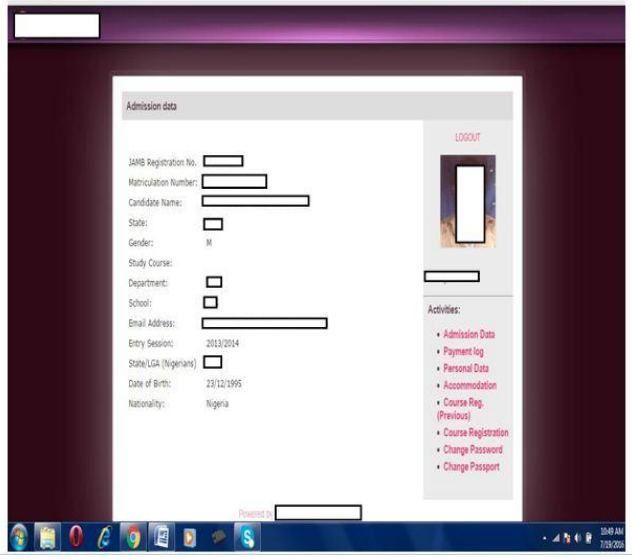

Figure 2. Genuine student being impassionated (Source: e-portal of the Anonymous University)

Figure 2 show the admission data of a genuine student of the anonymous University whose Identification number was used to defraud an unsuspecting candidate shown in figure 1.

E. The implication of figure 1 and figure 2

The victim that was defrauded had thought that he was already a student and he started attending lectures until when the semester examination was approaching and he could not register on the school porter for continuous assessment tests. The Continuous Assessments (CAs) test in this particular University is being conducted by Computer Base Test (CBT). The porter rejected the student's Identification number that the victim entered because, he was never admitted in the first place and so could not be found in the admission data base.

A careful look at figure 1 and 2 revealed some discrepancies in Student ID numbers and other features in the genuine payment receipt (figure 2) with those in the fake payment receipt (figure 1). In the end when the guardian discovered, he was very surprised to know that his ward was not even admitted in the university; this is largely because there was no feedback channel from the University to him to know the true status of his ward.

This is the motivation for this research and hence the author wants to solve this problem by codifying the Short Message Service (SMS) algorithm and integrating into existing institution online payment system.

II. REVIEW OF EXISTING ONLINE PAYMENT SYSTEMS

Exchange of goods and services are mainly based and evaluated in terms of money all over the world today as civilization advances from the primitive era where trade by barter and other forms of methods were used in the exchange of goods and services.

Payment for goods and services is the only authentication that ensures that such exchange has occurred. Several payment methods or systems has been in use such as, Cash

payment, payment through banks, payment through checks, payments by credit transfer, automated clearing house, wire transfer services payments cards.

Researchers have been *extensively* researching on general e-payment systems [6] *observed the rapid* Evolution of payment models, and discovered that there have been numerous payment systems with both new and variations on established models. The author also take a look at some development in this regard, in January of 2012, one of the leading social media company Facebook launched its own payment card which is a normal plastic gift card that allows users to order for small mail delivery to recipients. The card is in addition to Facebook's Gifts feature that was launched in September 2012, the card allows users purchase physical goods such as chocolate, shirts, or flowers for friends, make charitable donations, buy subscriptions, purchase gift cards, and more. this card the author observed, is different from other prepaid competitors because it can be accepted by retailers like: Jamba Juice, Target, Sephora, and Olive Garden, the card can also be integrated with the Facebook mobile app.

[7] Noted that most communication channels are no longer one to one, as other devices in the network also receives data generated by a device in the same network through multicast transmission architecture. This is due to the fast improvement of information and network technologies. These multicast systems that enhance rapid delivery of messages in the network also open up loopholes to snooping attacks in the network. The study submits that one to one encryption is no longer effective for the security of data. So, the authors proposed a novel anonymous multi-receiver encryption, in which receiver's decryption key is fixed. Furthermore, the model provided anonymity of receivers, performance analysis and comparisons with other schemes.

[8] Present a resource efficient reconfigurable hardware implementation of Advanced Encryption Standard (AES) using an object oriented programming language approach on Field Programmable Gate Array (FPGA) for rapid development. In order to boost performance, the authors use Xilinx System Generator that utilizes efficient conventional blocks, having used primitive level approach and customize all the operations in the design of the study.

The common process to purchase anything online is for the prospective customer to visit the merchant's site for the products of interest and select the product [9],. When he is ready to buy those products, he proceeds to provide his shipping and billing address, his payment information (e.g., debit or credit card information) to the merchant. This payment information is sent to the merchant in an encrypted or hashed form so that the merchant cannot obtain it. In order to receive payment for his sale, the merchant forwards the customer's payment information to the payment gateway.

The author observed that in these existing payment systems, information must go through a payment gateway which makes the system vulnerable to hackers and other cyber criminals. The authors therefore developed an approach for online payment which ensures that customer payment information is provided directly to the payment gateway instead of routing the financial information through a merchant. The author discovered some design issues arising from this approach which was also addressed the use of a trusted third party called identity provider, IP, and a commitment scheme called Pedersen commitment. An IP verifies the identity of a merchant before processing the payment. This Pedersen commitment helps to validate transactions.

According to [10], the online payment is an ecosystem which is mostly being targeted by cybercriminals. Since online payment system involves the use credit and debit cards, there will be many stages of interaction for a cycle of transaction this includes consumers and their payment cards, merchants and their point-of-sale (POS) payment systems, the card brands (i.e. Visa, MasterCard, Discover Network, American Express), issuing banks, and card processors. The author explains that end-to-end encryption is needed to maintain the integrity of transactions carried out online, because highly sensitive information is involve in the exchange of yearly traction running into billions of dollars which is very attractive to cybercriminals.

The author submit that software are not save just like the internet that was primarily designed for connection and not necessarily designed for security, although, the author agreed that some software based encryption can remedy the security issue to some extent but cannot give a total guarantee. Like:. AES (Advanced Encryption Standard) which is presently the best encryption available. Hardware security and implementing multi-criterion authentication in mobile platform is also very important measure to be considered in the security of online payment system, [11]. This is achieved by introducing a hardware-protected tamper-resistant security module (TRSM) [10], it ensures that data is protected at the beginning of card transaction before passing through the merchant system,

While the security measures suggested by the author has a far reaching effect on online payment systems, the challenge of feedback information to some stake holders who sometimes are the financier of the whole transaction is still posing a lot of challenges that we seek to solve with this paper. In our case, the stake holders are the parents that are providing the funds for their children's school fees.

[12] The authors did extensive work that highlights the significance of university portal for Nigerian universities, the paper also discussed the best practices that could be put in place to avoid redundancies in future system and processes. Various uses were also highlighted by the authors. Although, information and inquiries tracking was explained as important features of University portal system, however, their paper did not look at payment system which is an integral part of university portal system and was not able to deal in details with the security issues involved in the universities' portal system. This gap in security issues was the focus of this very paper.

A. Example of stages and interfaces involved in a typical institution's online payment system

Figure 3 is the personal data interface where the student enters all his or her relevant Biodata. The students are required to fill in their own name, age, sex, permanent home address, state and local government of origin and most importantly, the name and telephone number of his parent or guardian.

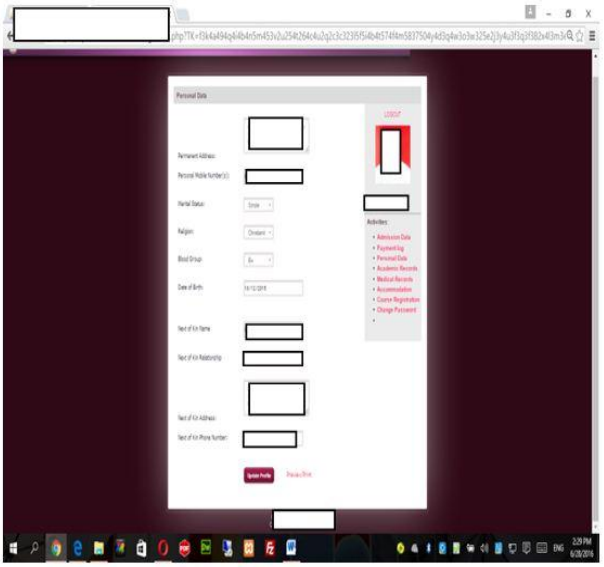

Figure 3. Personal data (Source: e-portal of the Anonymous University)

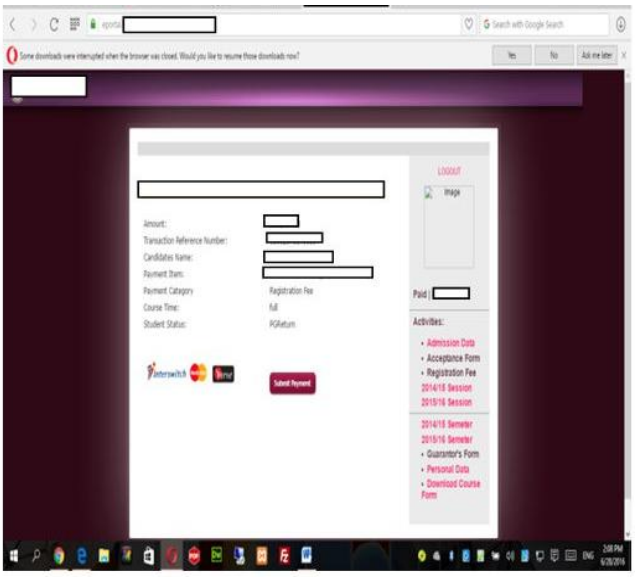

Figure 5. Payment voucher generated by interswitch payment gateway (Source: e-portal of the Anonymous University)

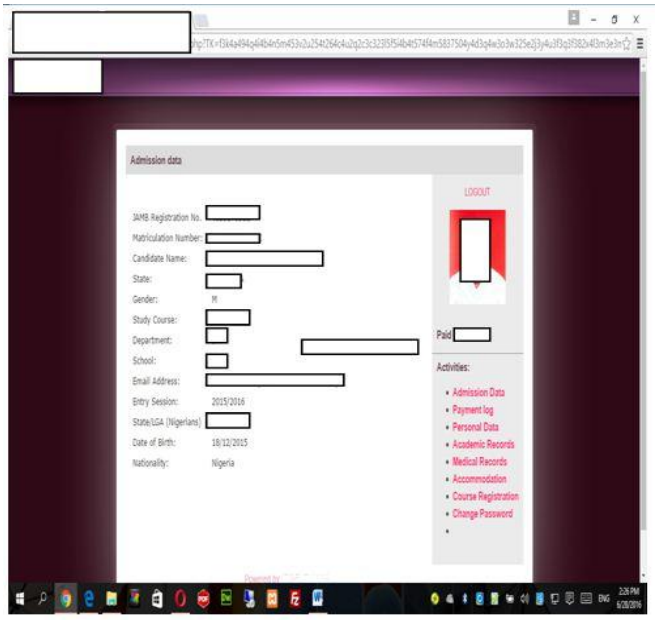

Figure 4. Admission data (Source: e-portal of the Anonymous University)

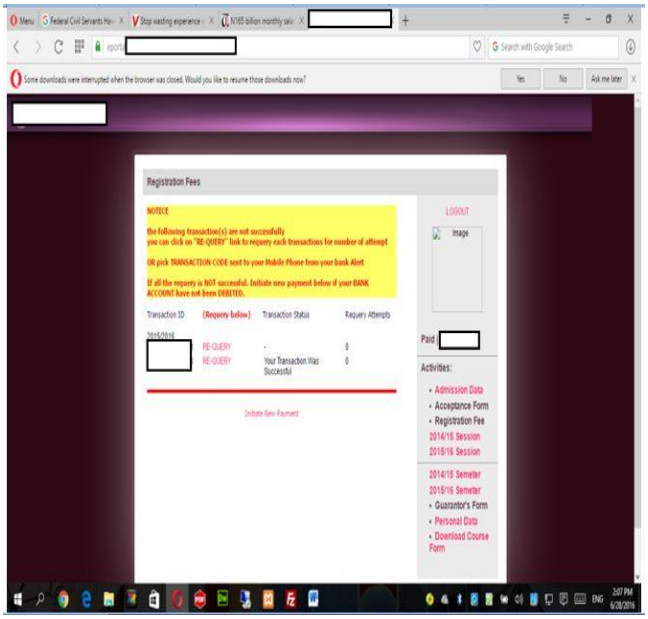

Figure 6. Successful transaction (Source: e-portal of the Anonymous University)

Figure 4 is the admission data interface containing some of student's data again like ; age, sex, state, local government area, student's identification number, course of study, level and department.

Figure 5 is the interface showing the payment agent which generate payment voucher containing the amount of fees required of student to pay. The payment agent for this particular university is the inter-switch; there are several other online payment agents.

Figure 6 is the interface showing payment transactions. When student initiate payment, transaction details are shown whether payment is successful or unsuccessful. At this stage, the transaction details are being sent to the telephone number of the parent or guardian of the student automatically as Short Message Service (SMS). This is where the work of this research comes to function.

III. INTEGRATION OF THE PARENTAL ALERT ALGORITHM INTO THE EXISTING ONLINE PAYMENT SYSTEM

A. The model of institution online payment system

The method used by the authors to solve this problem can be said to be straight forward and simple, but the complexity was in the coding and stringing of the parental SMS alert model into the main existing payment model.

Figure 7 and 8 shows the existing model and the implemented model with the parental alert system respectively.

In the usual online payment system, the focus of the authors which is institution online payment portal, candidates registered on the portal to have students' Identification

number(ID number), or user name and a passwaord, for a freash student, while a returning students who already has an ID or usaul name will have to login with the ID or user namee to access his or her page on the portal on the student's page as were shown earlier by the interfaces of figurs 1 to 6 in the review chapter of this paper, the student then click and navigate to the payment Data link .the payment data interface is linked with any of the payment gateway that the instittution is in collaboration with for the financial transaction proper which in this case, is the paymayment of tuition or any other fees payable to the institution by the concerned student.

The student gets all transaction details from the payement gateway via the institution portal.

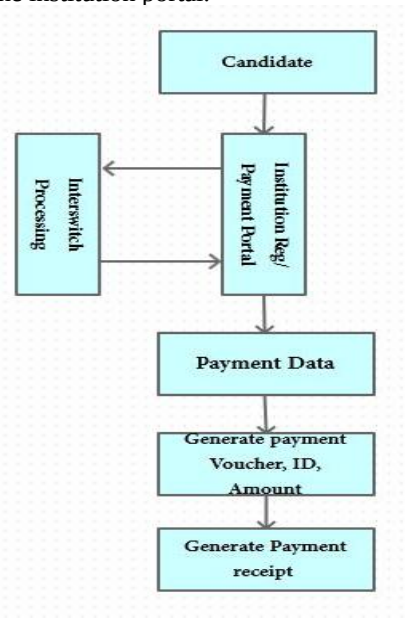

Figure 7. A typical existing Online payment system for an institution

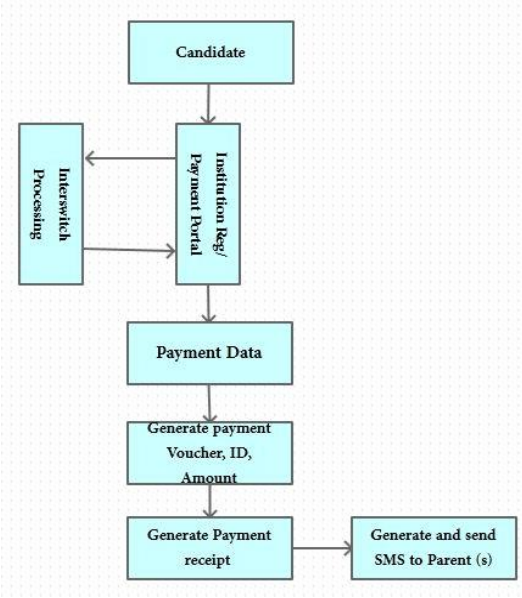

Figure 8. Parental SMS alert system integrated online payment system

Figure 8 is the institution online payment system integrated with the parental alert SMS algorithm. As proposed by this paper, the processes involved in the institution payments is the same as figure 7 but the parental alert system is introduced at the stage of transaction interactions between the student making the payment , the institution payment server and the payment gateway otherwise known as the third party.

B. Algorithm for institution online payment system

```
START
        SELECT TARGET FILE
        ENTER STUDENT ID AND PASSWORD
        GOTO PAYMENT RECORDS
        IF FRESH STUDENT/RETUNING STUDENT
            CHECK STATUS
            GOTO PAYMENT
                IF PAYMENT UNSUCCESSFUL
                   SEND UNSUCCESSFUL_
                      _FEEDBACK TRANSACTION_
                      _DETAILS
                ELSE
                    GOTO PAYMENT
                ENDIF
                IF PAYMENT SUCCESSFUL
                     SEND SUCCESSFUL FEEDBACK_
                       _TRANSACTION DETAILS
                ENDIF
        ENDIF
STOP
```

C. Algorithm for institution online payment system with integrated parental alert system

```
START
  SELECT TARGET FILE
  ENTER STUDENT ID AND PASSWORD
  GOTO PAYMENT RECORDS
  IF FRESH STUDENT/RETUNING STUDENT
        CHECK STATUS
        GOTO PAYMENT
        IF PAYMENT UNSUCCESSFUL
          SEND UNSUCCESSFUL FEEDBACK_
            _TRANSACTION DETAILS
          SEND UNSUCCESSFUL SMS/EMAIL TO_
             _PARENT
        ELSE
          GOTO PAYMENT
        ENDIF
          IF PAYMENT SUCCESSFUL
              SEND SUCCESSFUL FEEDBACK_
                _TRANSACTION DETAILS
              SEND SUCCESSFUL SMS/EMAIL TO_
                _PARENT
          ENDIF
    ENDIF
STOP
```

IV. DISCUSSION

In the existing online payment systems, the actors that are acting on the system are; the candidate (student) making the payment, the university portal administrator, the merchant account bank and the payment processor as explained in figure 7. All transaction details and feedbacks are only to candidate, the parent is not among the actors interaction with the system directly. The normal payment algorithm as shown in (b), does not accommodate external actor. The integrated alert algorithm (c) has now extended some aspect of the transaction information to the parent or guardian in a way that when even the student make an unsuccessful attempt to pay any fees, the feedback will be sent to parent(s), when the payment is successful, the parent is also aware.

V. CONCLUSION AND RECOMMENDATIONS

In this research, an automated instant alert message (SMS) into the online payment system was designed and tested. The payment portal delivers information to parent and guardians the very moment payments were made by their children or ward. This allows the parent or guardian to keep track of the status of their children or wards in the institution. The SMS alert algorithm that instantly provides payment information to parents was introduced to existing system as one of the contributions to the security features of students' online payment. This paper utilized the integrated SMS codes as a metric to compare other reviewed papers that were not able to integrate parental automated feedback mechanism in their works

It is recommended that students' examination result could also be sent to the parent or guardian through this integrated system. Also the institution authority should verify the data of the parents or guardian entered in the personal data page on the portal shown in figure 3. There are license software the institution's authority can use to verify the authentic owner of telephone numbers supplied by the students.

REFERENCES

[1] D. Montague,"Essentials of Online Payment Security and Fraud Prevention," John Wiley& Sons, Inc., Hoboken, NewJersey, 2011.

[2] Nasashi Nakajima, "Payment system technologies and functions: innovations and developments," Reitaku University, Japan, 2011, pp. 89.

[3] R. Meyer, "10 excellent online payment systems" http://sixrevisions.com/tools/online-payment-systems, 2012.retrieved 22.02 2016

[4] California Department of Education, "Information for parents and family members about becoming involved in the education of their children" http://www.cde.ca.gov/ls/pf/pf/, June 2016.

[5] M. A. Alnatheer, Information Security Culture Critical Success Factors 2015 12th International Conference on Information Technology - New Generations King Abdul-Aziz City for Science and Technology (KACST) Riyadh, Saudi Arabia

[6] J. R. Ross, "Electronic payments industry explodes with new developments in everything from social media-marketed gift cards to city-sponsored debit/ID cards," http://www.mozido.com/electronic-payments-industry-explodes-with-new-developments-in-everything-from-social-media-marketed-gift-cards-to-city-sponsored-debitid-cards/ 2013 Retrieved 22.07.2016

[7] L. Harn, C.C. Chang, and L. W. Hsiao, "An Anonymous Multi-Receiver Encryption Based on RSA" International Journal of Network Security 15(4) 307-312. www.ijns.femto.com, 2013.

[8] A. Aziz and N. Ikram, "Hardware Implementation of AES-CCM for Robust Secure Wireless Network" Available online at http://www.academicjournals.org/JEAPS

[9] S. Pant, "A Secure Online Payment System", University of Kentucky, 2011, pp 13, 51.

[10] M. steven elefant, "secure online payment system requires end-to-end encryption", http://searchsecurity.techtarget.com/magazinecontent/secure-online-payment-system-requires-end-to-end-encryption retrieved july 23, 2016.

[11] P. Smita and D. Noumita, "Study and Implementation of Multi-Criterion Authentication Approach to Secure Mobile Payment System", International Journal of Engineering Science and Advanced Technology, (IJEAST), 2014, 3(3), 117-122.

[12] S. M. Abdulhamid, and I. Idris, "Design Evaluation of Some Nigerian University Portals: A Programmer's Point of View". GESJ: Computer Science and Telecommunications, 2010 5(28), 21–28.