www.ijecs.in
International Journal Of Engineering And Computer Science ISSN:2319-7242
Volume 2 Issue 6 June, 2013 Page No. 1727-1738

ISCLOUD V.1.0: AN INTERACTIVE CLOUD SHOPPING CART BASED ON SOFTWARE AS A SERVICE COMPUTING MODEL WITH HYBRID CRYPTOGRAHIC ALGORITHM

Okafor KC, Udeze CC, Okafor CM

Electronics Development Institute, Awka, National Agency for Science and Engineering Infrastructure, NASENI Federal Ministry of Science and Technology, Nigeria.

Abstract

Online Shopping Cart Access Control presents a new security concerns for cloud computing applications in general. Contemporarily, these solutions (Online Shopping Cart) now leverages on Cloud Computing Software as a Service, Platform as a Service, and infrastructure as a Service delivery models viz: Cloud Web Hosting,Cloud Hosting, Reseller Web Hosting, Business Web Hosting, Dedicated Instances, and Web Hosting Business solutions. Shopping Carts can now be dedicated to providing customers with the most reliabile web order as well as web hosting services in real time. Candidate models like X-cart, S-cart Now by Amazon Services,Cubecart,Zen Cart, aspdotnetstorefront,WDL and Mal's E-commerce among others leverages on the potential benefits associated with today's e-commerce. Most e-Commerce proposals in literature lacks adequate security integration and trust, making online transactions vulnerable at large. This paper presents ISCloud V.1.0, an interactive cloud shopping cart based SaaS with Hybrid Cryptography in which a fast high-quality symmetric-key and public key encryption algorithm is used for access authentication. In context, the generated symmetric key is used for integrity encryption for the authentication access in ISCloud V.1.0 SaaS model. For service trust by customers,a Secured Socket layer Certificate authority (domain validation) will be acquired from a trust Certificate Authority at its deployment. The design methodology and service framework is detailed in the body of this paper. PhP,XAMPP Apache and MySQL is used for a prototype implementation.

Keywords: Cloud Computing,Service Delivery Models,Security integrations, Symmetric key,Encryption

INTRODUCTION

Secure Electronic Transaction (SET) is a standard protocol for securing credit card transactions over insecure networks, specifically, the Internet [1]. SET is a set of rules and regulations that enable users to perform financial transactions through existing payment system over insecure wireless network (internet) in much secure and reliable manner [2].

According to [3], Online shopping or 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 [3]. 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).

In this work, SET is an application to provide various security services as confidentiality, data integrity and authenticity for all electronic transactions over the internet. Interestingly, every Online shopping solution however, places a stringent requirement on SET owing to trust and reliability.

Generally, 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 way of thinking has emerged with the advent of hybrid cryptographic online web based order

management system that not only solves the above problems, but entrenches stronger authentication encryption scheme at various hierarchies.

The main objective of this work is to develop an intelligent web portal (SaaS) with a hybrid cryptographic encryption algorithm for trust access control in online business transactions. This paper seeks to make a novel contribution by formulating a SaaS model for a customer centric business solution that improves customers satisfaction and retention, while modelling the hybrid security algorithm for access control for a super administrator Sa_1, Assigned Administrators A_a and Cloud customers C_c in ISCloud V.1.0.

This research will help offline enterprise organizations involved with large scope business transactions to fasten response to customer needs, access customers and make larger sales from any location in the world, enabling overall system flexibility while maintaining security. It will also enable staff and owners of companies, businesses or institutions, etc to appreciate the importance of online customer care in enhancing cost savings, while increasing revenue and sales with accurate sales tracking and management. Besides, describing cloud computing offerings and delivery model will facilitate a good understanding of ISCloud V.1.0 Service offerings in our context.

A. SaaS 3-TIER ARCHITECTURE OF WEB APPLICATION

Before discussing on the security and implementation model of ISCloud V.1.0, we first discussed about the 3-tier logical view architecture of web applications as outline in [4]. The well illustrated in figure 1

1) The User interface tier: This layer forms the front end of the web application. It interacts with the other layers based on the inputs provided by the user.

2) The Business logic tier: The user request and its processing are done here. It involves the server side programming logic. It forms the intermediate layer between the user interface tier and the database tier.

3) The Database tier: It involves the database server. It is useful in storage and retrieval of data.

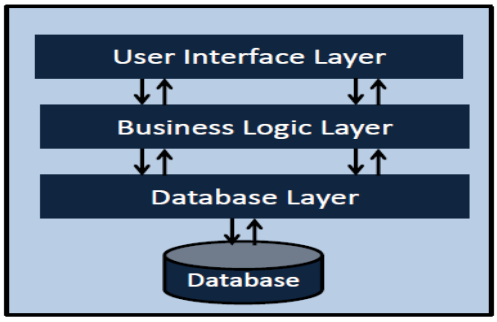

Figure 1. Web 3-tier architecture [4]

B. CLOUD COMPUTING SERVICE SETS

Before presenting the system model and its security algorithm formulations, a review on cloud computing will be carried out. A cloud taxonomy is shown in figure 2 which shows the layered architecture of cloud computing. According to [5], cloud computing is not a completely new concept for development and operation of web applications, however it allows for the most cost-effective development of scalable web portals on highly available and fail-safe infrastructures. From [6], everything is now perceived to be a service (XaaS) like Software as a Service (SaaS), Platform as a Service (Paas),Infrastructure as a Service (IaaS), Hardware as a service (HaaS), ([Development, Database, Desktop] as a Service), Framework as a Service (FaaS), Business as a Service (BaaS), Organization as a Service (OaaS), etc. In this work, user access layer security architecture forms the major basis for the ISCloud V.1.0 implementation. This application thus conforms to the SaaS paradigm. Figure 1 shows typical cloud layered architecture. As depicted in figure 1, cloud architecture is the design of software applications that uses internet-accessible on-demand service. Based on model of deployment, a cloud can be classified as public, private, community, or hybrid [5, 7, 8, 9,] as shown in Figure 1.

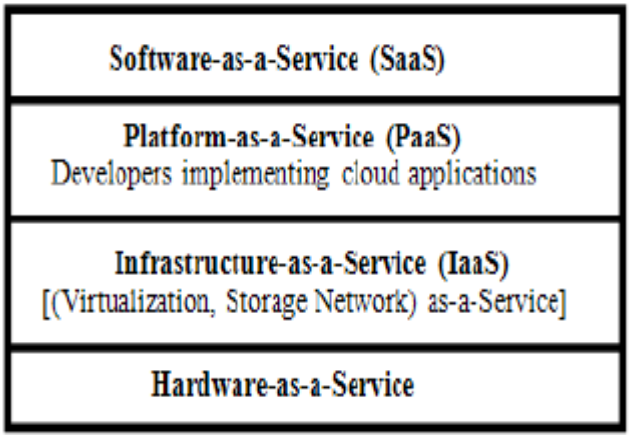

Figure 1: Cloud Layered Architecture

C. GENERALIZED CLOUD COMPUTING SECURITY ISSUES

Cloud security [10] evolved from information security and includes a wide set of controls, technologies, and policies used to protect the associated infrastructure, applications, and data of cloud computing. The authors in [11] noted that security issues relating to cloud computing can either be security issues experienced by end users or security issues experienced by cloud suppliers. In general, cloud computing security fall into three general categories [11]: Contractual or Legal Issues, Compliance, and Privacy and Security. These issues were articulated in their work viz:

i. For the contractual and legal issues, end users and cloud vendors have to negotiate about liability, end-of service, and intellectual property.
ii. They must agree about the degree of liability of each party when data has been compromised or lost.
iii. They must also agree on how the applications and data can be returned to the client when the contract is not renewed.
iv. Cloud providers must also take into consideration how the records are kept because there certain statutes which require electronic records to be kept in a certain way.
v. Public institutions which are utilizing the cloud and storage must consider the laws regarding record keeping.
vi. With regards to data and storage to the cloud, there are various rules and regulations which must be adhered to and Cloud computing vendors must be able to enforce their users to adhere to such rules and regulations easily.
vii. There must also be data recovery and business continuity plans so that service can be maintained in case of emergency and/or disaster. The clients must be able to review such plans so that they will have an assurance that their information is safe with the cloud providers.
viii. Cloud computing providers must be able to provide audit trails and logs and such items must be maintained, secured properly, and accessible in case a forensic investigation takes place.
ix. The cloud data centers must be maintained in such as a way that they adhere to compliance requirements.
x. In terms of privacy and security, every user must have his identity management system in order to access computing and information resources. The cloud providers must be able to provide such system to their users. Aside from securing access of data through the internet, the cloud providers must be able to assure their users that the physical servers are all secured and that access to such servers and even user data are all documented. They must also ensure that users can easily access their applications and data when and where they need them.
xi. In the production environment, cloud suppliers must be able to secure applications by implementing procedures not only for packaged or outsourced application but also an application security must be implemented.
xii. Lastly, cloud vendors must be able to secure every critical data like credit card numbers by masking and restrict access to such data. Credentials and digital identities must be secured just like any data which cloud providers produce or collect from their users cloud activities

On the other hand, the authors in [12] explained that security architecture is a cohesive security design, which addresses the requirements (e.g. authentication, authorization, etc.) and in particular the risks of a particular environment/scenario, and specifies what security controls are to be applied as well as where the design process should be reproducible.

D. ENCRYPTION AND CRYPTOGRAHPHY

i. ENCRYPTION

Definition: This fundamentally consists of scrambling a message so that its contents are not readily accessible while decryption is the reversing of that process [13]. These processes depend on particular algorithms, known as ciphers. Suitably scrambled text is known as cipher text while the original is referred to as the plain text.

Readability is neither a necessary nor sufficient condition for something to be plain text. It's also quite possible to construct a mechanism whose output is readable text but which actually bears no relationship to the unencrypted original. A key is used in conjunction with a cipher to encrypt or decrypt text. The key might appear meaningful, as would be the case with a character string used as a password, but this transformation is irrelevant, the functionality of a key lies in its being a string of bits determining the mapping of the plain text to the cipher text [14].

ii. CRYPTOGRAPHY

Definition: *Cryptography* is the study of mathematical techniques related to aspects of information security such as confidentiality, data integrity, entity authentication, and data origin authentication. Cryptography is not the only means of providing information security, but rather one set of techniques.

According to [14], protecting access to information for reasons of security is still a major reason for using cryptography. It's also increasingly used for identification management systems, for authentication and for non-repudiation. This is particularly important with the growth of the Internet, global trading and other activities [15]. The identity of e-mail and Web users is trivially easy to conceal or to forge, and secure authentication can give those interacting remotely confidence that they're dealing with the right person and that a message hasn't been forged or changed. In commercial situations, non-repudiation [15] is an important concept ensuring that if, say, a contract has been agreed upon one party can't then renege by claiming that they didn't actually agree or did so at some different time when, perhaps, a price was higher or lower. Digital signatures and digital timestamps are used in such situations, often in conjunction with other mechanisms such as message digests and digital certificates [14].

Of all the information security objectives in literature, the following four forms a framework upon which the others will be derived: (1) privacy or confidentiality (2) data integrity ; (3) authentication ; and (4) non-repudiation .

1. *Confidentiality* is a service used to keep the content of information from all but those authorized to have it. *Secrecy* is a term synonymous with confidentiality and privacy. There are numerous approaches to providing confidentiality, ranging from physical protection to mathematical algorithms which render data unintelligible.
2. *Data integrity* is a service which addresses the unauthorized alteration of data. To assure data integrity, one must have the ability to detect data manipulation by unauthorized parties. Data manipulation includes such things as insertion, deletion, and substitution.
3. *Authentication* is a service related to identification. This function applies to both entities and information itself. Two parties entering into a communication should identify each other. Information delivered over a channel should be authenticated as to origin, date of origin, data content, time sent, etc. For these reasons this aspect of cryptography is usually subdivided into two major classes: *entity authentication* and *data origin authentication*. Data origin authentication implicitly provides data integrity (for if a message is modified, the source has changed).
4. *Non-repudiation* is a service which prevents an entity from denying previous commitments or actions. When disputes arise due to an entity denying that certain actions were taken, a means to resolve the situation is necessary. A cryptographic trust procedure can be employed to address such disputes. The fundamental goal of cryptography is to adequately address these four areas in both theory and practice.

The authors in [14] made an attempt to propose a Hybrid security protocol well depicted in figure 3, though was not applied in any software implementations. In their work, the new Security Protocol has been designed for better security, but combines of both the Symmetric and Asymmetric Cryptographic Techniques, hence providing Cryptographic Primitives such as Integrity, Confidentiality and Authentication.

In their model, a given plain text can be encrypted with the help of Elliptic Curve Cryptography, ECC and the derived cipher text can be communicated to the destination through any secured channel. Simultaneously, the Hash value is calculated through MD5 for the same plain text, which already has been converted into the cipher text by ECC. This Hash value is encrypted with Dual RSA and the encrypted message of this Hash value also sent to destination. In their judgment, if intruders try to hack the original information from the encrypted messages, he might capture both the encrypted messages of plain text and the hash value and try to decrypt these messages to get original one. But since the hash value is encrypted with Dual RSA, and the plain text encrypted with ECC, it will then be impossible to extract the plain text from the cipher text, as such, the message can be communicated to the destination with highly secured manner.

Again, the new hash value is calculated with MD5 for the received originals messages and then it is compared with decrypted hash message for its integrity. This is the primitive feature of this hybrid protocol.

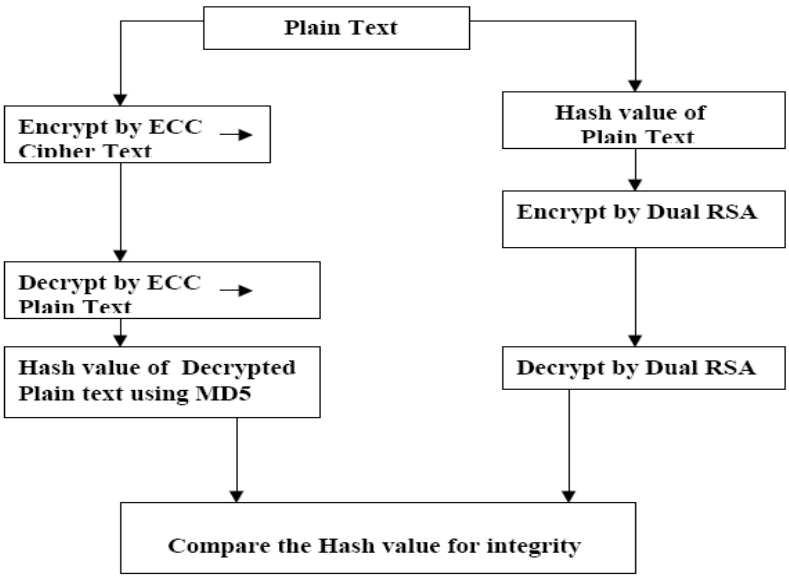

Figure 3 : Hybrid Protocol Architecture [14]

As shown in the figure 3, the Symmetric Key Cryptographic Techniques such as Elliptic Curve Cryptography and MD5 are used to achieve both the Confidentiality and Integrity. The Asymmetric Key Cryptography technique, Dual RSA used for Authentication. The above discussed three primitives can be achieved with the help of this Security Protocol Architecture in [14].
Since the security objective of this paper is to reinforce security by ensuring access control and authentication in ISCloud V.1.0 SaaS model, an addition of a digital signature algorithm called HCA Digital Signature Rand_256bits, will be formulated in this paper.

1. ISCLOUD V.1.0 HIGH LEVEL MODEL

The dynamics of a cloud shopping cart model developed in this work is shown in figure 4 with the various entities and attribute subsystems well represented. A discussion on its operational mechanism is presented in figure 4.

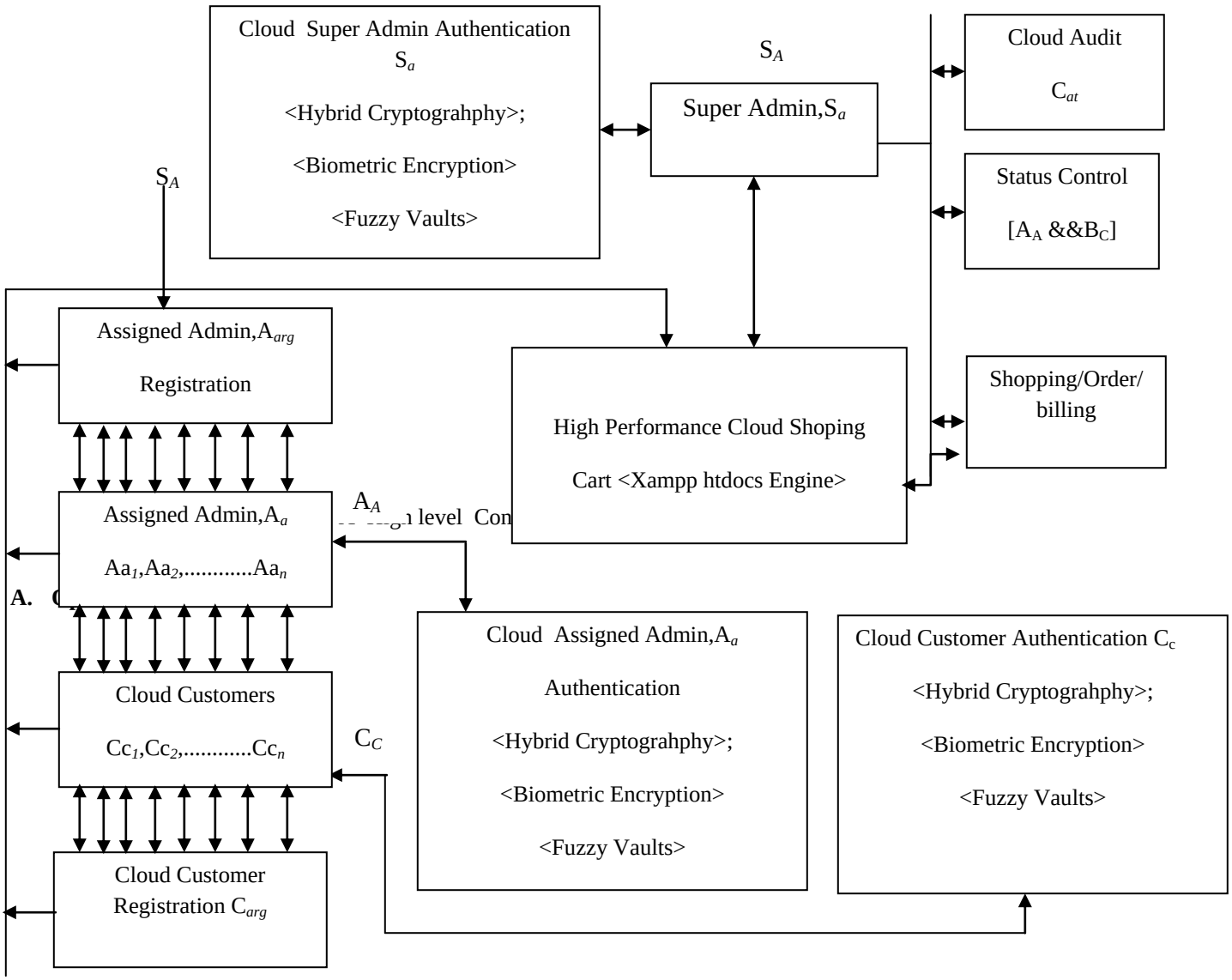

Figure 4 depicts the proposed cloud shopping cart model (ISCloud V.1.0) which was developed after the SaaS paradigm. In its architecture, the super admin S_a on the cloud portal assigns low level administrators Aa_1.....Aa_n, that cordinates and assists numerous registerd cloud customers Cc_1,Cc_2,.....Cc_n. From user perspective, the cloud customers who are legitimately registered can be authenticated using Hybrid Cryptograhphy in context. Other authentication algorithm for future work in a proposed online cloud repository system will includes Biometric Encryption and Fuzzy Vaults [16, 17]. The access control authentication and encryption algorithm intelligently grants or denies access to ISCloud V.1.0 shopping domain based on the logon or log off status of the assigned administrators *Aa*. The status control serves to enforce discipline on either A_A or C_c, while the cloud audit stores the cloud logs for all A_A and C_c.

In this paper, the developed cloud shopping cart model (ISCloud V.1.0) is designed to run on our proposed High Performance Datacenter Model [14] in our earlier work, tested on a localhost Dell Inspiron 1525 window7 running Apache, MySql and CS4 adobe Dreamweaver IDE.

HYBRID CRYPTOGRAPHY SECURITY ALGORITHM

As studied in literature, some of the known and widely used public-key algorithms includes:The Diffie–Hellman, RSA algorithms, the Cramer–Shoup cryptosystem, ElGamal encryption,and Elliptic Curve Cryptography [18,19,20,21,22]. Basically, Public-key algorithms

are most often based on the computational complexity of hard problems, often from number theory (Eg. RSA is related to the integer factorization problem, Diffie–Hellman and DSA are related to the discrete logarithm problem and more recently, elliptic curve cryptography security algorithm is based on number theoretic problems involving elliptic curves). Because of the difficulty of the underlying problems, most public-key algorithms involve operations such as modular multiplication and exponentiation, which are much more computationally expensive than the techniques used in most block ciphers, especially with typical key sizes. Consequently, a proposed Hybrid Cryptographic Algorithm (HCA) which uses a fast high-quality symmetric key encryption (256bits wide) leveraging on existing proposals to protect and control access in figure 2. Each time a valid customer or administrator log's in with his/her authentication details which is encrypted with CA, the exact hybrid digital signature is computed. These algorithms are required to provide reinforced security and user's authenticity. The HCA was implemented in ISCloud V.1.0 for better security using a combination of both symmetric and asymmetric cryptographic techniques as studied in existing works.

A. HCA Digital signatures

A cryptographic primitive which is fundamental in authentication, authorization, and no repudiation in HCA is the digital signature. The purpose of a digital signature is to provide a means for an entity to bind its identity to a piece of information. The process of signing entails transforming the message and some secret information held by the entity into a tag called a signature. A generic description follows below.

Consider $M*S$ consists of all pairs (m,s) where $m \in M$, $s \in E$, called the Cartesian product of *M* and *S*. *Now let,*

- *M* is the set of *login details* which can be signed.
- *S* is a set of elements called signatures, possibly binary strings of a fixed length.
- S_A is a transformation from the *login details* set *M* to the signature set *S*, and is called a *signing transformation* for entity *A*. The transformation S_A is kept secret by *A*, and will be used to create signatures for messages from *M*.
- V_A is a transformation from the set $M * S$ to the set {*true*; *false*}. V_A is called a *verification transformation* for *A's* signatures, is publicly known, and is used by other entities to verify signatures created by *A*.

Definition- The transformations S_A and V_A provide a *digital signature scheme* for *A*. This could be called *digital signature mechanism* whose formulation is shown below.

Given digital signature scheme $M = \{m1, m2, m3\}$ and $S = \{s_1, s_2, s_3\}$. The right side of Figure 5 shows a signing function S_A from the set *M* and, the left side the corresponding verification function V_A.

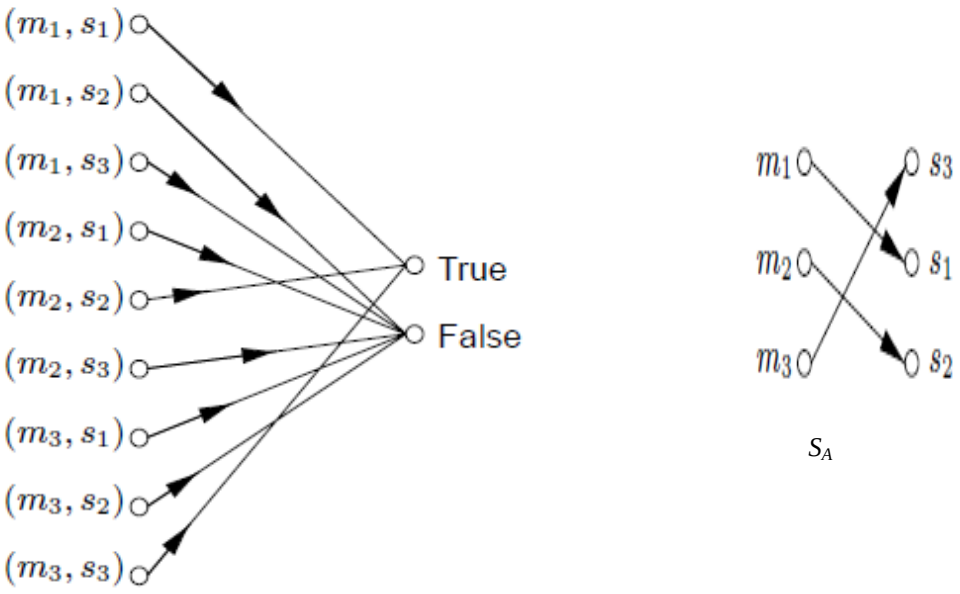

Figure 5: A Signing and verification function for HCA digital signature scheme

Figure 5 shows a graphically display of HCA property in (a) where there is an arrowed line in the diagram for V_A from ($m_i;s_j$) to *true* provided there is an arrowed line from m_i to s_j in the diagram for S_A. HCA Property in (b) provides the security such that the signature uniquely binds *A* to the *login details* which is signed.

B. Construction For HCA Digital Signature (HCA Certificate)

i. Algorithm I: HCA Digital Signature Rand_256bits

Begin ( )

Signing procedure

Entity A (the *signer*) creates a signature for a *login details* mϵM, by doing the following:

1. Compute s = $S_A(m)$.
2. Transmit the pair (*m;s*). *s* is called the *signature* for *login details m*.

Verification procedure

To verify that a signature *s* on a message *m* was created by *A*, an entity *B* (the *verifier*) performs the following steps:

1. Obtain the verification function V_A of *A*.
2. Compute $u = V_A(m;s)$.
3. Accept the signature as having been created by *A* if *u* = *true*, and
4. Reject the signature if *u* = *false*

End ( )

ii. Properties of HCA for Signing and Verification Functions

There are several properties which the signing and verification transformations must satisfy.

(a) *s* is a valid signature of *A* on *login_details m* if and only if $V_A(m;s) = true$.

(b) It is computationally infeasible for any entity other than *A* to find, for any $m\epsilon$M, an sES, such that $V_A(m;s) = true$.

(c) In the HCA, its Public-key cryptography facilitates efficient signatures (particularly non-repudiation) and key mangement while its Symmetric-key cryptography is efficient for encryption and some data integrity applications

Materials and Methods

In section 4, we employed and implemented Object Oriented Analysis and Design (OOAD) method with PhP for the client interface and MySQL server for the backend interface. The implementation follows sound software engineering principles to realize a properly developed ISCloud V.1.0 software package in the least time possible. Object oriented processes are utilized from the analysis to design phases while fusing all the hierarchies using PhP programming language (coding). Also the flowchart standard diagrams are used to effectively design the software package according to internationally approved standards. The implementation combined coding, testing, and the integration of the various software components to construct the software system. Figure 6 shows the implementation CS4 IDE.

In [15], our proposed HPDM allows our web services to be load balanced and can auto scale to 100s of dedicated instances (servers) which could enable us to increase or decrease capacity on the datacenter network within minutes. Because we are able to control this with our automatic processes in the HPDM, our cloud computing web application and hosting services will automatically scale itself up and down depending on its needs. The flexibility of our cloud web portal and possible software hosting services can serve an unlimited customer base with great reliability.

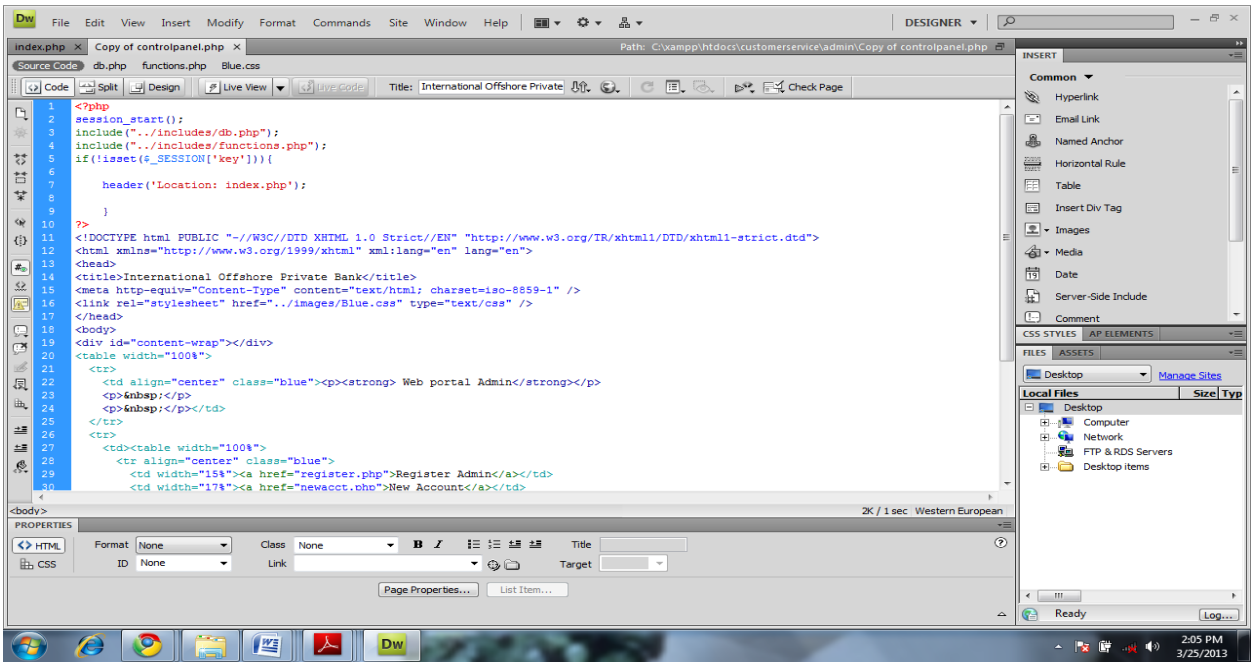

Figure 6: ISCloud V.1.0 CS4 Coding Environment

DISCUSSIONS AND RESULTS

HCA certificate are bits of code installed on ISCloud V.1.0 that encrypt logins, passwords, credit card numbers and other information so that hackers will have extreme restrictions on the SaaS. Basically, after a Secure Socket Layer (SSL) certificate is installed on a site, it uses an extensive system of security checks to establish a domain and server as trustworthy. To encrypt logins, registration forms, credit card transactions and other situations where sensitive information needs to be sent between web browsers and servers, an SSL certificate uses a private key (i.e. essentially a long string of complex code) that is unique to the individual server that hosts the web site and a public key that is sent to web browsers. The private key can only be unlocked by the public key, and vice versa, helping to ensure that the data remains secure. Usually a vast majority of businesses obtain SSL certificates from third-party providers called Certificate Authorities (CAs) online. In addition to providing the SSL certificate, a CA will also authenticate an online business to help ensure that the company represented by the web portal actually exists.

Since SSL is now considered a standard internet security technology, E-commerce user interfaces, administrator's control panels must be carefully be made secured from the developer's perspective to avoid vulnerabilities associated with SaaS. The HCA with the SSL digital certificate is then proposed to address possible security issues in ISCloud V.1.0. Figures 7a, and figure 7b shows the user's frontend and super admin control panel for shopping access. Figure 8a and figure 8b shows the XAMP Panel and MySQL Database for access authentication in ISCloud V.1.0. Figures 9a and 9b shows the customers audit logs

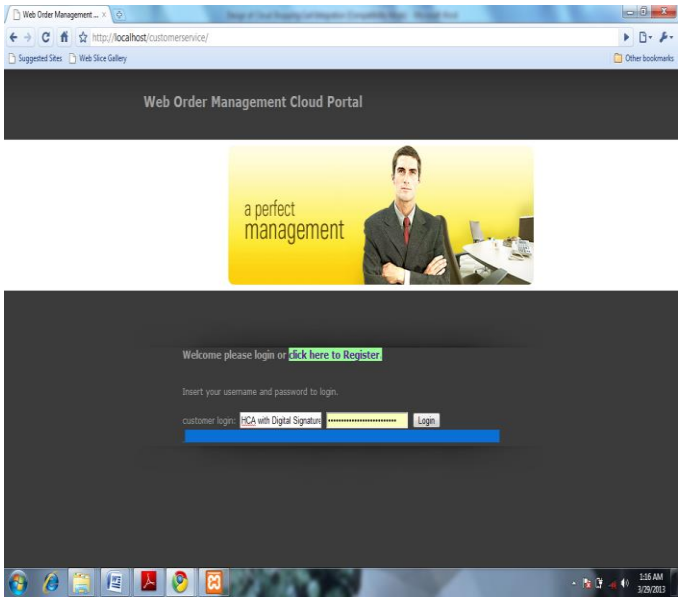

Figure 7a: User Interface(Client Side)

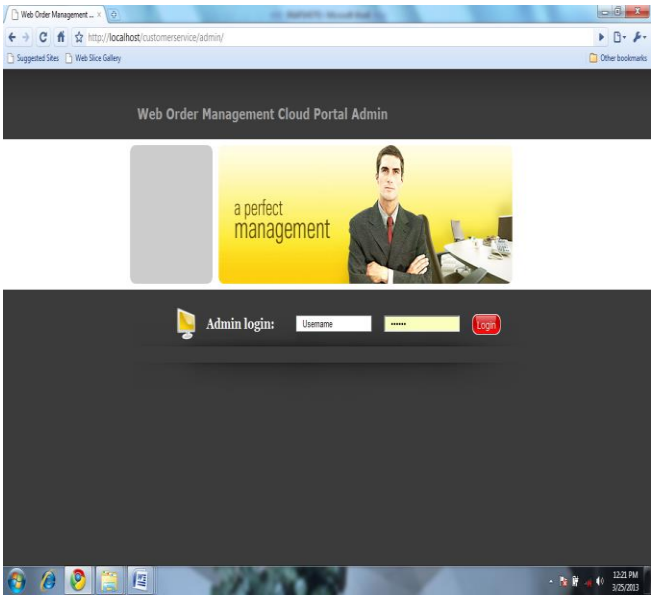

Figure 7b: Super Admin Control Panel login

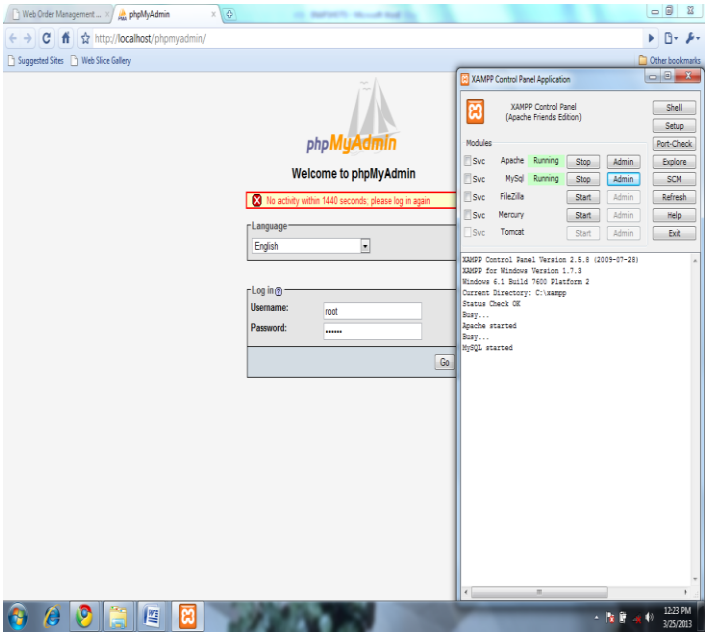

Figure 8a: XAMP Panel with HCA Authentication

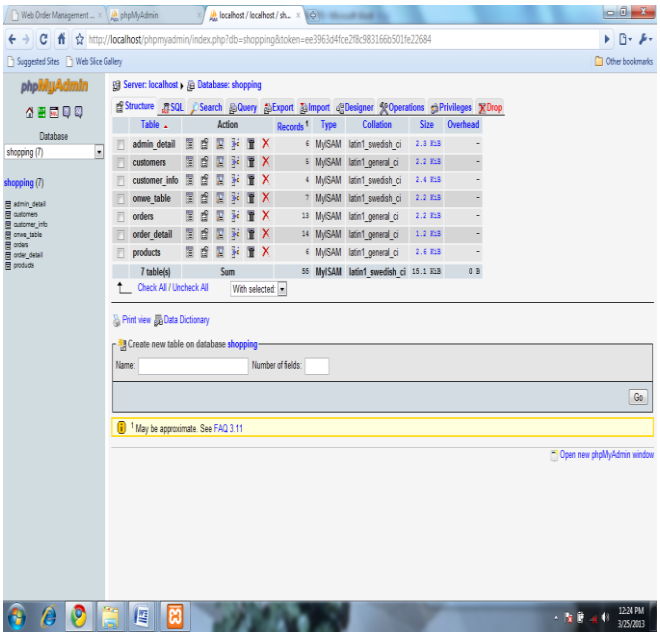

Figure 8b: MySQL Database based on HCA Authentication

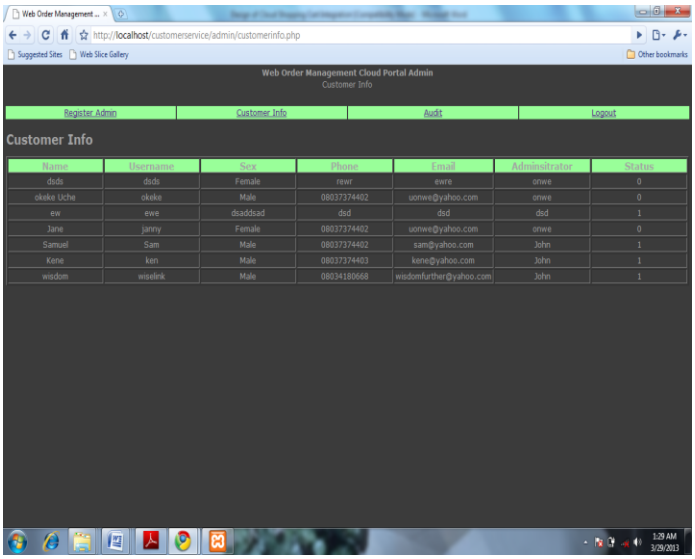

Figure 9a: Cloud Customer Info (Super Admin)

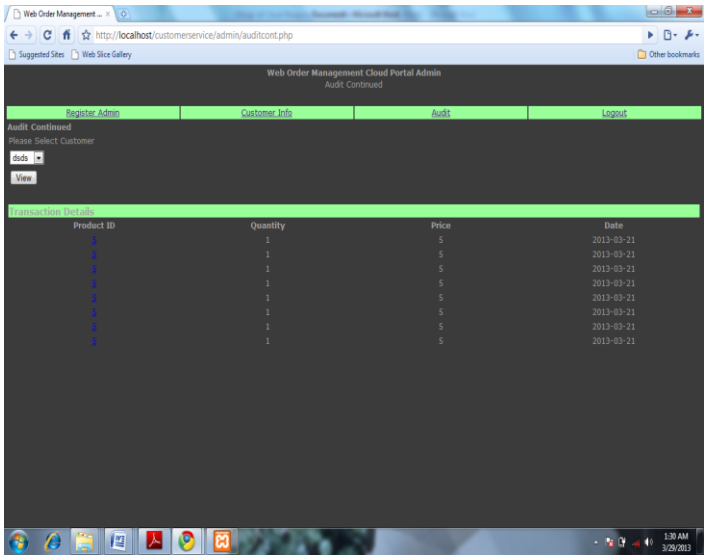

Figure 9b: Transaction Audit by Super Admin

CONCLUSIONS

E-commerce has made it possible for entrepreneurs to extend their reach farther than they could have ever imagined via cloud computing technology. Hybrid encryption is an ambivalent encryption technique for Secure online transaction and it will play an important and revolutionary role in secure electronic transaction over the internet.

This paper has proposed an online shopping cart called ISCloud V.1.0. This was developed after the SaaS paradigm. Hybrid encryption for secure access authentication in online transaction is implemented in ISCloud conceptual model. In our context, the HCA enhances security as well as integrity of confidential data due to multiple encryption operations. The main advantage of our encryption scheme is that it provides better security because even if some secret or encryption keys are cracked or some part of cipher texts are broken, the confidentiality and privacy of original data can still be maintained by multiple encryption. Secure electronic transactions with ISCloud V.1.0 encryption is shown to be an important consideration for future electronic commerce SaaS models. Such level of security is required to earn the interest and trust of customers, merchants and financial organizations for online transaction over the internet. The ideal of the secure electronic transactions using HCA with robust encryption scheme taking cognizance of its digital signature is important for the success of electronic commerce in online shopping carts.

REFERENCES

1. Himanshu Gupta, " Role Of Multiple Encryption In Secure Electronic Transaction" *International Journal of Network Security & Its Applications (IJNSA)*, Vol.3, No.6, November 2011, DOI : 10.5121/ijnsa.2011.3606 89.
2. Wikipedia: The free Encyclopedia, Technical Weblink:

   http://en.wikipedia.org/wiki/Secure_Electronic_ Transaction#History_and_development.

3. Wikipedia: Online Shopping:

   http://en.wikipedia.org/wiki/Online _Shopping

4. Jeom-Goo Kim, " Injection Attack Detection using the Removal of SQL Query Attribute Values"
5. Bhaskar Prasad rimal, Eunmi Choi, ian Lumb, "A Taxonomy and Survey of Cloud Computing Systems" *In Proceeding IEEE Computer Society,Fifth Int'l Joint Conference on INC,IMS and IDC*, 2009. Pg 44-51.
6. Gathering Clouds of XaaS! http://www.ibm.com/developer.
7. P. Mell and T. Grance, The NIST Definition of Cloud Computing, National Institute of Standards and Technology, Information Technology Laboratory, Technical Report Version 15, 2009.
8. R. Buyya, J. Broberg, A.Goscinski. Cloud Computing: Principles and Paradigms. New York, USA: Wiley Press. pp. 1-44.

9. Wikipedia, “Cloud Computing”, http://en.wikipedia.org/wiki/Cloud_computing
10. Cloud computing security, http://www.cloudtweaks.com/2012/03/fundamental-elements-of cloud-computing-security/
11. Atesh Kumar, Ashish Ranjan, Unique Gangwar, “An understanding Approach towards Cloud Computing” *International Journal of Emerging Technology and Advanced Engineering*, Volume 2, Issue 9, September 2012).
12. Anthony Thorn, Tobias Christen, Beatrice Gruber, Roland Portman, Lukas Ruf , “ What is a Security Architecture?” Information Security Society Switzerland (ISSS), Oct,2008
13. S. D. Galbraith, C. Heneghan, and J. F. McKee, “Tunable balancing of RSA”, 2005. Updated version of ACISP 2005.
14. S. Subasree and N. K. Sakthivel, “Design Of A New Security Protocol Using Hybrid Cryptography Algorithms” IJRRAS 2 (2), February 2010
15. Ravindra Kumar Chahar and et.al., “ Design of a new Security Protocol”, IEEE International Conference on Computational Intelligence and Multimedia Applications, pp 132 – 134, 2007
16. Okafor Kennedy. C, Victor.C, Prof.Inyama.,Udeze Chidiebele .C; Okezie Christiana. C; “Validation On Biometric Encryption in SMARESiM Electronic Voting System. (Accepted)
17. Walter j. Scheirer and terrance e. Boult, “Cracking fuzzy vaults and Biometric Encryption”.
18. N. Gura, A. Patel, A. Wander, H. Eberle, and S.C. Shantz, “Comparing Elliptic Curve Cryptography and RSA on 8-bit CPUs”. Proceedings of Workshop on Cryptographic Hardware and Embedded Systems (CHES 2004), 6th International Workshop, pages 119–132, 2004
19. B. den Boer and A. Bosselaers, “Collisions for the compression function of MD5”, Advances in Cryptology, Eurocrypt „07, pages 293-304, Springer-Verlag, 2007
20. Hung-Min Sun, and et al., “Dual RSA and its Security Analysis”, IEEE Transaction on Information Theory,Aug 2007, pp 2922 – 2933,2007
21. H.-M. Sun, M. J. Hinek, and M.-E. Wu, On the design of Rebalanced-RSA, revised version of [37] Centre for Applied Cryptographic Research, Technical Report CACR 2005-35, 2005 [Online]. Available: http://www.cacr.math.uwaterloo.ca/techreports/2005/cacr2005-35.pdf
22. Wikipedia: Cryptography:

    http://en.wikipedia.org/wiki/cryptpography

23. Okafor Kennedy. C, Victor.C, Prof.Inyama.,Udeze Chidiebele .C; Okezie Christiana. C; “High Performance Datacenter Model (HPDM): A Design Integration for Cloud Services” (Unpublished)