Scholars Journal of Engineering and Technology (SJET) **ISSN 2321-435X (Online)**
Sch. J. Eng. Tech., 2017; 5(10):513-523 **ISSN 2347-9523 (Print)**

(An International Publisher for Academic and Scientific Resources)
www.saspublishers.com

Customers Influx, Awareness and Security Management in E-Commerce

Otaru Ekhare Natheniel[1], Ezeoke Grace[2], Ashikodi Anthony Ifeanyi[3], Ajagun Kehinde Oluwatomi[4], Okorun Ambrose Ali[5],
National Engineering Design Development (NEDDI). Nnewi, Anambra State.

***Corresponding author**
Otaru Ekhare Natheniel

Article History
Received: 28.09.2017
Accepted: 05.10.2017
Published: 30.10.2017

DOI:
10.36347/sjet.2017.v05i10.001

Abstract: Customer's awareness and embracing e-commerce transaction have been a major issue in recent years. This is because people are still scared about electronic commerce customer's safety. The weaknesses of safety and lack of security are barriers in conducting any transactions in online business and banking transactions. This work focuses on managing and increasing customer's awareness and influx, and ensuring low or no risk with effective risk managing on E-Commerce. Trust is the most critical factor that drives the business either it is traditional or e-business. There are number of factors that contribute to the e-commerce trust. The use of personal and credit card information during online transactions bring a lot of concern to the users as how their information will be used. Organizations in online businesses are also concerned on how the customers and their businesses can be secured. There is fear of the unknown in the system. An expository review and instances are made to make people of the world be sure of security, reliability and the convenience in the e-business with a technical stepwise presentation of security, contributory role of providers and costumers, as well as services.
Keywords: Customers' influx, awareness, security, reliability, e-commerce

INTRODUCTION

Cloud computing security architecture is a critical element in establishing trust in the cloud computing paradigm. Confidence in using the cloud depends on trusted computing mechanisms, robust identity management and access control techniques, providing a secure execution environment, securing cloud communications, and supporting micro architectures. The viability of e-commerce is threatened with various forms of insecurities which allow quick or direct access in the e-commerce by mere logging in and shopping, it comes to notice that it can discourage users as its lack of securities is prone to frauds and the monotonous in changing of IDs due to the incessant interference of hackers will go a long way to discouraging users as it could be taken as sailing in an uncharted water characterized by unsafe conditions for the users. E -commerce is versatile with fast growing media by which businesses and other market forms are achieved without the physical presence of the individuals in the business as against the traditional ways of marketing system. Thus, the need for a system with a secured administrator interface that can identify customers, view and show list of customers, and able to disable and enable customers through IDs(usernames) and password verification with a well-designed portal with an encryption cryptographic algorithm for secured business transactions that allows users for secured interactivity on the internet cloud and interconnectivity using the concept of packet switching process on the network switch buffer with quick response signals to satisfy current web security and network requirements in a cloud data Centre model. To curb this vulnerability of e-commerce to insecurities, the design of an E-commerce cloud application model called. For emerging ecommerce designs; effective networks must satisfy excellent resource utilization for such designs as well as other related web services. Such network model should scale gracefully with network capacity, providing high utilization, dynamic stability represented by stabilized throughput. This project 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 over the web, 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 presence thereby enhancing cost savings, while increasing revenue and sales with accurate sales tracking and management. Hence, a cloud data Centre is needed with a designed portal that allows users for secured interactivity on the internet cloud and interconnectivity using the concept of packet switching

process on the network switch buffer with quick response signals to satisfy current web security and network requirements in a cloud data Centre model through the use of an E-commerce cloud application model called Cloud E-commerce System (CES).

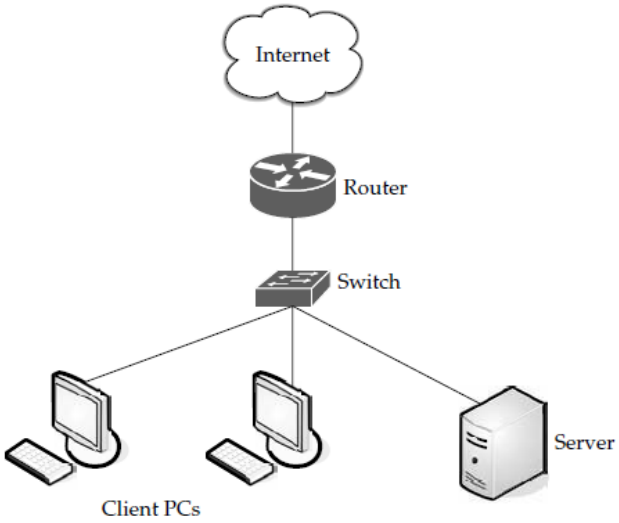

Fig-1: Acloud is used in network diagrams to depict the internet

E-commerce Security is a component of the Information Security framework and is applied to the components that affect e-commerce that include Computer Security, Data security and other wider factors of the Information Security framework. E-commerce security has its own particular nuances and is one of the highest visible security components that affect the end user through their daily interaction with business. Organizations like commercial, industrial, military, and government IT operations have a variety of regulatory and statutory requirements with regard to the security of sensitive data or information. Migration from a conventional IT server environment to a cloud paradigm poses new challenges and risks, and provides cost-saving opportunities.IT organizations have relied on standards and guidelines from a number of organizations, including the National Institute of Standards and Technology (NIST), the International Organization for Standardization (ISO), the Open Web Applications Security Project (OWASP), the Organization for the Advancement of Structured Information Standards (OASIS), and the European Telecommunications Standards Institute (ETSI). These standards address life cycle issues, including requirements, architectures, implementation, deployment, and security. In order for cloud computing to gain acceptance and trust, standards have to be developed for the cloud environment. In addition, important aspects of cloud security such as incident management and response, encryption, key management, and retirement of hardware and software must be addressed and incorporated into cloud computing implementations.

Security services offering protection from security threats are: identification, authentication, confidentiality, integrity, access control, and non-reputation. Currently, e-business applications are doing more than ever to increase efficiency and In relation to trust and internet technologies, consumers are concerns about two main things which are privacy and security. This study is borders on the issues relating to e-business, such as its importance, issues and the solutions in order to overcome related to the security and trust in e-business. There is almost an uncountable number of ways that an e-business setup could be attacked by hackers, crackers and disgruntled insiders. Common threats include hacking, cracking, masquerading, eavesdropping, spoofing, sniffing, Trojan horses, viruses, bombs, wiretaps, etc.

The customer's problems are:

- Lack of understanding on how e-business operates.
- Lack of confidentiality in e-business or online transactions
- Lack of awareness regarding the problem of security involved in e-business.
- Lack of an in-depth understanding relating the trust involved in e-business.

Statement of Problem

The versatility and flexibility in the use of E-commerce that prompt the fast growing global world market has been proven beyond reasonable doubt to encourage international markets growth through online business transactions involving individuals, financial institutions, corporate organizations ,stock exchange markets. E -commerce as an online business allows the

people access for on line business activities this has become open door for insecurity for the system as it is an analogy to open market operation that allows room for free entry and exit without identity without any sanction or penalty attached. Every user(s) are anonymous for lack of provisions for identity that will show case users at every point in time. E-commerce becomes vulnerable to insecurity that can reduce partnering of people. Therefore, to encourage people who find e-commerce as a profitable fast and easy means of transaction than the traditional way of offline business transactions? The traditional way of business transactions has a lot of limitations to prospective customers and business owners. Some of these include improper shopping navigation, account auditing, poor inventory documentation, inflexibility and poor service delivery in terms of billing, etc. The need to enhance the used of e-commerce that incorporates securities that will identify usernames and passwords of users, show list of user at a point in time, and be able to enable and disable users if there is evident of wrong use of pass codes or activities likely to be frauds.

Aims and objectives

Developing an E-commerce cloud application model-Cloud E -commerce system with securities online business transaction is aimed to develop an ecommerce portal with an encryption cryptographic algorithm for secured business transactions which will fit into a proposed cloud data centric network model. This leverages on a proposed reengineered service process for internet backbone. This paper work addressed the objectives as stated:

- Create an understanding on how e-business operates.
- Enhance confidentiality in e-business or online transactions
- Create awareness regarding the problem of security involved in e-business.
- Create an in-depth understanding relating the trust involved in e-business..

Scope of the Work

Reliability of E-commerce, its models, as well as embracing it with a review to working and transacting in safe environment become paramount to enhance ecommerce. Its security concepts, network architectures and implementation technologies were analyzed and building of reliable security. New types of attacks are constantly surfacing, and attackers often employ new ways to exploit and hide in legitimate traffic. This places organizations in a continual mode of catch-up, trying to make sure that they have appropriate Protection against the latest vulnerabilities and threats. With the emergence of new applications, the security landscape continues to change. Although existing intrusion prevention techniques are still applicable, simply identifying source and destination addresses and port combinations no longer offers sufficient. This work is expository on creating awareness, making a thorough understanding of ecommerce operation, understanding its security measures to draw consumers' attentions and interests.

Security

Supports rigorous security needed at each step in the lifecycle of commerce applications—from raw input sources to valuable insights to sharing of data among many users and application components. Security services enable identity and access management, protection of data and applications, and actionable security intelligence across cloud and enterprise environments. It uses the catalog and user directory to understand the location and classification of the data it is protecting.

Key capabilities in this domain include:

Identity and Access Management: Enables authentication and authorization (access management), as well as privileged identity management. Access management ensures each user is authenticated and has the right access to the environment to perform their task based on their role (that is, customers, employees, partners, supply chains, and business users). Capabilities should include granular access control (giving users more precision for sharing data) and single sign-on facility across big data sources and repositories, data integration, data transformation, and analytics components. Privileged identity management capabilities protect, automate, and audit the use of privileged identities to ensure that the access rights are being used by the proper roles, to thwart insider threats, and to improve security across the extended enterprise, including cloud environments. This capability generally uses an enterprise user directory.

b. Application and Data Protection: Services that enable and support data encryption, infrastructure and network protection, application security, data activity monitoring, and data lineage.

- Data encryption: Secures the data interchange between components to achieve Confidentiality and integrity with robust encryption of data at rest as well as data in transit.
- Infrastructure and network protection: Supports the ability to monitor the traffic and Communication between the different nodes (like distributed analytical processing nodes) as well as prevent man-in-the-middle, disk operating system attacks. This servicealso sends alerts about the presence of any bad actors or nodes in the environment.
- Application security: Ensures security is part of the development, delivery, and execution of

application components, including tools to secure and scan applications as part of the application development lifecycle. Application security identifies and remedies security vulnerabilities from components that access critical data before they are deployed into production.

- Data activity monitoring: Tracks all submitted queries and maintains an audit trail for all queries run by a job. The component provides reports on sensitive data access to understand who is accessing which objects in the data sources.
- Data lineage: Traces the origin, ownership, and accuracy of the data and complements Audit logs for compliance requirements.

c. Security intelligence: Enables security information event management, audit and compliance support for comprehensive visibility, and actionable intelligence to detect and defend against threats through the analysis of events and logs. High-risk threats that are detected can be integrated into enterprise incident management processes. This component enables auditingcapability to demonstrate that the analytics delivered by the big data platform sufficiently protects Personally Identifiable Information (PII) and delivers anonymity. It also enablesautomated regulatory compliance reporting. Security / fraud detection is an important part of the payment processing steps and if fraud is detected it gets reported directly to the enterprise For immediate action.

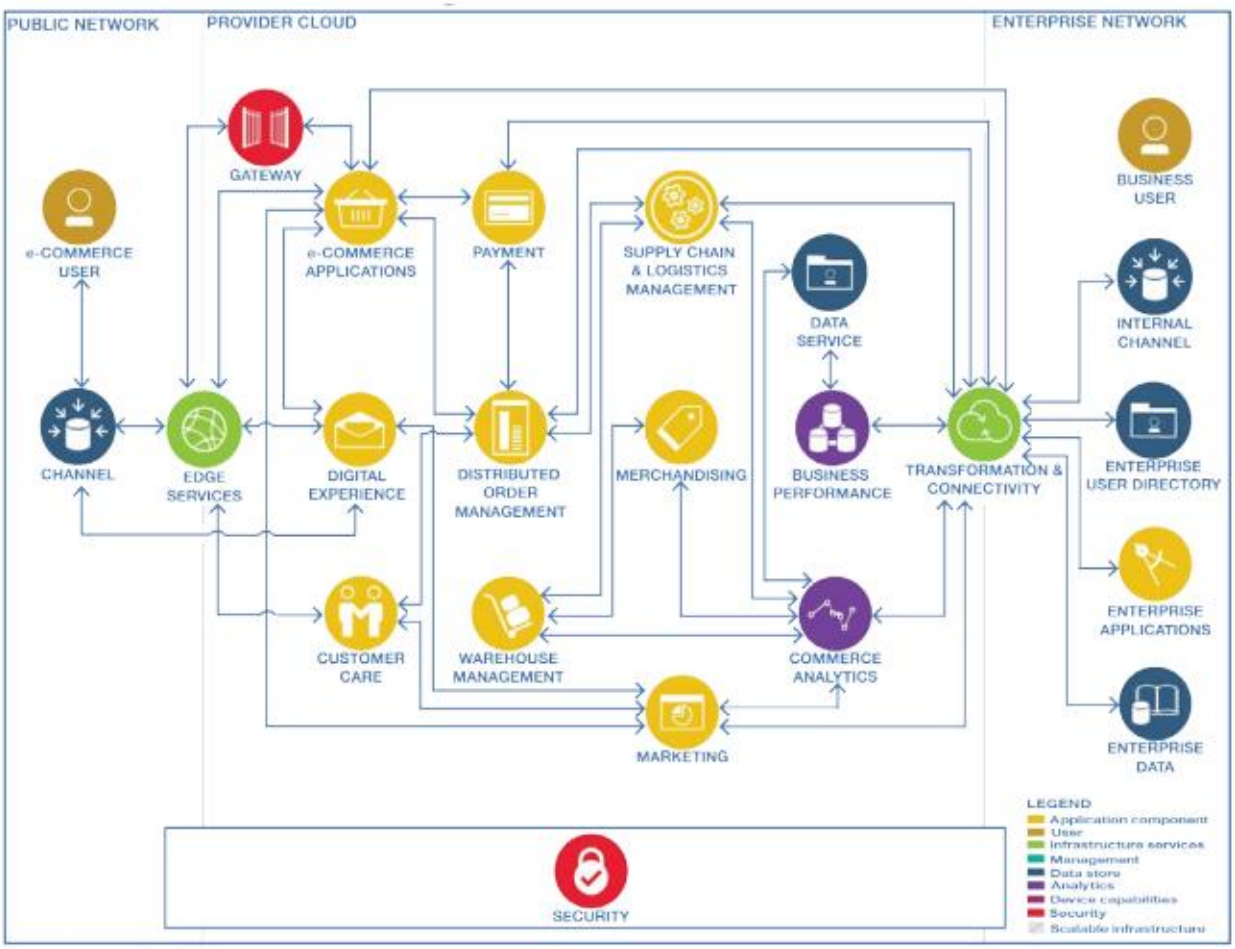

Fig-2: Cloud Component Relationships for e-Commerce

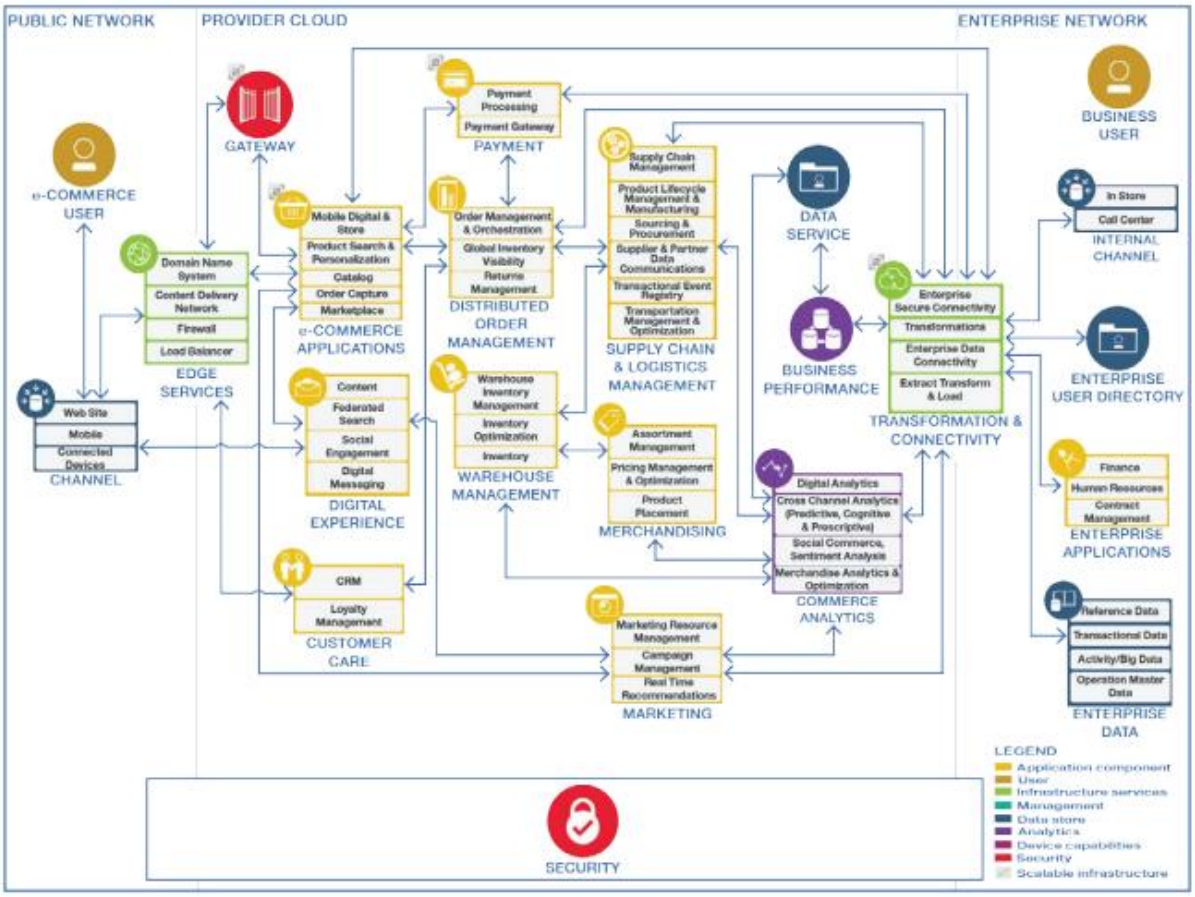

Fig-3: Detailed Components Diagram

HuiQing software firm is trying to help enterprises to comply with the above reference standard whenever we are asked to provide ebusiness solutions. Shanghai HuiQing Information Technology Limited was registered at Shanghai Pudong Software Park, which was incorporated by the CIT lab of Shanghai Jiaotong University and two professors who received the Ph.D. degrees from Stanford University. HuiQing has a strategic partnership with HiQTech, Inc. at San Francisco. HuiQing provides an integrated total solution of ebusiness. The mission of the company, via its own proprietary software products and consulting services, is to update information systems for China enterprises, to facilitate the potential capabilities of China enterprises in the area of new product development and operational and strategic business management, therefore, to speed seamlessly their advancement to world-class level. HuiQing Total E-Business Solution Set includes six modules as follows:

HiQ-SCM

This is a rapid re-configurable and re-constructed agile supply management system, which can support an integration of different ERP, different MIS systems, and workflow management.

- HiQ-INS: This is an integrated network security system. It includes a Digital Certificate System with our proprietary CSP module, a Secured E-mail system, and a Secured Firewall supporting VPN tunnel and a secured data management system to ensure the integrity and tracibility of all kinds of important data, documents, and transactions of both intra- and inter- enterprises.
- HiQ-WFM: This is an intra/inters enterprises workflow management system. It provides a modeling and management platform for rapid deployment of business process reengineering and product development process reengineering. It provides a versatile process control and management capabilities, including a unified workbench for daily coordination and communication among team members, while each activity can be tightly connected with and bounded by enterprises' ISO 9001 regulations.
- HiQ-CBD: It is a case based knowledge management system (KMS) for DFX applications and other decision-making applications. To meet the requirements of dynamically changing and expanding KMS, HiQ-CBD allows user to define and modify case attributes dynamically whereas the back-end database and front-end GUI could be self-

adjusted by the system. Users could simply define and modify domain ontology and inference rules to control the behavior of those intelligent agents.

- HiQ-CRM: This is a Customer Relationship Management System. It is based on a combination of CTI and web platform for operation management for customer responses and a business intelligence system for studying customer behavior.
- 6HiQ-IDM: This a financial portfolios management and forecast system for the various markets in China financial industry with the intelligence support engine with an integration of modern statistical signal processing, fuzzy neural network, and genetic algorithms.

Security tools

Tools for Detecting and Preventing Fraud Transactions

Many merchants have attempted to develop comprehensive strategies for detecting and preventing fraud. With the right tools and technologies because of the risk inherent in a CNP transaction environment. Merchants can apply these strategies to safely conduct business online without simply accepting fraud as a "cost of doing business." Until recently, many of the best risk assessment and fraud management solutions were designed and targeted only towards larger merchants—even though merchants of all sizes are equally vulnerable. In fact, merchants with smaller sales volumes can be at even greater risk due to relative inexperience in fraud detection and a lack of dedicated fraud management resources,[1]. Fortunately, powerful tools and technologies for fraud management are now available—and affordable—for merchants of all sizes. With these technologies, e-commerce merchants have the opportunity to implement fraud management programs using any or all of these three key functions:

Automated transactional risk scoring

Specific logic and settings can help to distinguish normal purchase behavior from risky transactions. Fraud risk is calculated based on multiple data factors and assigned a numerical score for each transaction. The scores, which serve as relative risk indicators, determine "next steps" for that transaction according to a merchant's preferred operating procedures.

Real-time categorizing and resolution

Transactions with risk scores exceeding certain thresholds—determined by either the merchant or the fraud solution provider—can be automatically placed into different categories for further action. Generally, atransaction is either immediatelyaccepted or rejected—but it can also be flagged for manual review if it falls somewhere between those two categories. Depending on the fraud solution provider, this categorization process may require manual efforts to synchronize with the authorization, settlement, and fulfillment procedures. Fortunately, some providers allow the fraud service to operate "in-line" with the payment authorization flow, requiring minimal intervention by the merchant, and streamlining business processes.

Post-purchase transaction management Optimal fraud service offerings should also include an interface for reviewing transactions that fall between the "accept" and "reject" thresholds, so than members of the merchant's staffcan determine the appropriate activity on a transaction with a single dashboard. The dashboard can include multiple tools and features to assist merchants not only with the initial resolution of a transaction, but follow-up activities such as reporting and performance analysis. It is important to note that the life cycle of fraud management does not begin and end simply with the purchase attempt. In order to continue proactively handling fraud attempts (as well as to resolve chargebacks and disputes efficiently), merchants need a database that can maintain detailed records and be used to understand transaction trending over an extended period of time.

Re-presenting and resolving fraudulent chargebacks can be a complex and time-consuming effort. Dashboards like the ones mentioned above can help easily extract details about a transaction to help win re-presentment attempts. Some fraud solution providers will outsource transaction review and chargeback re-presentment efforts for an extra cost. Merchants need to evaluate the appropriate level of risk management they can administer internally versus outsource, dependent on budget, staff, and other resources available.

Adjusting Fraud Rules and Parameters One common pitfall to avoid is the "one and done" mentality—too often, merchants dedicate a resource to configuring fraud parameters once, but not to ensuring that the parameters are still relevant weeks, months, or years later. Fraud trends evolve rapidly and detection tools need an equally quick response to remain effective. Regardless of which tools merchants are using to prevent fraud, those tools should be referenced against reports and analytics on a regular basis. Merchant staff should also be trained to react to immediate critical occurrences, such as a sudden attack from a fraud ring in a particular geographical location. These may require significant—but temporary—changes to the existing fraud settings. With these powerful fraud management capabilities, online retailers of all sizes can efficiently: determine what levels of risk are acceptable for various products, order profiles, shopping behaviors, and other combinations of factors adjust rules and logicas needed, based on

evolving fraud patterns easily categorize all orders, ideally including a resolution procedure that flows "in-line" with the payment process streamline administrative processes during the entire life cycle of a transaction By integrating fraud management tools into checkout processes, even small eCommerce businesses are empowered. Fraud management becomes an intuitive, practical, controllable business process.

Risk Scoring

Online retailers can use dozens—or even hundreds—of different factors to screen and categorize all attempted purchases for indicators of possible fraud. These data factors can be focused on payment method details, shipping choices, velocity (or frequency) behavior, geo-location details, and other characteristics. The more data that is collected and referenced to determine each transaction's score, the more accurate that score will be. The more advanced risk assessment models typically use a scoring engine to compare as many transaction characteristics as possible against fraud triggers defined by the merchant and the service provider. Here are some examples of rules that might contribute to a negative risk assessment:

- A single IP address has been used with multiple payment cards in the last "x" days.
- The shopper's billing address is more than "y" miles from the shipping address.
- The e-mail address has been flagged in a negative database of known fraud activity by other merchants participating in the same fraud detection strategy.
- The BIN (Bank Identification Number) on the payment card indicates the transaction comes from a high-risk country.

Using a combination of these factors can be especially beneficial for merchants engaging in international ecommerce, where factors like address verification are unreliable by themselves.An algorithm calculates a numerical score based on a weighted point system assigned to each "rule" like those listed above. For example, if the first rule (IP address) is triggered, it may add 50 points to the score. And if the third rule (e-mail address in a negative database) is triggered, it may add another 250 points to the score. Each score is then matched against a merchant's profile settings to determine how the transaction is to be resolved or reviewed. Risk scoring parameters enable near-instantaneous analytical and workflow results. Online retailers should select a fraud solution provider that allows simple and frequent adjustments to scoring parameters, based. on a merchant's preferences and ability to review transactions manually. Different businesses can set up widely varying scoring parameters and order resolution rules to address their specific needs. For example: A seller may deem requests for overnight delivery of heavy items or high-quantity items to be an order that requires review, while overnight delivery of one small camera is considered completely normal. Items that are considered staples or commodity products mayhaveless rigid rules than luxury items, such as electronics and jewelry, which are more likely to appeal to fraudsters? An airline could set up stricter fraud policies for holiday flights or international destinations. Risk assessments reports help analyze the effectiveness of manual reviews, and spot opportunities to eliminate costly review practices when analysis shows them to be unnecessary. According to one study, merchants ultimately accept over 70 percent of the orders they manually review, and 57 percent of merchants accept 90 percent or more of manually reviewed orders, [2].To cut review costs, merchants may prefer to limit manual reviews to suspicious transactions exceeding certain dollar thresholds, which can vary by product, geography, or other parameters. With these sophisticated yet user-friendly capabilities, merchants of all sizes can significantly bolster their defenses against the high costs of fraudulent transactions. The following illustration shows how the scoring and assessment process can work in real time as a transaction is being processed.

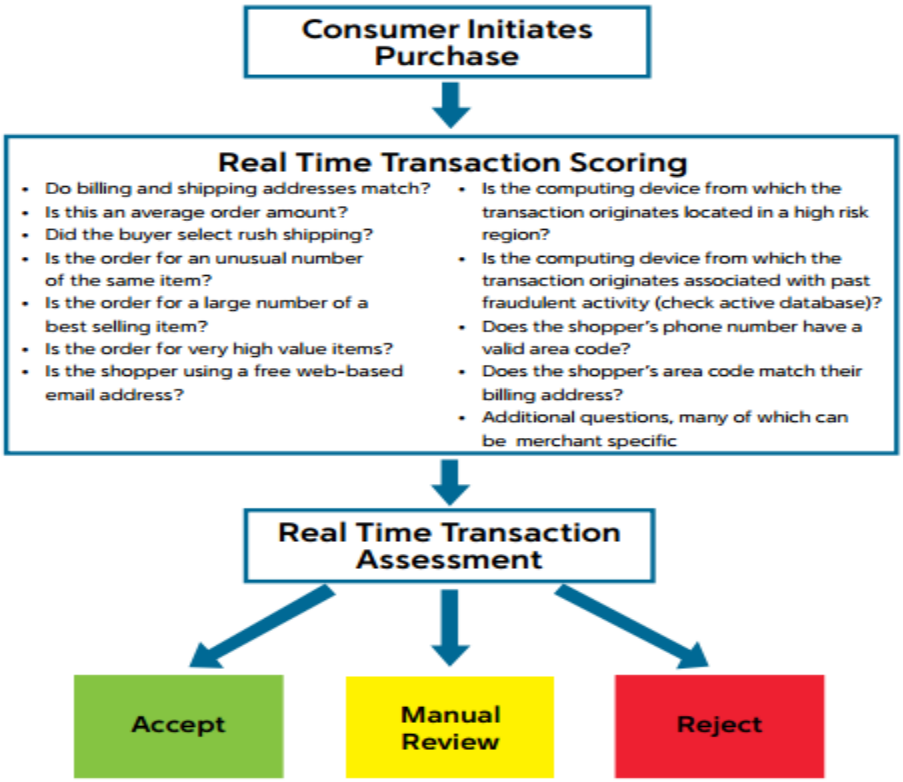

Fig-4:This is a simplified illustration of how a transaction scoring and assessment process can become an automated part of processing any on-line transaction.

Trust and E-Commerce

Trust is the reliance on the integrity, ability, etc. of a person or thing. The concept of trust has been widely analyzed in different areas of study. Psychologists, sociologists and economists among others define trust from different views. Trust is a personal characteristic by psychologists, as a social framework by sociologists, and as an economic mechanism for selection by economists. In addition, trust is a very complex construct, which has many definitions. For example, there seems to be a distinction between interpersonal trust and organizational trust. These are diverse definitions of trust, but all point in the same direction Interpersonal trust is trust in which the trustee is another individual. The target of trust is the person, which is not based on their position, title, or because they represent an organization. Trust is a method of dealing with uncertainty; when dealing with independent agents, institutions or providers of resources (including knowledge), one trusts them if one accepts their characterization of what they will do. Trust can be amoral notion (X trusts Y to act in X's interests), or not (X trusts Y to perform some task T). Adopting the attitude of trust towards others means that one can plan and cooperate more efficiently, at the cost of greater risk of wasting resources when trust is misplaced. There is background technical information on cryptographic systems, including Public Key Cryptography, the system underlying SSL the basis for every e-commerce trust infrastructure. Encryption is the process of transforming information before communicating it to make it unintelligible to all but the intended recipient. Encryption employs mathematical formulas called cryptographic algorithms, or ciphers, and numbers called keys, to encrypt or decrypt information. There are some of secure solutions for reduce concerns on using e-commerce include : Symmetric Cryptography ,Public-Key Cryptography, Modern Cryptography Systems (A Hybrid Approach), The Key Management Problem, Digital Signatures, Digital Certificates. A secure awareness of the packages listed in the ecommerce consumer confidence help. A model to understand e-commerce trust is provided below (model developed by Cheskin and Archetype Studio). Four phases can be distinguished: unawareness, building trust, confirming trust, and maintaining trust. Obviously, the aim of every ecommerce Web site is to arrive at the latest phase, which will be called lock-in in this thesis. Although the last phase is the most interesting one to an ecommerce Web site, the second phase, building trust, is the most important one. By completion of this phase, one travels from the trial threshold to the purchase threshold. As the figure shows, building trust is a long process of several Web site specific activities: browsing, searching, comparing, considering, validating, assessing, registering, transacting, and confirming. As will be discussed and investigated, building trust in e-commerce Web sites is

primarily achieved by pursuing several good Web design strategies. Building trust in a Web site is not only a matter of using an appropriate Web design strategy. There are some factors, which we call extraneous factors that have a great impact on trust but cannot be influenced by the developer of an e-commerce Website. Lack of consumer trust in e-commerce merchants-commerce technology, and the social, financial and legal infrastructures of the e-commerce environment, poses a major challenge to the large-scale uptake of business to consumer e-commerce.

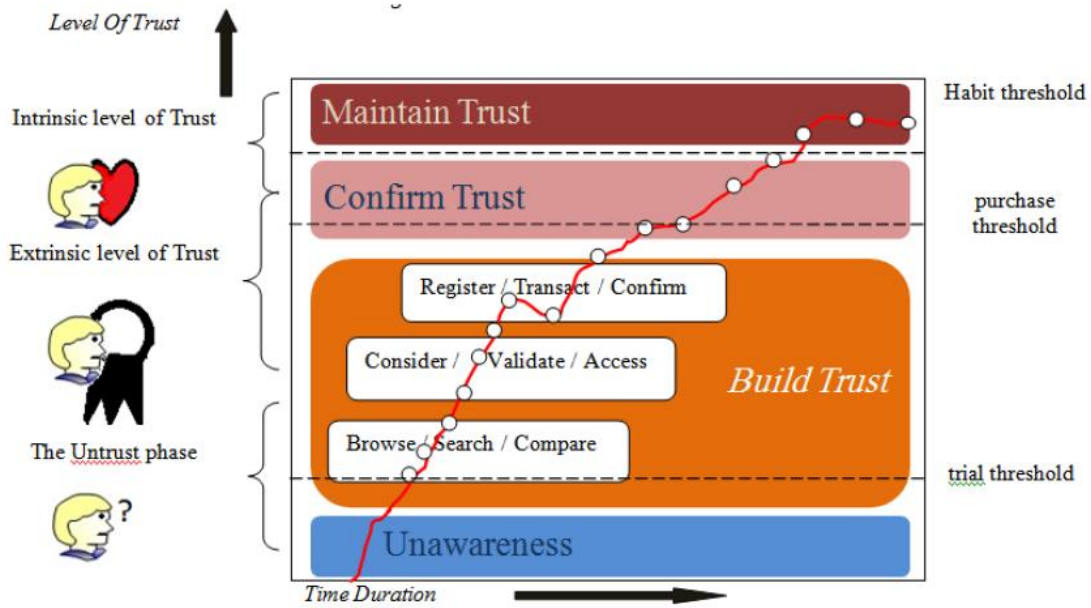

Fig-5: A Model to Understand E-commerce Trust
Source, [6]

Four extraneous factors can be distinguished that have an impact on trustworthiness in an ecommerce Web site: increased experience with using the Internet, higher numbers of hours online at home, use of the Web for financial services, and a significant reliance on e-mail. Note that these factors not only increase trustworthiness, but also result in an increase of online spending. Trust is built on a foundation with a multitude of influential elements. If the e-commerce website cannot attractive the consumer or visitor, the greater the likelihood the visitor will go elsewhere, like a competitor's site.

Address Verification Systems

Address verification systems (AVS) are a widely- used fraud detection tool, but one that is no longer effective on its own for several reasons. For example, AVS does not apply to international purchases. In addition, legitimate customers may mistype their address or use a new address not yet known to their bank. On the other side, fraudsters often know to make sure the billing address and the billing zip code match in order to get an AVS match response. AVS should always be used for the best interchange qualification and for additional safety, but is only one of many factors used in overall risk calculation.

The Benefits of Fraud Management Tools for eCommerce Merchants

- Access fast, efficient ways to help filter out risks
- Instantly accept or denymost orders based on easily defined and easily changed rules
- Quickly adjust scoring and resolution parameters to optimize results for changing business needs
- Reduce staff time spent on costly manual reviews of orders that don't "fit the mold" of an ideal order
- Focus more staff attention on growing the business instead of thwarting fraud
- Stay current with the latest tactics of fraud perpetrators
- Reduce overall chargeback costs and use an integrated fraud dashboard to manage chargebacks that do occur.an ecommerce operation can take steps to effectively minimize the risks of transaction fraud at checkout.

Advanced fraud management services are fast, flexible, and affordable. Even small online retailers can utilize sophisticated, real-time risk assessment as an integral part of the checkout process, and lay a

foundation of security best practices on which their business can grow.

Practices for Online Retailers

Online retailers should consider implementing these best practices:

- Deploy a combination of end-to-end encryption and tokenization to simplify PCI compliance and protect customers' payment card data from being stolen and used fraudulently.
- Make sure all employees understand the risks of card-not-present transactions. Compensate for the lack of in-store controls with real-time screening using both payment information and anti-fraud intelligence from other sources.
- Enable proactive security measures. Don't accept fraud as "just anothercost of doing business."
- Every ecommerce merchant can wield the power to detect and stop most attempts to make fraudulent online purchases.
- Configuring the right kind of fraud logic in the early stages of your business can help you avoid problems later.
- Leverage as many tools as are available to you through your payment provider and other resources.
- Experiment with the use of automated order screening early on, when transaction volume is low and suspicious behavior anomalies are more easily recognized. Constantly re-evaluate the risk settings and resolution rules that will catch most fraud attempts without requiring many transactions to be reviewed or denied.
- Participate in forums, webinars, and other shared experiences with fellow merchants; in many ways, collaboration is the greatest advantage we have against fraud.
- Additionally, for support and guidance on the nuances of fraud management, eCommerce merchants should talk to their payments processor.
- Ask how to use both payment and non-payment information to detect fraud and gain visibility into shopper behavior.
- Get recommendations on how to define rules that effectively assess order risk and determine the appropriate resolution of each order.
- Find out what level of support to expect in implementing industry best practices for reporting, scoring, order resolution and scoring parameters.
- Find out if the payment processor's solution has a user-friendly workflow for resolving transactions and managing chargebacks and reversals.
- For additional information about PCI compliance, data security, and automating fraud detection as part of a payment processing solution, contact First Data or visit our website at FirstData.com.

Quing and Server Utilization

Cloud computing "refers to both the applications delivered as services over the Internet, and the hardware and system software in the data centres that provide those services", according to Armbrust *et al*.[3], and "is a utility oriented distributed computing system consisting of a collection of inter-connected and virtualized computers that are dynamically provisioned and presented as one or more unified computing resource(s) based on service-level agreements established through negotiation between the service provider and consumers" according to Buyya *et al*.[4]. Both definitions capture the real essence of this new trend in distributed systems, where both software applications and computing infrastructure are moved from private environments to third party data centres, and made accessible through the Internet. Cloud computing delivers infrastructure, platform, and software (applications) as subscription-based services in a pay-as-you-go model. The datacenter is the collection of servers where the application to which you subscribe is housed. It could be a large room in the basement of your building or a room full of servers on the other side of the world that you access via the Internet. A growing trend in the IT world is virtualizing servers. That is, software can be installed allowing multiple instances of virtual servers to be used. In this way, you can have half a dozen virtual servers running on one physical server.

The quality of service (QoS) in providing internet protocol (IP) based service in wireless and wired networks have been carried by Jukka Manner *et al.* [7]. The study focused on the shortcomings of real time transport protocol (RTTP), in siginia and its umo protocols. The study focused on the methodologies like strict flow shaping at the network edge, coupling of micro-mobility and quality of service (QoS) protocols, advanced reservations, pre handover negotiations and context transfer methodologies were adopted for improvement in quality of service (QoS) [5] discussed the OPNET simulation modeling and analysis of enhanced Mobile. To facilitate simulation studies of Mobile IP performance and comparative analysis of enhanced mobile IP handover mechanisms, development was done based on simulation model of Mobile IP using OPNET modeling environment

CONCLUSION

Trust building in e-commerce web sites is very hard and very difficult to develop and make it reliable. Lots of financial frauds have been committed and

bleach of business agreements with fake IPs and convincing costumers on reliability of ecommerce will involve different steps of growth in level of trust to be actualized. The maximum trust can be built at the presentation where the client interacts with the vendor's website because he does not know the underlying technologies or tools used. So by displaying the maximum presentation layer attributes trust can be developed. The research introduced the top issues in the current e-commerce environment, namely privacy, security issues and reliability. These two issues are one of the main reasons to be addressed to further e-commerce development. It elaborated about security issues like identity theft and financial fraud, its effect on e-commerce growth, reasons behind it and the importance of providing secure communication networks in order to attract and successfully retain customers. It also explained privacy issues in e-commerce and the importance of well-established privacy settings that ensures confidentiality and safety of customer's information. This was all done in order to facilitate the further expansion and development of e-commerce as optimization process is not undermined from the models that have ever be developed by various researchers.

REFFERENCE

1. Strategy J. Research. 2011. ". Payment Card Issuer Strategies. 2010.
2. Sullivan RJ. The changing nature of US card payment fraud: industry and public policy options. Economic Review-Federal Reserve Bank of Kansas City. 2010 Apr 1;95(2):101.
3. Armbrust M, Fox A, Griffith R, Joseph AD, Katz R, Konwinski A, Lee G, Patterson D, Rabkin A, Stoica I, Zaharia M. A view of cloud computing. Communications of the ACM. 2010 Apr 1;53(4):50-8.
4. Buyya R, Yeo CS, Venugopal S. Market-oriented cloud computing: Vision, hype, and reality for delivering it services as computing utilities. InHigh Performance Computing and Communications, 2008. HPCC'08. 10th IEEE International Conference on 2008 Sep 25 (pp. 5-13). Ieee.
5. Park T, Dadej A. OPNET simulation modeling and analysis of enhanced Mobile IP. IEEE; 2003 Mar 20.
6. Najafi I. The role of e-commerce awareness on increasing electronic trust. Life Science Journal. 2012;9(4):1487-94.
7. Manner J, Toledo AL, Mihailovic A, Munoz HL, Hepworth E, Khouaja Y. Evaluation of mobility and quality of service interaction. Computer Networks. 2002 Feb 5;38(2):137-63.