ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 3, Issue 6, June 2014

Establishment of simulated Cloud on a LAN and Execute appropriate services like SAAS, Infrastructure service with security

Varun C R[1], R Srinivasan[2]

PG Student, Department of Computer Science & Engineering, M.S.Ramaiah Institute of Technology, Bangalore, India[1]

Professor, Department of Computer Science & Engineering, M.S.Ramaiah Institute of Technology, Bangalore, India[2]

Abstract: An E-commerce software has been developed and implemented under a cloud with a view to upload this under public cloud as Application as Service. The application consists of a customer checking the goods on a merchants web site and placing the order, payment transaction done through bank and authentication for secure E-transaction (SET) verified via Dual Signature Process.

Keywords: E-transaction, Cloud computation, Secure E-transaction, Dual signature implementation.

I. INTRODUCTION

Cloud Computing is a conceptualization of a variety of computing aspects which involves considerably large number of computers connected through a communication network it provides secure means through which the resources Computing power, infrastructure, Applications, Business processes is being delivered as service on user demand it finds its applications across a wide variety of services like utility computing, software as a service (SAAS).Here in this project E-transaction software service between merchant and customer has been developed and planned to upload it under cloud once the cloud lab is set up in the college.

Electronic commerce is a process of doing business through computer networks. A person sitting on his chair in front of a computer can access all the facilities of the internet to buy or sell the products. Security is the challenge facing E-commerce today and there is still a lot of advancement made in the field of security the main advantage of E-commerce over traditional commerce is the user can browse online shops, compare prices and order merchandise sitting at home on their computers.

II. SCOPE OF THE PROJECT

A segment of four to five computers created as part of the LAN this can be ported on a cloud the cloud access would require a secure login via secure shell (SSH).The cloud consist of a SAAS application for E-transaction and authentication for secure E-transaction (SET) implementing Dual Signature.

III. CLOUD FORMATION AND COMPUTATION

Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model promotes availability and is composed of five essential characteristics, three service models, and four deployment models The characteristics of cloud computing include on-demand self service, broad network access, resource pooling, rapid elasticity and measured service.

Types of clouds

There are different types of clouds that you can subscribe to depending on your needs. As a home user or small business owner, you will most likely use public cloud services.

1. 1. Public Cloud : A public cloud can be accessed by any subscriber with an internet connection and access to the cloud space
2. Private Cloud : A private cloud is established for a specific group or organization and limits access to just that group.
3. Community Cloud : A community cloud is shared among two or more organizations that have similar cloud requirements.
4. Hybrid Cloud : A hybrid cloud is essentially a combination of at least two clouds, where the clouds included are a mixture of public, private, or community.

Characteristics

Cloud computing has a variety of characteristics, with the main ones being:

- **Shared Infrastructure** : Uses a virtualized software model, enabling the sharing of physical services, storage, and networking capabilities. The cloud infrastructure, regardless of deployment model, seeks to make the most of the available infrastructure across a number of users.
- **Dynamic Provisioning**: Allows for the provision of services based on current demand requirements. This is done automatically using software automation, enabling the expansion and contraction of service capability, as needed. This dynamic scaling needs to

ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 3, Issue 6, June 2014

be done while maintaining high levels of reliability and security.

- **Network Access** : Needs to be accessed across the internet from a broad range of devices such as PCs, laptops, and mobile devices, using standards-based APIs (for example, ones based on HTTP). Deployments of services in the cloud include everything from using business applications to the latest application on the newest smartphones.
- **Managed Metering** : Uses metering for managing and optimizing the service and to provide reporting and billing information.

In this way, consumers are billed for services according to how much they have actually used during the billing period. In short, cloud computing allows for the sharing and scalable deployment of services, as needed, from almost any location, and for which the customer can be billed based on actual usage.

There are three types of cloud providers that you can subscribe to: Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS). These three types differ in the amount of control that you have over your information, and conversely, how much you can expect your provider to do for you. Briefly, here is what you can expect from each type.

1. **Software as a Service** : A SaaS provider gives subscribers access to both resources and applications. SaaS makes it unnecessary for you to have a physical copy of software to install on your devices. SaaS also makes it easier to have the same software on all of your devices at once by accessing it on the cloud. In a SaaS agreement, you have the least control over the cloud.
2. **Platform as a Service** : A PaaS system goes a level above the Software as a Service setup. A PaaS provider gives subscribers access to the components that they require to develop and operate applications over the internet.
3. **Infrastructure as a Service** : An IaaS agreement, as the name states, deals primarily with computational infrastructure. In an IaaS agreement, the subscriber completely outsources the storage and resources, such as hardware and software, that they need.

Deployment of Cloud Services

- Cloud services are typically made available via a private cloud, community cloud, public cloud or hybrid cloud.
- Generally speaking, services provided by a public cloud are offered over the Internet and are owned and operated by a cloud provider. Some examples include
- services aimed at the general public, such as online photo storage services, e-mail services, or social networking sites. However, services for enterprises can also be offered in a public cloud.
- In a private cloud, the cloud infrastructure is operated solely for a specific organization, and is managed by the organization or a third party.
- In a community cloud, the service is shared by several organizations and made available only to those groups. The infrastructure may be owned and operated by the organizations or by a cloud service provider.

IV. E-COMMERECE APPLICATION IN SAAS

Electronic commerce (EC) is possibly the most promising application of information technology witnessed in recent years. It is revolutionizing supply-chain management and has enormous potential for manufacturing, retail and service operations. The tremendous importance of EC has prompted us to write this paper. We have attempted to define e-commerce and examine major EC elements that link organizational systems.

The application of EC in manufacturing, retailing and service operations is examined, and a framework for describing EC components and their role in different areas of an organization is proposed.

And other knowledge-based intangible products. Although most EC is currently at the inter-corporate and inter-organizational level, services targeted at individual customers are evolving rapidly. The Internet is the most obvious example of this and is a major catalyst in the diffusion of EC, helping to foster a common environment for electronic transactions of all kinds. At present, business-to-business EC seems still to be of greater volume than business-to-consumer EC, but this may change in the future. These trends are important to the global economy and to the economy of individual countries because EC contributes to economic efficiency in five important ways. They are as follows:

1. Shrinking distances and timescale
2. Lowering distribution and transaction costs,
3. Speeding product development,
4. Providing more information to buyers and sellers and Enlarging customer choice and supplier reach.

Electronic Commerce is an emerging area that encompasses processes directly and indirectly related to the buying, selling and trading of products, services and information via computer networks – including the Internet. Kolkata and Whinston define EC from these four perspectives:

1. communication perspective : EC is the deliverer of information, products/services or payments over telephone lines, computer networks or any other electronic means

2. Business process perspective – EC is the application of technology towards the automation of business transactions and work flows

3. Service perspective : EC is a tool that addresses the desire of firms, consumers and management to cut service costs while improving the quality of goods and increasing the speed of service delivery Online perspective : EC provides the capacity to buy and sell

ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 3, Issue 6, June 2014

products and information on the Internet as well as other online services.

Advantages of Internet-based EC

- Shorten procurement cycles through the use of on-line catalogues, ordering, and payment
- Cut costs on both stock and manufactured parts through competitive bidding
- Reduce development cycles and accelerate time to-market through collaborative engineering,product, and process design, regardless of the location of participants
- Gain access to worldwide markets at a fraction of traditional costs
- Ensure that the product, marketing information and prices are always up to date
- Significantly increase the speed of communication especially international communication
- Drastically reduce purchasing and production cycles
- Reduce the cost of communications directly(E-mail and EDI save on postage) and speed up communication can reduce inventory and related inventory and purchasing costs
- Promote closer relationship with customers and suppliers, e.g. web sites enable companies to maintain customers and suppliers apprised of developments that concern them and practice effective relationship marketing
- Provide a quick and easy way of exchanging information about a company and its products, internally and externally e.g. WWW sites, Intranets, and extranets
- Take advantage of alternative sales channels and tap new markets or markets niches.

ELECTRONIC PAYMENT SYSTEM

Electronic payment systems are becoming central to on-line business transactions nowadays as companies look for various methods to serve customers faster and more cost effectively. Electronic commerce brings a wide range of new worldwide business opportunities.

A conventional process of payment and settlement involves a buyer-to-seller transfer of cash or payment information (e.g. credit card or check). The actual settlement of payment takes place in the financial processing network.

A cash payment requires a buyer's withdrawal from his bank account, a transfer of cash to the seller, and the seller's deposit of the payment to his/her account. Non-cash payment mechanisms are settled by adjusting, i.e. crediting and debiting, the appropriate accounts between the banks based on payment information conveyed via check or credit card.

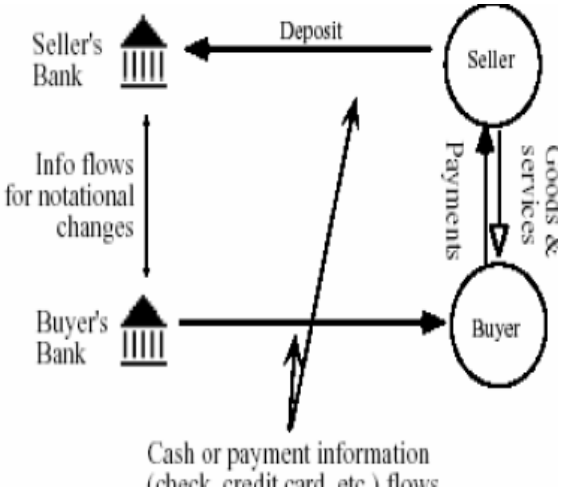

Fig 1. Merchant transaction via Bank

When face-to-face purchase is replaced with on-line commerce, many aspects of a transaction occur instantly, under which various processes of a normal business interaction are subsumed. For example, a typical purchase involves stages of locating a seller, selecting a product, asking a price quote, making an offer, agreeing over payment means, checking the identity and validity of the payment mechanism, transferring of goods and receipts. In order to be used as a substitute for face-to-face payments, online payment systems must incorporate all or some of these stages within their payment functions. The lack of face-to-face interaction also leads to more secure methods of payment being developed for electronic commerce, to deal with the security problems for sensitive information and uncertainty about identity. Consequently, electronic commerce transactions require intermediaries to provide security, identification, and authentication as well as payment support.

The key benefit of this payment clearing system is that it separates sensitive and non-sensitive information and only non-sensitive information is exchanged online. This alleviates the concern with security that is often seen as a serious barrier to online commerce. In fact, First Virtual does not even rely on encryption for messages between buyers and sellers. A critical requisite for this system to work is the users' trust in the intermediaries.

Payment Based on Electronic Currency The third type of payment systems transmit not payment information but a digital product representing values: electronic currency. The nature of digital currency mirrors that of paper money as a means of payment. As such, digital currency payment systems have the same advantages as paper currency payment, namely anonymity and convenience. As in other electronic payment systems, here too security during transmission and storage is a concern, although from a different perspective, for digital currency systems doubles pending, counterfeiting, and storage become critical issues whereas eavesdropping and the issue of liability (when charges are made without authorization) are important for notational funds transfers. Figure 4 shows a digital currency payment scheme. The only difference from

ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 3, Issue 6, June 2014

Figure is that the intermediary in Figure 4. acts as an electronic bank which converts outside money, into inside money (e.g. tokens or e-cash) which is circulated within online markets.

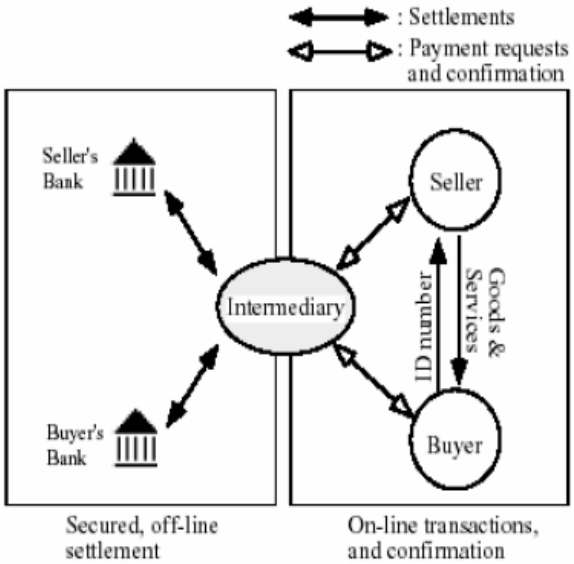

Fig 2. Merchant transaction via Bank transaction

The Secure Sockets Layer (SSL) protocol was designed by Netscape as a method for secure client-server communications over the Internet. Using public key cryptography and certificates, SSL offers a mechanism so that clients and servers can authenticate each other and then engage in secure communication. During an initial handshaking phase, the client and server select a secret key crypto scheme to use and then the client sends the secret key to the server using the server's public key from the server's certificate. From that point on, the information exchanged between the client and server is encrypted. SSL/TLS is an intermediate protocol layer that sits between TCP and a higher-layer application. SSL/TLS can be employed by any application layer protocol running over the Transmission Control Protocol (TCP), including Hypertext Transfer Protocol (HTTP), File Transfer Protocol (FTP), As the SSL/TLS protocol handshaking.

Algorithm & Flow Chart

5.4.1. Algorithm for Order Creation

Step 1: Customer selects products from the available list of products

Step 2: Customer adds to shopping cart

Step 3: Customer initiates transaction

Step 4: Customer credit card information is validated, if invalid aborts the transaction

Step 5: Customer balance is checked against product value, if insufficient aborts the transaction

Step 6: If Customer balance is sufficient and credit card information is valid, order information is encrypted

Step 7: Product information is encrypted

Step 8: Order Information and Product information is concatenated and saved into file.

Step 9: File is saved along with Customer's private key.

Step 10: File is sent to Merchant and Bank

Step 11: Merchant decrypts file using customer's public key and verifies the product information

Step 12: Bank decrypts using customer's public key and verifies customer payment information

Step 13: Bank deducts product amount from Customer account and transfers equal amount to Merchant's account

Step 14: Merchant receives payment and arranges for shipment of products to customer

Step 15: Customer receives products.

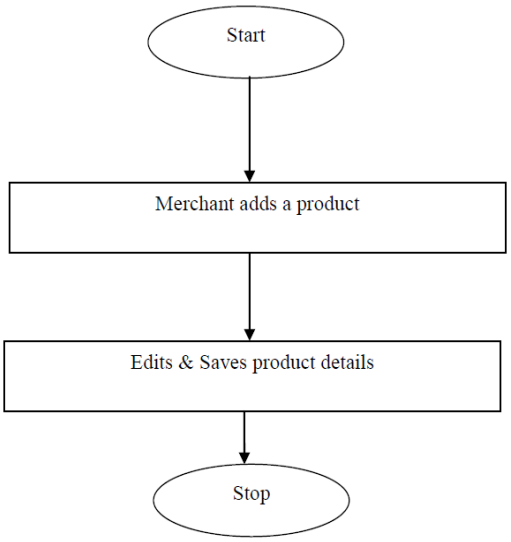

Fig 5.5.Flow chart of product creation

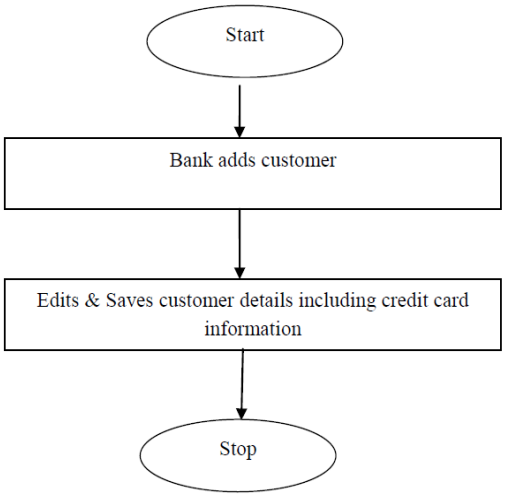

Fig 5.6.Flowchart of Customer Details creation

The flow chart for Different phases of the design consist of the details and shows the design flow. There are different instances like product creation, customer details creation, order creation, Order completion.

ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 3, Issue 6, June 2014

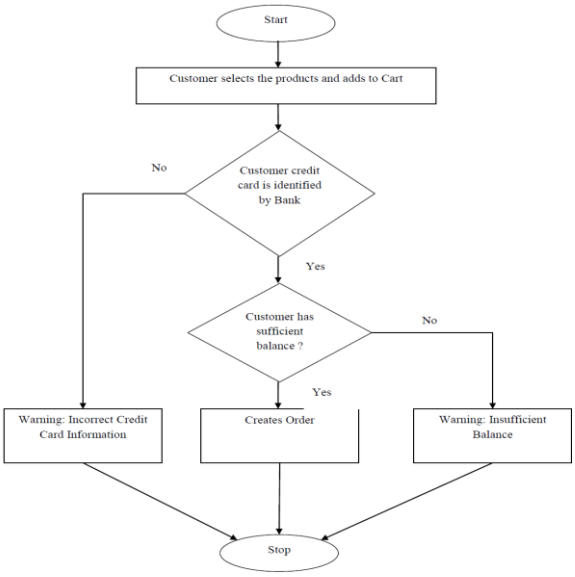

Fig 5.7.Flowchart of Order Creation Flow

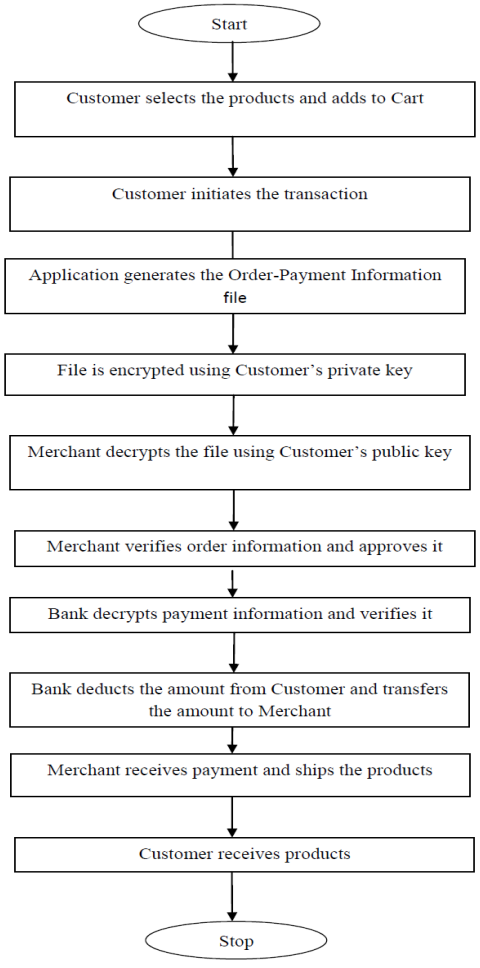

Fig 5.8.Flowchart of Order Completion Flow

V. SECURE ELECTRONIC TRANSACTION PROTOCOL (SET)

The Secure Electronic Transaction (SET) protocol specifically handles electronic payments. Fraud prevention is a primary motivator behind SET. That would seem to indicate that the current model of using SSL to protect transactions is adequate. SET has the potential to reduce the chance of fraud by providing rigorous authentication measures in addition to encrypting transactions. SET provides a high degree of privacy for customers by encrypting payment information so that only the bank can see it. Customer software sends a purchase request to the merchant containing the following unencrypted order information and a dual signature, intended for the merchant; payment instructions and a dual signature, both encrypted and intended for the payment gateway; and the cardholder‘s digital certificate to be used by the merchant and the payment gateway for authentication.

To carry out transactions successfully and without compromising security and trust, business communities, financial institutions and companies offering technological solutions wanted a protocol that works very similar to the way how a credit card transactions work . In this paper, we focus on the implementation of SET key construct: the dual signature. This mechanism lets the customer agree the order details with the merchant while hiding those details from the bank; at the same time, it lets the customer share his credit card details with the bank while hiding them from the merchant. An important innovation introduced in SET; the dual Signature. The purpose of the dual signature is the same as the standard electronic signature: to guarantee the authentication and integrity of data. In this case, the customer wants to send the order information (OI) to the merchant and the payment information (PI) to the bank. The merchant does not need to know the customer`s credit card`s number, and the bank does not need to know the details of the customer`s order. The customer is afforded extra protection in terms of privacy by keeping these two items separate. However, the two items must be linked in a way that can be used to resolve disputes if necessary. The link is needed so that the customer can prove that this payment is intended for this order and not for some other goods and service.

Key Features of SET

♦ **Confidentiality of information**: cardholder account and payment information is secured as it travels across the network. An interesting and important feature of SET is that it prevents the merchant from learning the cardholder’s credit card number; this is only provided to the issuing bank. Conventional encryption by DES is used to provide confidentiality.

♦ **Integrity of data**: payment information sent from cardholders to merchants includes order information, personal data, and payment instructions. SET guarantees that these message contents are not altered in transit. RSA digital signatures, using SHA-1 hash codes, provide message integrity. Certain messages are also protected by HMAC using SHA-1.

♦ **Cardholder account authentication**: SET enables merchants to verify that a cardholder is a legitimate user of a valid card account number. SET uses X.509v3 digital sertificates with RSA signatures for this purpose.

ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 3, Issue 6, June 2014

♦ **Merchant authentication**: SET enables cardholders to verify that a merchant has a relationship with a financial institution allowing it to accept payment cards. SET uses X.509v3 digital certificates with RSA signatures for this purpose.

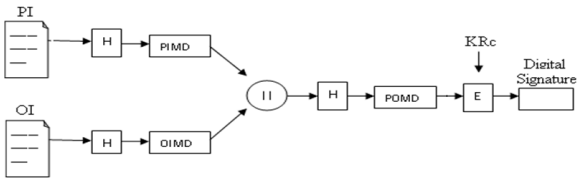

Fig 3.Dual Signature Verification

Figure 3 shows the model of dual signature. When the dual signature is constructed, it gets the hash of the concatenated hashes of OI (Order Information) and PI (Payment Information) as inputs. The dual signature is the encrypted MD (with the customer's secret key) of the concatenated MD's of PI and OI. The dual signature is sent to both the merchant and the bank. The protocol arranges for the merchant to see the MD of the PI without seeing the PI itself, and the bank sees the MD of the OI but not the OI itself. The dual signature can be verified using the MD of the OI or PI.

Within the SET protocols there is a circumstance where the cardholder communicates with both the merchant and payment gateway in a single message. The message contains an order section, with details of the products/services to be purchased, plus a payment section. The payment information will be used by the banker and the order information by the merchant, but the messages are both sent collectively this means that the message packaging must:

1. Prevent the merchant from seeing the payment instruction
2. Prevent the banker from seeing the order instruction
3. Link the two parts of the message, so that they can only be used as a pair

In this case, SET uses a procedure called dual signature. When the order and payment instructions are sent by the cardholder, the merchant will be able to read the order instruction, and the banker is able to read only the payment instruction.

The merchant will not see the cardholder's account information. In a SET transaction, the transfer of money and offer are linked allowing the money to be transferred to the merchant only if the cardholder accepts the offer. The bond is needed so that the customer can prove that this payment is intentional for this order and not for some other goods and service

Sequence of events for transactions

1. The customer opens a credid card account.
2. The customer receives a certificate.(X.509v3)
3. Merchants have their own certificates.(2 certificates for 2 public keys – one for signing and one for key exchange – needs a copy of gateways public-key certificate)
4. The customer places an order.
5. The merchant is verified.
6. The order and payment are sent.
7. The merchant request payment authorization. (from payment gateway)
8. The merchant confirms the order.
9. The merchant provides the goods or service.
10. The merchant requests payments. (to payment gateway)

VI. RESULTS

An E-Commerce application is been developed on a Cloud which is been created and configured on a LAN. The snap shots of the transactions of the customer, merchant and bank are show below in a sequence.

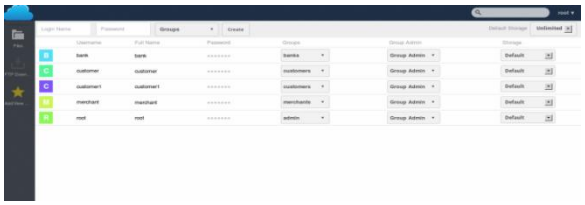

Fig 4. user creation

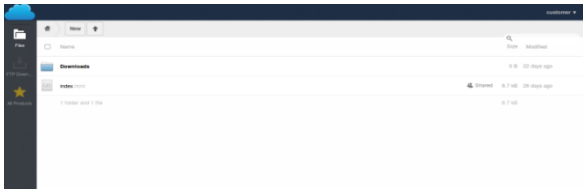

Fig 5. Default home page for customers

Fig 6. Default home page for Bank

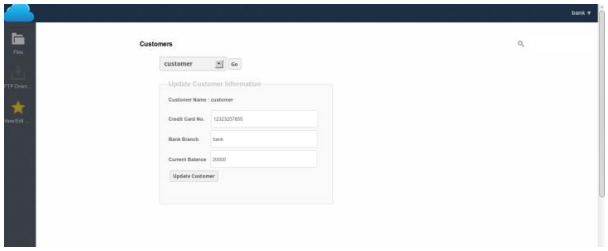

Fig 7. Editing customer information

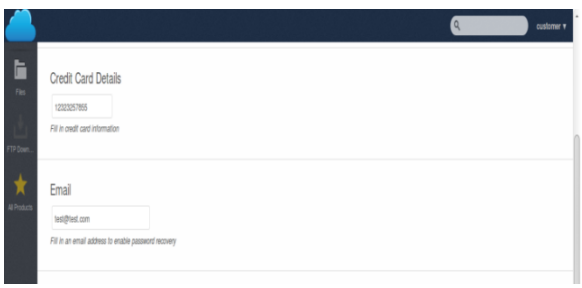

Fig 8. Credit card Details

ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 3, Issue 6, June 2014

Fig 9. Adding products to Cart

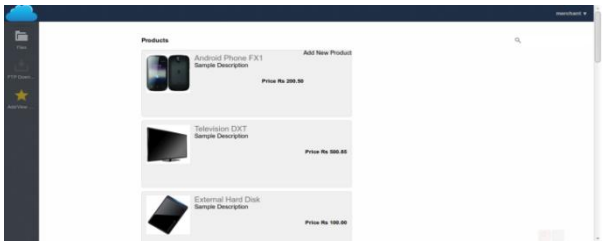

Fig 10. View Products

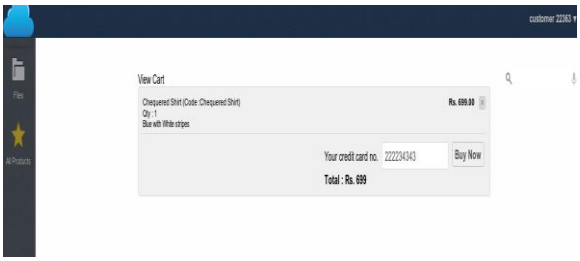

Fig 11.Order Buy process

VII. CONCLUSION

- The project concentrates on e-commerce application and been implemented on a private cloud.
- A private Cloud has been created and configured for a few systems under a LAN and been tested for SaaS (Software as a Service) application.
- An E-commerce application has been developed under SaaS. The application consists three entities Customer, Merchant and bank.
- The electronic transaction between the three entities are shown in the application and even the payment norms have been developed.
- The payment norms and e-transaction is done using secured authentication.A SET (Secured Electronic Transaction) protocol is used for authentication using Dual signature.
- The payment process has been verified and authentication via dual signature has been verified. The e-commerce application is run on the Cloud and verified.

REFERENCES

[1] http://blog.animoto.com/2008/04/21/amazon-ceo-jeff-bezos-on-animoto/
[2] "Let it rise – A special report on corporate IT", The Economist, October 25th, 2008
[3] Jeff Cogswell, "RightScale eases developing on Amazon EC2" e-week.com, October 21st, 2008
[4] Peter Wayner, "Cloud versus cloud – A guided tour of Amazon, Google, AppNexus and GoGrid", InfoWorld, July 21, 2008
[5] James Staten, "Is Cloud Computing Ready for the Enterprise?", Forrester Report, March 7, 2009,
[6] http://searchitchannel.techtarget.com/generic/0,295582,sid96_gci1336995,00.html
[7] http://en.wikipedia.org/wiki/Cloud_computing - Cloud computing
[8] Ms.Vaishnavi.J.Deshmukh1 Sapna.S.Kaushik2 Mr. Amit.M.Tayade3 Lecture Computer Engg Department Lecturer Computer Engg Department Lecturer Computer Engg Department SGBAU-Amravati University SGBAU-Amravati University SGBAU-Amravati University India. India. India "Payment Processing Systems and Security for E-Commerce: A Literature Review "International Journal of Emerging Research in Management &Technology ISSN: 2278-9359 (Volume-2, Issue-5)
[9] Dr.Rao Mikkilineni and Vijay Sarathy kawa Objects,Inc.Los Altos, CA, IEEE " Cloud Computing and the Lessons from the Past" 2009 18th IEEE International Workshops on Enabling Technologies: Infrastructures for Collaborative Enterprises
[10] Mohamed A. El-Refaey Arab Academy for Science, Technology and Maritime Transport College of Computing & Information Technology Cairo, Egypt and Dr. Mohamed Abu Rizkaa Arab Academy for Science, Technology and Maritime Transport College of Computing & Information Technology Cairo, Egypt IEEE "Virtual Systems Workload Characterization" 2009