3-TIER E-COMP: A NOVEL E-COMMERCE MANAGEMENT PORTAL BASED ON SECURED SDLC APPROACH

[1]Okafor N. I, [2]Okafor K.C, [4]Udeze C.C. & [5]Onwusuru I. M.
[1,2,4&5]Electronic Development Institute, ELDI-NASENI
Awka-Nigeria.

[3]Ugwoke F. N.
[3]Computer Science Department
Michael Okpara University
Umudike, Nigeria

ABSTRACT

In today's business world, there is an urgent need to develop a new approach for customer to business owner transactions securely. This research develops, implements, and discussed a novel 3 – Tier E-Commerce Management portal. This makes online business very flexible and secured on the part of business owners and customers. Our proposed system seeks to replace the conventional E-commerce models on the internet today. We argue that process logic manipulation using Secured Software Development Life Cycle (SSDLCM) on Ecommerce platform is a promising scheme for studying and understanding script processing on the new web paradigms. In this research, we define security calculus for 3 Tier EComP with the aim of eradicating SQL injection possibilities as well as exploiting Software as a service in a dynamic Ecommerce domain. Also, we developed a new access hierarchy for E-commerce comprising of Application layer users, designated administrator and super administrators in the 3 – Tier EComP. We developed a new encryption scheme based on XAMP MD5 Random Curve Cryptography (XMD5 – RCC) running on Secure Socket Layer (SSL) which protects the user and administrators on the Ecommerce platform. The result of encryption scheme randomly generates and secures the login details dynamically on the server during the authentication and authorization phases. The programming was accomplished with PhP, and MySQL Server. The overall methodology as detailed in the body of the work could serve as good template for application developers and other researchers.

Keywords: E-Commerce, XMD5-RCC, SSL, Platform, SSDLCM, Software, Service

1. INTRODUCTION

The advent of the internet has now created a new dimension to service provisioning in the context of buying and selling. In this regard, online shopping, e-commerce, e-banking, and the newest era of cloud computing has brought about a dramatic change in business transactions. However, owing to current market competition by organizations and private enterprises, customers are becoming ever more demanding both in terms of the quality of goods and services that they receive while seeking for flexibility in business transactions. In particular, their interaction with these organization/administration in ensuring a good transaction platform will be highly dependent on how well designed such a platform is integrated. Since the internet plays a major role in e-commerce platforms, it is important to solve security vulnerability problems in such online platforms.

According to [1], online retailing is a form of electronic commerce which allows consumers to directly buy goods or services from a seller over the Internet using a web browser. Alternative names are: e-shop, e-store, Internet shop, web-shop, web-store, online store, and virtual store [1]. An online shop evokes the physical analogy of buying products or services from a retailer or shopping center.

This process is referred to as business-to-consumer (B2C) online shopping. In the case where a business entity buys from another business entity, the process is called business-to-business (B2B) online shopping. Statistics have shown that eBay and Amazon are the largest online retailing corporations in the world (both based in the United States). Generally, in Nigeria today, the traditional way of offline business transactions presents a lot of limitations to prospective customers and business owners. Some of these include security vulnerabilities, improper account auditing, poor inventory documentation, inflexibility and poor service delivery, etc. A new paradigm has emerged with the advent of E-commerce and its associated technologies to address these issues.

Since the issue of security vulnerability will always constitute enormous constraint for numerous users on the E-commerce domain, the need for a re-engineered e-commerce platform with a robust encryption algorithm that will allow access and protect the users and the web owners will gain wide acceptance. This follows the fact that secure communication is an intrinsic requirement of today's world of on-line transactions. Whether exchanging financial, business or personal information, good authentication, data integrity and confidentiality needs to be guaranteed. In this work, a 3-Tier management framework optimized for E-commerce which employs an improved SDLC as well as a highly secured cryptographic algorithm for access security is proposed to solve the above problems at various hierarchies. The framework comprising of the User Front-end, business/integration logic and the server backend will help to deal with the issue of scalability, and technologies such as PhP script and Web services facilitate the development of distributed 3Tier EComP application.

1.2. Our Contribution

The main objective of this work is to develop a 3-Tier EComP framework with a cryptographic algorithm for SQL injection cancelation as well as maintaining access hierarchy in the platform. The security mechanism uses an enhanced cryptography (256bits message digest algorithm), to address vulnerability issues in our developed e-commerce platform. Our specific objective is to demonstrate user interaction on the 3-Tie EComP using the architectural framework as shown in figure 5 and figure 6. Other features of the application are outlined in section 4.4. The rest of the paper is organized as follows: Section 2 presents a brief description of the traditional e-commerce Security Vulnerabilities cases. This is followed in Section 3 by developments in the e-commerce model/landscape and related works. In Section 4 is presented the proposed 3Tier E-commerce Platform with its operational mechanism. System models and flowchart designs are presented in Section 5, The implementation methodology is discussed in Section 6 and the conclusion in Section 7.

1.3. E-commerce Security Vulnerabilities

In this section selected security vulnerabilities in e-commerce models as well as other web applications are identified and discussed below,

(i) SQL Injection

The author in [4] explained that SQL injection refers to the insertion of SQL meta-characters in user input, such that the attacker's queries are executed by the back-end database. Typically, attackers will first determine if a site is vulnerable to such an attack by sending in the single-quote (') character. The results from an SQL injection attack on a vulnerable site may range from a detailed error message, which discloses the back-end technology being used, or allowing the attacker to access restricted areas of the site because he manipulated the query to an always-true Boolean value, or it may even allow the execution of operating system commands. SQL injection techniques differ depending on the type of database being used.

For instance, SQL injection on an Oracle database is done primarily using the UNION keyword [5] and is much more difficult than on the MS SQL Server, where multiple queries can be executed by separating them with the semi-colon [6]. In its default configuration, MS SQL server runs with Local System privileges and has the 'xp_cmdshell' extended procedure, which allows execution of operating system commands. The most publicized occurrences of this vulnerability were on the e-commerce sites of Guess.com [7] and PetCo.com [8]. SQL injection vulnerabilities have also been discovered in shopping cart software such as the VP-ASP Shopping Cart [9], Generic Free Shopping Cart [10],[11], [12], etc.

(ii) Price Manipulation

This is a vulnerability that is almost completely unique to online shopping carts and payment gateways.
In the most common occurrence of this vulnerability, the total payable price of the purchased goods is stored in a hidden HTML field of a dynamically generated web page. An attacker can use a web application proxy such as Achilles [13] to simply modify the amount that is payable, when this information flows from the user's browser to the web server. Similar vulnerabilities have also been found in third-party software such as in the 3D3 Shop Factory Shopping Cart [14], where price and item-related information was stored in client-side cookies, which could easily be manipulated by an attacker. As shown in [15], Smartwin Technology's CyberOffice Shopping Cart 2.0 could be attacked by downloading the order form locally, and resubmitting it to the target server with the hidden form fields modified to arbitrary values.

(iii) **Buffer overflows**

It has been reported that, buffer overflow vulnerabilities are not very common in shopping cart or other web applications using Perl, PHP, ASP, etc. From the structure of the web site and the visible hyperlinks there would have been no way to determine that there existed the 'admin' directory within the 'func' sub-directory below the main Document Root. Multiple buffer overflows were also discovered in the PDG Soft Shopping Cart [16], which potentially allowed the attacker to execute code of his choice by over-writing the saved return address. In these applications, error pages can serve as a valuable source for critical information.

(iv) Cross-site scripting

The Cross-site Scripting (XSS) [17] attack is primarily targeted against the end user and leverages two factors viz: the lack of input and output validation being done by the web application. In this case, the trust placed by the end-user in a URL that carries the vulnerable web site's name. By crafting a URL, which contains this JavaScript, a victim can be social engineered into clicking on it, and the script executes on the victim's system. A typical XSS attack URL would look like this:

http://www.vulnerablesite.com/cgi-bin/search.php?keywords=&lt;script>alert("OK")&lt;script>.

In this case, when the victim clicks on this link, a message box with the text "OK" will open up on his system [18]. In most cases, the attacker would craft the URL in order to try and steal the user's cookie, which would probably contain the session ID and other sensitive information. The JavaScript could also be coded to redirect the user to the attacker's website where malicious code could be launched using ActiveX controls or by utilizing browser vulnerabilities such as those in Internet Explorer or Netscape Navigator. However, the JavaScript can also be used to redirect the user to a site that looks similar to the original web site and requests the user to enter sensitive information such as his authentication details for that web site, or his credit card number or social security number [19] [20].

(v) Remote Command Execution

The most devastating web application vulnerabilities occur when the CGI script allows an attacker to execute operating system commands due to inadequate input validation. This is most common with the use of the 'system' call in Perl and PHP scripts. Using a command separator and other shell metacharacters, it is possible for the attacker to execute commands with the privileges of the web server. For instance, Hassan Consulting's Shopping Cart allowed remote command execution [21], because shell metacharacter such as |;& were not rejected by the software. In another case, Pacific Software's Carello Shopping Cart [22] had a vulnerable DLL that allowed the execution of remote commands due to directory traversal attacks that could be carried out using a specially crafted URL.

2. RELATED WORKS

The paper in [2] review the current state of internet banking in Nigeria vis-à-vis privacy protection issues and bring to fore, use of one time password, card-based authorization codes, transaction password and digital certificate as some other options to addressing customer privacy in online banking and transaction in Nigeria. The work in [3] discussed the traditional e-payment model in the context of five entities: the client, the merchant, the issuer, acquirer, the payment system service provider, and layer violating security measures has been found not to be realistic given the developments and trends in e-payment systems and their environments .

The author in [23] presented Privacy and Security Issues in E-Commerce while examining privacy from social psychological, organizational, technical, regulatory, and economic perspectives. In e-commerce context, the work concluded that privacy and security are still ongoing research problems. The work in [24] presented a design of a new security protocol using hybrid cryptography algorithm. The work observed that security attacks compromises the security in network and web applications. It further buttressed that various symmetric and asymmetric cryptographic algorithms have been proposed to achieve the security services such as Authentication, Confidentiality, Integrity, Non-Repudiation and Availability. The authors noted that at present, various types of cryptographic algorithms provide high security to information on controlled networks but these algorithms are required to provide data security and users authenticity. To improve the strength of these security algorithms, their work then focused on a new security protocol for on line transaction can be designed using combination of both symmetric and asymmetric cryptographic techniques.

This protocol provides three cryptographic primitives (such as integrity, confidentiality and authentication) which will be achieved with the help of Elliptic Curve Cryptography, Dual-RSA algorithm and Message Digest MD5. In this regard, the protocol uses Elliptic Curve Cryptography for encryption, Dual-RSA algorithm for authentication and MD-5 for integrity. They concluded that this new security protocol is optimized for better security with integrity using a combination of both symmetric and asymmetric cryptographic techniques.

From [25], the author reported that the major problem faced by consumers in an online transaction is security. From survey report, it is obvious that most reports acknowledged that transaction based on e-commerce has been constrained by security. In addition, consumers are concern about their privacy especially when their personal information are required to facilitate transaction besides, potential risks are also posed to those using credit cards to make purchase online. Secured system is needed to enhance online shopping since consumers cares for their privacy and security. Furthermore, the author [25] opines that online shopping paves way to fraudulent act and unworthy credit orders which is also attributed to unsecured services. Trust also plays an essential role on consumer's choice for online purchase. Roca et.al. [26] Reported that trust in online businesses determines consumers' willingness to engage in online business. In another study [27], it was pointed out that security, protection policy and as well as reliabilities of companies are major barriers to online shopping.The work in [28] opines that oonline shopping could become predominant source of shopping method, if the barriers associated with insecurity, trust and customer's protection are tackled. The paper highlighted the limitations associated with e-commerce transaction in Libya and proposes relevant steps towards overcoming these constrains. Snapshots of existing online shopping/Ecommerce Models are captured in Figures 1a and 1b.

vpasp
Shopping Cart Software
"VP-ASP has allowed me to go from $0 to over $1 million in sales per year."
View Online Demo

Figure 1a: (Source: http://www.vpasp.com)

Figure 1b: (Source: http://www.jumia.com.ng)

Following our survey, the work generalized the following as the limitations of existing E-commerce Platforms, viz:
1. Most of the platforms lack the benefits of software as a service generally.
2. Most of these models lack multi-tier security functionality to address vulnerability issues.
3. In most of the systems, their modularization design lacks the capability for audit trails and logs for transaction computations
4. Integration is highly capital intensive as they are designed devoid of cloud computing ideology.
5. Heavy and complex cart models makes for inflexibility making difficulty in user experience
6. Open e-commerce models are highly vulnerable such as *http://www.amazon.com/, http://www.alibaba.com/ etc.*

This research now proposed a new framework for online transaction involving secured modularization via roles and privileges as well as password random encryption which will eradicate the existing security vulnerabilities while offering flexible and user friendly online interaction

2.1 3-TIER ECOMP Framework Dynamics

The dynamics of a 3-TIER EComP developed in this work is shown in figure 4 while figure 5 depicts the conceptual model with the various entities and attribute subsystems well represented. In this research, leveraging the limitations of existing works in literature, figure 4 was developed with Microsoft Visio 2003 where a new concept of Secured SDLC with reuse model was exploited in developing the online business transaction processes. The framework design combined all the basic functionalities of the e-commerce models while improving on the security and process architecture as shown in figure 5. On the secured web page, on lunching the URL, after the user validation from XMD5-RCC, the tier-1 user interface generates a user process which facilitates negotiation and buying activities. Basic orders are often sent electronically through the IP cloud. At the remote server location, the XMD5-RCC verifies incoming request in the password file. Also, the XMD5-RCC completely eliminates all the vulnerability scenarios discussed previously. Basically, the customers who have duly registered can place an order of products and services they have transacted based on administrators role privilege assignments. Depending on the status of the designated administrator, the connection bridge of the instance connector always interacts with the server process as well as the background processes. The connection can be idle, open, or closed depending on decision of the business owner.

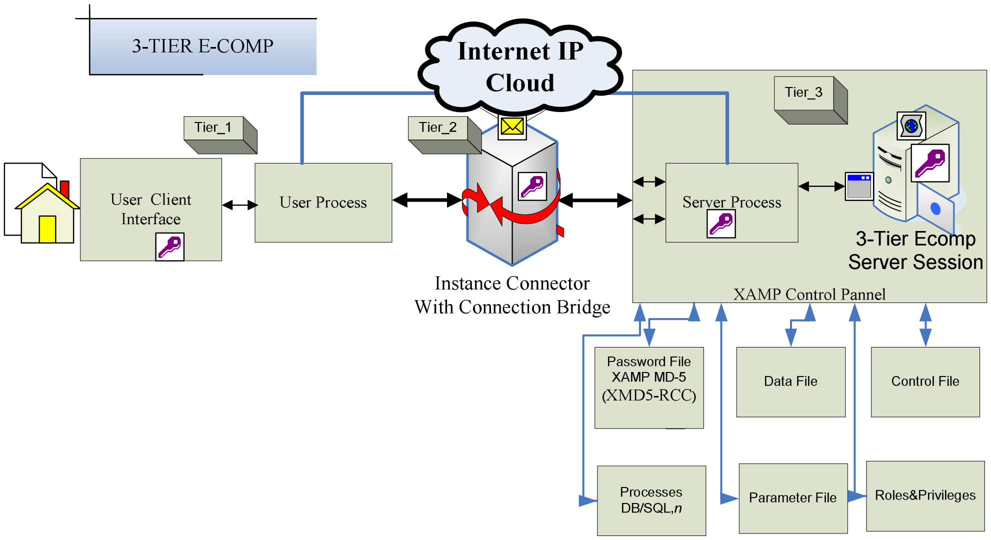


Figure 3: Proposed 3-TIER E-Commerce logical Framework

2.2 Process Architecture Integration

The process architecture is a three tier model comprising of the client interface, the business logic and the server backend with database support. This is logically depicted in Figure 3. Also, in the Cloud 3-Tier EComP server architecture, the logic instance is a collection of the background processes and the shared memory allocated by the server during the normal operation.

There are three major structures in our Cloud 3-Tier EComP process architecture viz:

(i) Process structures: User process and server process

The user process is the connection to the Cloud3-Tier EComP via encrypted password authentication while the Cloud creates server process that handle the requests of users or client processes that connect to the logic instance. This server process is in dedicated server mode where each user process has its own server process.

(ii) Background Structures/ processes

In cloud 3-Tier EComP, a set of background processes for the logic instance that interacts with each other and with the server to manage memory structure, asynchronously perform I/O to write data to the server are enabled. They provide parallelism for better performance and reliability. Every transaction in the Cloud 3-Tier EComP forms a session based on structured query language patterning for user connection into the server via the logic instance as discussed above. In all cases, the PHP programming was used in the server integration (Apache) as shown in our research outcomes.

3. DESCRIPTION OF THE 3-TIER ECOMP OPERATIONAL MECHANISM

We now synthesized Figure 3 into a decomposed model with the discussion on its operational mechanism presented in this section. In our developed model shown in figure 5, the principal actors include:

1) Cloud Super Admin Authentication Sa
2) Assigned Admin, Aarg
3) Cloud Customers Cc1,Cc2,............Ccn
4) Cloud Audit
5) Shopping/Order/billing

Figure 4 depicts the proposed 3-TIER ECOMP operational model which was developed after the SaaS paradigm deployable in a public cloud. In its architecture, the super admin Sa on the cloud portal assigns low level administrators Aa1..............Aan, that coordinates and assists numerous registered cloud customers Cc1,Cc2,............Ccn.. From user perspective, the customers who are legitimately registered can be authenticated using XMD5-RCC in context. The ac-cess control authentication and encryption algorithm intelligently grants or denies access to 3-Tier EComP domain based on the logon or log off status of the designated or assigned administrators Aa. The status control serves to enforce discipline on either AA or Cc, while the cloud audit stores the cloud logs for all AA and Cc.

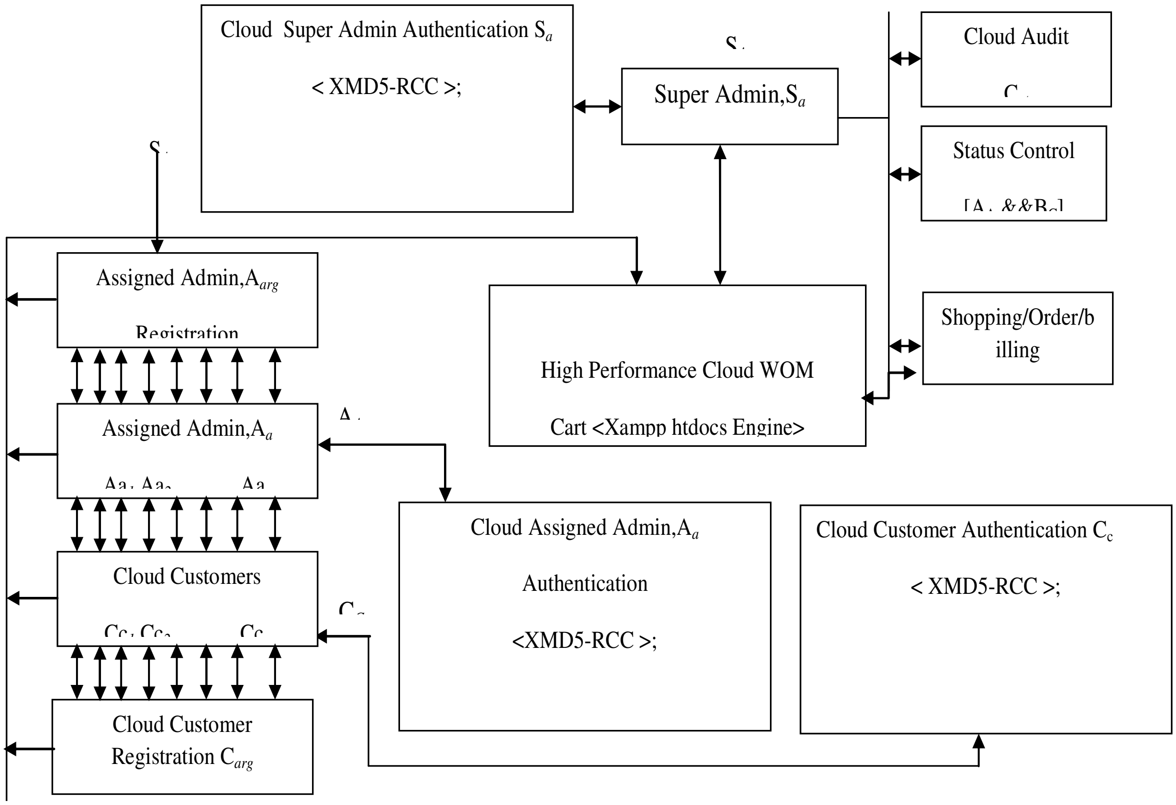

Cloud Super Admin Authentication S_a
< XMD5-RCC >;
Super Admin,S_a
Cloud Audit
Status Control
Shopping/Order/billing
Assigned Admin,A_{arg}
Registration
High Performance Cloud WOM Cart <Xampp htdocs Engine>
Assigned Admin,A_a
Cloud Assigned Admin,A_a
Authentication
<XMD5-RCC >;
Cloud Customer Authentication C_c
< XMD5-RCC >;
Cloud Customers
Cloud Customer Registration C_{arg}

Figure 4: Architectural Model of 3-Tier EComP

4. ADVANTAGES OF THE PROPOSED SYSTEM

The 3-TIER ECOMP facilitates efficient scheduling which improves cost accounting and saves a company's cash as-set. Other advantages include:

1) Security modularization based on encryption is another functional feature of our 3-TIER ECOMP.
2) Supports latest version of MySQL database for cloud back end support
3) Offers close source web order cart behaviour as well as an all-in-one ecommerce solution.
4) It allows the super administrator to create successful online store with unlimited number of products while al-lowing for smart management of the work order store.
5) The application is less prone to a cross-site scripting vulnerability, SQL injection and other vulnerability issues faced by other systems.
6) Other feasible features include: Browse products by manufacturer, category or price, transaction tracking and auditing is guaranteed, supports industry standard image extension such as jpg, png, gif, automatic resize/resample of the uploaded images, support for raw flash movies as product images, modular design, easy to add/remove/create custom modules for your shop, skinable template driven interface, user-friendly admin control panel for the administrators, it can be integration with leading payment-processing companies

5. METHODOLOGY

Secured System Development Life Cycle (SSDLC) was leveraged to realize 3-Tier EComP. In our approach, the adopted SSDLC consists of the following steps:

1. System Conceptualization: System Conceptualization refers to the consideration of all aspects of the targeted business function or process, with the goals of determining how each of those aspects relates with one another, and which aspects will be incorporated into the system.
2. Systems Analysis: This step refers to the gathering of system requirements, with the goal of determining how these requirements will be accommodated in the system. Extensive communication between a sample sized customer and the developers was carried out.
3. System Design: After all the requirements were gathered and analyzed, we then identified in detail how the system will be constructed to perform necessary tasks (ie. task set re-engineering). More specifically, the System design phase is focused on the data requirements (what information will be processed in the system?), the software construction (how will the application be constructed?), and the interface construction (what will the system look like? What standards will be followed?). Using encryption tool in XAMP control panel, we implemented XMD5-RCC. The Random curve connotes the 256bits encryption pattern on all registered user and the trimming of the PhP codes for injection, phishing, etc vulnerabilities.
4. Coding: The programming implementation was the step was carried out. This involved the creation of the system software as depicted in figure 4 and figure 5 respectively. Requirements and systems specifications from the System Design step are translated into machine readable computer code via the CS4 Integrated development environment (IDE). As shown in figure 6, phases 3, 4 and 5 took care of all the security considerations before the system testing.
5. Testing: As the software is created and added to the developing system, testing is performed to ensure that it is working correctly and efficiently.

The testing generally focused on two areas: internal efficiency and external effectiveness. The goal of external effectiveness testing is to verify that the software is functioning according to system design, and that it is performing all necessary functions or sub-functions. The goal of internal testing is to make sure that the computer code is efficient, standardized, and well documented. Testing can be a labour-intensive process, due to its iterative nature. Figures 6 show the software engineering mapping for SSDLC with various feedback routines

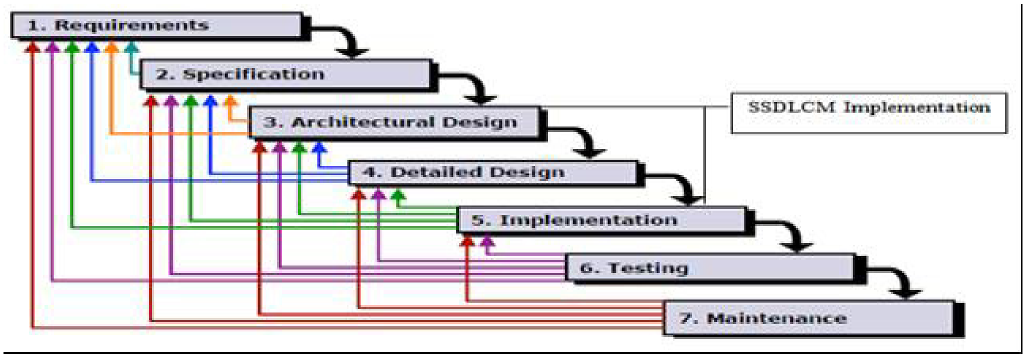


Figure 5: A Flow for SSDLC Model with Feedback

5.1. Implementation Results and Analysis

Design Specifications

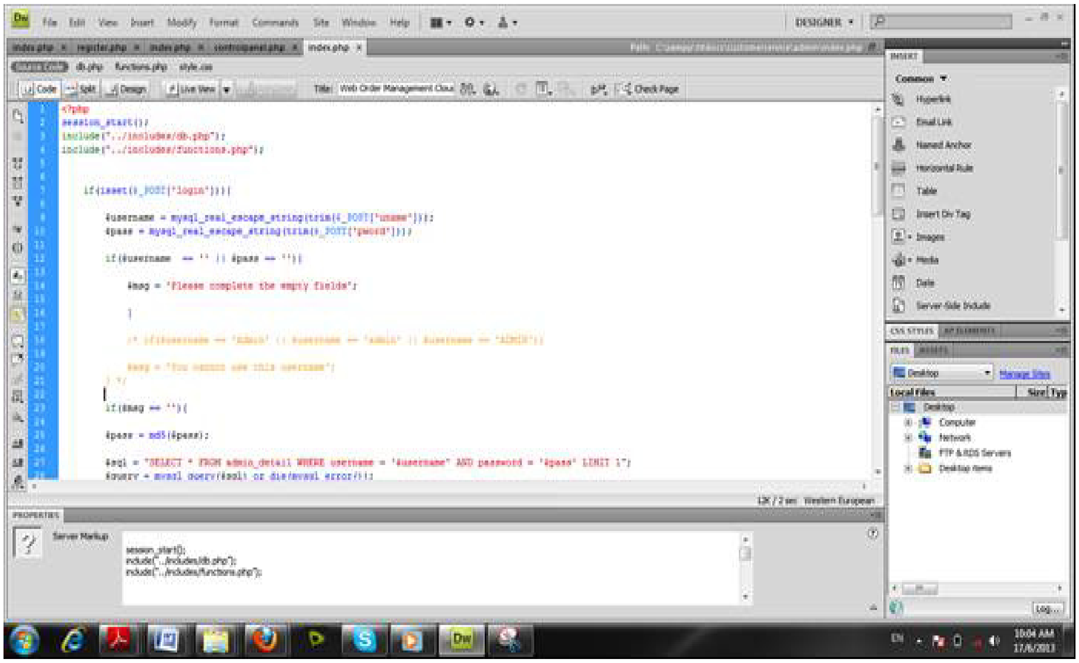
Following the discussions on Figure 3, Figure 4 and Figure 5, the reengineered 3-TIER ECOMP SaaS design focused on the three layers: Access layer and logic instance connection and the server side database. In this context, the connection instance was configured for the SaaS application. The logic instance and the background processes facilitate connection to the server. The reengineered 3-Tier EComP developed in this research was accomplished with the following system specifications below comprising of the software and hardware requirements.

The prototype deployment server system requirements are as follows: i) Memory requirements: 1 GB for the logic instance (connection manager) ii) Disk space requirements: 1.5 GB of swap space, 400 MB of disk space in the /tmp directory, Between 1.5 GB and 3.5 GB for the CloudMesh software, 1.2 GB for the preconfigured database (optional), 2.4 GB for the flash recovery area (optional) and Operating system requirements.

Others include adequate temporary space, 64-bit versus 32-bit issues, Windows 7/Server 2007 and Linux Redhart, OS patch level, System packages, System and kernel parameters, Sufficient swapping, Nonempty XAMP htdocs_HOME.

Development Environment - CS 4 Dreamweaver Editor

For the IDE, the adobe Dreamweaver is a development environment with a visual editor that supports Web technologies such as CSS, JavaScript, and various server-side scripting languages and frameworks including ASP (ASP JavaScript, ASP VBScript, ASP.NET C#, and ASP.NET VB), ColdFusion, Scriptlet, and PHP. Figure 7 shows the integrated development environment for 3-TIER ECOMP design. It was configured with My SQL server in XAMP control panel which have integrated supports for Apache server and MySQL database. In this work, entire program using the design phase of the SDLC Resuse model was tested using different data and system platform.



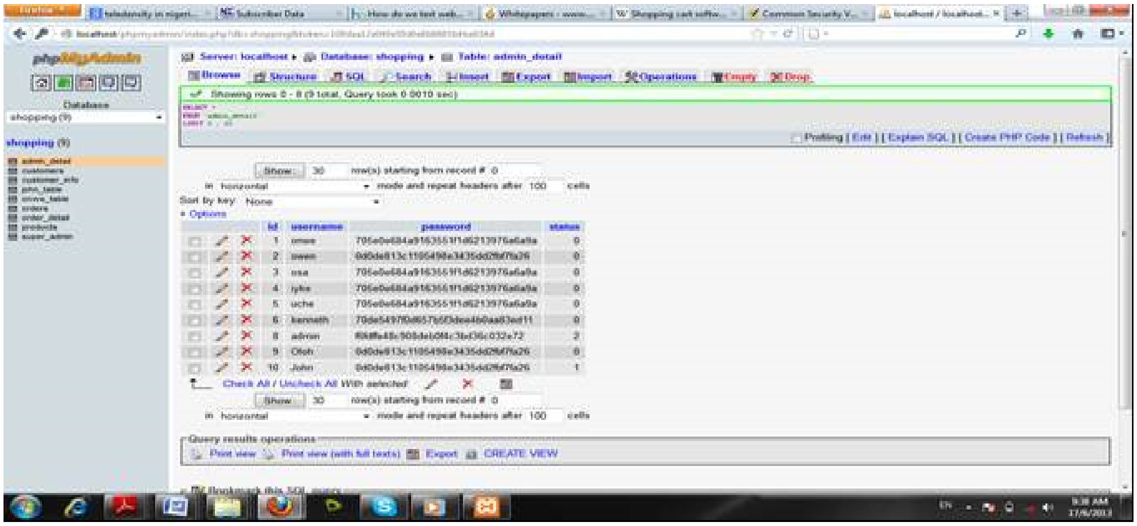
```
<?php
session_start();
include("../includes/db.php");
include("../includes/functions.php");


  if(isset($_POST['login'])){

      $username = mysql_real_escape_string(trim($_POST['uname']));
      $pass = mysql_real_escape_string(trim($_POST['pword']));

      if($username  == '' || $pass == ''){

          $msg = 'Please complete the empty fields';

          }

          /* if($username == 'Admin' || $username == 'admin' || $username == 'ADMIN'){

          $msg = 'You cannot use this username';
      } */

      if($msg == ''){

      $pass = md5($pass);

      $sql = "SELECT * FROM admin_detail WHERE username = '$username' AND password = '$pass' LIMIT 1";
      $query = mysql_query($sql) or die(mysql_error());
```

```
session_start();
include("../includes/db.php");
include("../includes/functions.php");
```

Figure 6: CS4 Adobe Dreamweaver IDE for 3-TIER ECOMP

5.1.2 Testing and Integration

Before the proposed 3-Tier EComP was made fully operational, it was thoroughly tested on a local host server while debugging and ensuring syntax errors giving rise to successful compilations while testing with real user test data. After several tests, the reliability of the system was ascertained while making the necessary documentation. In this research, figure 5 was designed is designed to run the high performance datacentre network infrastructure comprising of a Microtic server with localhost Dell Inspiron 1525 window7 running Apache, MySql and CS4 adobe dreamweaver IDE. Figure shows the XMD5-RCC Authentication (256bits) per encrypted user. Figure 8 shows XMD5-RCC activities as the id number 10 is the only active administer for authenticated users.



Showing rows 0 - 8 (9 total, Query took 0.0010 sec)

Show 30 row(s) starting from record # 0 in horizontal mode and repeat headers after 100 cells

Sort by key: None

id	username	password	status
1	omwe	705e0e684a9163551f1d6213976a6a9a	0
2	owen	0d0de613c1105498e3435dd2f6f7fa26	0
3	osa	705e0e684a9163551f1d6213976a6a9a	0
4	iykis	705e0e684a9163551f1d6213976a6a9a	0
5	uche	705e0e684a9163551f1d6213976a6a9a	0
6	kenneth	70de5497f0d657b5f3dea4b0aa83ed11	0
8	admin	f0kfffe48c905deb0f4c3bd36c032e72	2
9	Oloh	0d0de613c1105498e3435dd2f6f7fa26	0
10	John	0d0de613c1105498e3435dd2f6f7fa26	1

Figure 7: MySQL Database based on high bit MD5 Authentication for Assigned Administrators

6. DISCUSSION AND RESULTS

6.1. Implications of 3-TIER EComP

The implication of using the same password for more than one secure online account in the developed 3-TIER EComP is that if the one password be compromised, the entire ac-counts will be in jeopardy. Online transactions will be carried out in all the accounts with ease in a cashless ecommerce portal.

The findings in existing works reveals that for open e-commerce platforms, social engineering and impostors can easily misguide unsuspecting customers and so, new ecommerce models must be secured to reduce vulnerabilities.

Since the discipline to regularly change the password is lacking, it means that if the password is compromised, the account could be accessed for considerable periods of time. Again, this is not good for our cashless economy.

The practice of using personally meaningful numbers, one's own name etc as passwords is a serious malpractice that if not discouraged, will jeopardize the ecommerce cashless platform.

7. CONCLUSION AND FUTURE WORK

This research has discussed a generic framework for e-commerce portal. The Study observes that existing e-commerce/online web systems are highly vulnerable to attacks as a result of the architectural and implementation methodologies used. With the current e-presence ideology, it is expected that over 90% of business owners will be offering their transactions via these platforms while facilitating comfort and flexibility on the part of customers. This work then proposed a XMD5-RCC vulnerability approach in the architectural framework leveraging SaaS cloud computing paradigm. We argue that with the structure of the encryption scheme, adequate security is guaranteed for online transactions.

At this stage, our only constraints are on the manageability and safe keeping of the XMD5-RCC password by the customers. Though the encryption is very sensitive, the use of birthdays, anniversary dates, telephone numbers, identity numbers, personal names, etc is discouraged by the XMD5-RCC.

Since the current design of Password Selection Mechanism (PSM) does not help the user choose a good password, we recommend the feedback augmented PSM such as the progress bar that dynamically reflects the quality of the password, with a textual indicator that is updated at thresholds. Future work will address these issues and while presenting the formal model for the XMD5-RCC presented in this work as well as deploy the application on a cloud computing infrastructure for production usages.

REFERENCES

[1] Wikipedia: Online Shop-ping:http://en.wikipedia.org/wiki/Online _Shopping

[2] B. K. Olorisade, R. A. Azeez, Addressing Privacy in Online Banking and Transactions in Nigeria's Cashless Society" Towards a Cashless Nigeria, tools and strategy. In the Proc. NCS 2012,Uyo pp 47-50.

[3] E. E. Odokuma, G. M. M. Obi, "A Model Of A Pragmatic Secure E-Payment System" Towards a Cashless Nigeria, tools and strategy. In the Proc. NCS 2012,Uyo pp 47-50.

[4] K. K. Mookhey, "Common Security Vulnerabilities in e-commerce Systems"

[5] http://www.symantec.com/connect/articles/common-security-vulnerabilities-e-commerce-systems

[6] SQL injection and Oracle, Pete Finnigan, http://www.securityfocus.com/infocus/1644

[7] Advanced SQL injection, Chris Anley http://www.nextgenss.com/papers/advanced_sql_injection.pdf

[8] News article on SQL Injection vulnerability at Guess.com http://www.securityfocus.com/news/346

[9] Jeremiah Jacks at work again, this time at PetCo.com http://www.securityfocus.com/news/7581

[10] http://www.vpasp.com/?utm_expid=653874

[11] https://www.juniper.net/security/auto/vulnerabilities/vuln9773.html

[12] http://www.igeneric.co.uk/ig-shopping-cart.html

[13] Security Focus :http://www.securityfocus.com/bid/9301/discuss

[14] Achilles can be downloaded from http://achilles.mavensecurity.com/

[15] Security Focus: http://www.securityfocus.com/bid/6296

[16] . Security Focus:http://www.securityfocus.com/bid/1733

[17] Security Focus:http://www.securityfocus.com/bid/1256

[18] CERT Advisory Malicious HTML HTML Tags Embedded in Client Web Requests http://www.cert.org/advisories/CA-2000-02.html

[19] Yusuf Uzunay, "Design and Implementation of An Unauthorized Internet Access Blocking System Validating The Source Information In Internet Ac-cess Logs", M.sc, Sep.2006.

[20] Security Focus http://www.securityfocus.com/infocus/1745)

[21] Definition of 'phishing' http://www.webopedia.com/TERM/p/phishing.html

[22] Security Focus: http://www.securityfocus.com/bid/3308.

[23] Security Focus: http://www.securityfocus.com/bid/5192

[24] . Mark S. Ackerman and Donald T. Davis, Jr., "Privacy and Security Issues in E-Commerce" Review chapter for the New Economy Handbook (Jones, ed.), in press.

[25] S. Subasree And N. K. Sakthivel, " Design Of A New Security Protocol Using Hybrid Cryptography Algorithms", IJRRAS 2 (2), February 2010 Subasree & Sakthivel, Design of a New Security Protocol.

[26] Udo G.J., "Privacy and Security Concerns As Major Barriers for E-commerce: A Survey Study," Information Management & Computer Security, vol. 9, no.4, pp.165-174, 2001.

[27] 84. Roca J.C., Garcia JJ., de la Vega JJ., "The Importance of Perceived Trust, Security and Privacy in Online Trading Systems," Information Management & Computer Security, vol. 17, no. 2, pp. 96-113, 2009.

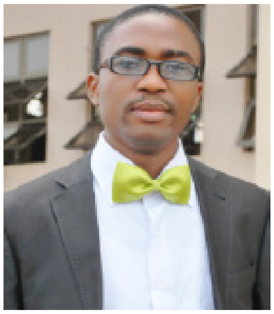
[28] Chen Y-H., Barnes S., "Initial Trust and Online buyer behavior," Industrial Management & Data Systems, vol. 107, no. 1, pp. 21-36, 2007.

[29] Abdulghader.A.Ahmed.Moftah, Siti Norul Huda Sheikh Abdullah, Hadya.S.Hawedi, " Challenges Of Security, Protection And Trust On E-Commerce: A Case Of Online Purchasing In Libya" International Journal Of Advanced Research In Computer And Communication Engineering, Vol. 1, Issue 3, May 2012

Authors Profile

Engr. Nneka Ifeyinwa. Okafor holds B.Eng. in Computer Engineering from Enugu State University of Science and technology, (ESUT) while currently pursing her M.Sc in Digital Electronics and Computer Engineering from University of Nigeria Nsukka,(UNN). She has Oracle 10g Expert Certification. Currently, she works as a Research Engineer II in Electronics Development Institute, Awka. She is a graduate Member of Nigerian Society of Engineers, Awka Chapter and a member of IAENG. Her research interests are on Software Graphics, Animation Modelling, Database Management and System Analysis. Contact: nekkydear2003@yahoomail.com

Engr.(Dr). Udeze Chidiebele .C. received his B.Eng, M.Sc and PhD in Electronics and Computer Engineering from Nnamdi Azikwe University, Awka, Nigeria. He holds his PhD in computer and control systems engineering. He is a Senior R & D Engineer with Electronics development Institute Awka, Nigeria. He works with Electronic Development Institute, Awka under National Agency for Science and Engineering Infrastructure, Nigeria as an R&D Engineer. He is a member of Nigerian Society of Engineers and has his COREN registration. His current research interest is on DataCenter networks, Cloud Computing and Applications, WSN Technologies, and Control Systems Engineering. Email: udezechidiebele@yahoo.com



Engr. Okafor Kennedy C. is a Systems Architect and R&D Consultant. He holds B.Eng in Electrical Electronics Engineering, (ESUT), M.Eng in Digital Electronics and Computer Engineering, (UNN) while currently pursuing his PhD in Electronics Engineering at University of Nigeria Nsukka. He works with Electronic Development Institute, Awka under NASENI, Nigeria as a Senior R&D Engineer. He has various vendor certifications including Cisco Certified Network Associate, A+, and Server+. He is a member of NSE, IEEE, NCS, and IAENG. He has many publications while his areas of interest include Network Design & Cloud Computing Design&Management, Middleware Technologies, Embedded Systems &VLSI, Enterprise-Wide Systems, Database Technologies, Application Development, Security, WSN Technologies, and Project Management. He can be reach via Email: *arissyncline@yahoo.com,* +2348034180668

Engr. Dr (Mrs.) Ugwoke, Fidelia Ndidi received her B.Eng in Computer Science and Engineering from Enugu State University of Science and technology (ESUT), Obtained MLS in Library and Information Science from Ebonyi State University, Abakaliki Ebonyi State (EBSU).She also holds a Ph.D in Computer Science from Ebonyi State University, Abakaliki Ebonyi State. Currently, she is a Lecturer I staff in Computer Science Department, Michael Okpara University of Agriculture, Umudike Abia State, Nigeria. She belongs to a number of professional bodies including NSE, NCS and CPN. She has many publications to her credit. E-mail address: ndidi.*ugwuoke@gmail.com,*+2348037174398, +2348116700273.