Survey of Privacy and Security Issues in Spice World E-Commerce Website

Palak Patel[1] Rucha Patel[2] Vishwa Patel[3] Trupti Pathrabe[4]
[1,2,3]UG Student [4]Assistant Professor
[1,2,3]Department of Computer Engineering
[1,2,3]SAL Institute of Technology & Engineering Research, Ahmedabad, Gujarat, India

Abstract— The term used for world-wide communication of computers over a single network is referred as Internet. It is a public network and consisting of thousands of private computers network which are connected together. Privacy is needed while doing online business with customers over the internet and it has become an ongoing and increasing relevant for the users, developers, administrators, policy makers as well as technologist. This paper lays the groundwork with brief introduction of recent trend in E-commerce with people; particularly it managing spice from the different area which are famous for providing online selling for growers and have better choice to end users. E-commerce Security is a part of the Information Security framework and is specifically applied to the components that affect e-commerce that include Computer Security, Data security and other wider realms of the Information Security framework.

Key words: Cryptography, E-Commerce, Security Issues, Security Threats

I. INTRODUCTION

E-commerce is mostly used to describe shopping over the Internet. It consists of the buying and selling of Indian Spices Products or services through such electronic systems as the Internet and other computer networks. As a new form of business, it is the commercial activity which utilizes online shopping or online business of spice products with better security system. Security is the one of the principle and continuing concerns that restrict customers and organizations engaging with E-commerce. Web E-commerce applications that handles payments such as online banking, Electronic transactions using some gateways i.e. PayUMoney,Debit card,Credit card,PayPal have more compliance issues are at increased risk from being targeted than other websites and greater consequences if there is a data loss or alteration. Online shopping websites having certain steps to buy a product with the safe and secure transactions. With the rapid expansion and use of E-commerce, privacy has become an ongoing and increasing concern for the users, providers, technologist as well as the policy makers. While it is difficult to complete a transaction in e-commerce by a user without providing private information, protecting that information from proliferating is another difficult issue for the providers, technologist and the policy makers.

II. RELATED LITERATURE

Web security is to meet the security expectations of users and developers. To that end, Web security is concerned with client-side security, server-side security and Transaction Security for E-commerce Web Application.

Secure transmission of informationis concerned with the techniques and practices that will guarantee protection from eavesdropping and intentional message modification. Client-side security is concerned with the techniques and practices that protect a user's privacy and the integrity of the user's computing system. Server-side security is concerned with the techniques and practices that protect the Web server software and its associated hardware from break-ins, Web site vandalism and denial of service attacks. [1]

In the digital business arena privacy is usually related to the use of customer information. Transacting typically makes the exchange of large amounts of personal data which are necessary. This may either be necessary for the e-business transaction itself (i.e. credit card information, banking account details, delivery details) or desired by the e-business partner: collecting customer data that later may be analyzed, shared with other businesses or even be sold. [2]

The most usual means of providing privacy to users with privacy information are privacy statements. In this way companies inform the website users what their policy is regarding data protection, and provide the information about who is collecting data and what it will be used for. Another way of increasing trust in online privacy of a website is to use privacy seal verifications. These trust-marks are usually links to the organizations that work towards a safer online environment by establishing whether a website follows an accredited privacy policy. If the website is verified by these companies, the user will be more comfortable with providing personal information. These seals might not be sufficient enough to provide the consumer with a trusting attitude towards the company but will reduce some of the uncertainty with regard to a website’s credibility and reinforce trust.[3]

The shopping through E-commerce has penetrated all segments of goods ranging from groceries to electronic goods and even vehicles. Rapid growth in mobile computing and communication technologies has facilitated popularity of E-commerce. The main impediment in growth of E-commerce is cyber fraud and identity theft. Hackers are people who carry out the cybercrime. Hence, poor security on E-Commerce web servers and in users computers is core issue to be resolved for rapid growth of E-commerce. This paper provides directions for E-commerce security so as to improve customer confidence in E-commerce shopping.E-Commerce refers to the exchange of goods and services over the Internet. [4]

Trading in the online shopping accessed through internet between business-to-business (B2B), business-to-consumer (B2C) and consumer-to-consumer (C2C) is mainly used in e-commerce. Parties involved in this kind of trading exchange information including private information like addresses (exchanged as mailing/billing information), credit card number (exchanged for payments), etc. to complete a transaction. Here is the catch; information exchanged by the parties is stored and warehoused for other business purposes like direct marketing, research, selling to third parties, etc.E-commerce is considered as a powerful tool to collect consumer’s private information. The same tool and their use in business also interfere on the privacy of individuals. [5]

Recognizing the fact that, in any given e-commerce scenario, there are five interconnected and interacting components (people, software, hardware, procedures and data), one comes to the conclusion that e-commerce systems are (and should be looked upon as) information systems, comprising a technological infrastructure and an organizational framework, rather than pure technological infrastructure. Therefore, addressing the problem of security in e-commerce must be done in an information system setting. In such a setting, security can be defined as an organized framework consisting of concepts, beliefs, principles, policies, procedures, techniques, and measures that are required in order to protect the individual system assets as well as the system as a whole against any deliberate or accidental threat [6]. Operationally, in order to compile such a framework, the pertinent requirements must be identified first. [2]

E-commerce web site owners on one side are thinking of how to attract more customers and how to make the visitors feel secured when working on the site, on the other side how the end users should rate ecommerce website and what they should do to protect themselves as one among the online community. Due to the increase in warnings by the media from security and privacy breaches like identity theft and financial fraud, and the elevated awareness of online customers about the threats of performing transactions online, e-commerce has not been able to achieve its full potential. Many customers refuse to perform online transactions and relate that to the lack of trust or fear for their personal information.[7]

Authorization, trustand authentication can not be used interchangeably because authorization and authentication have to be considered as basic security services of applications, while trust can not be considered as a basic security service but as an outcome resulting as a combination of the appropriate use of basic services.E-commerce web site owners on one side are thinking of how to attract more customers and how to make the visitors feel secured when working on the site, on the other side how the end users should rate ecommerce website and what they should do to protect themselves as one among the online community.[8]

III. Purpose of Survey

The main purpose of survey is online selling and purchasing of product over the secure transactions. and understand why we need security in E-commerce because some of that purchases are illegal but we focus on legal purchasing. for that we have to discuss about the different security issues and try to solve it. We survey about the efforts of various government organizations, private companies, security expert and e-commerce professionals in formulating policies and developing tools to help e-commerce users to protect their privacy. Online a cyber-crime, also leaves physical, electronic evidence, but unless good security measures and threats are taken, it may be difficult to trace the source of the cyber-crime. Security measures in e-commerce have various method and strategies for different purpose.

IV. E-business cycle

Security is a very important in a E-business. An e-business platform is commonly known as the software that enables a retailer to sell online. But many small & medium size retailers go above and beyond to extend their operations and improve efficiency.Almost anything can be bought such as Spices, toys, clothing, cars, food. some of that purchases are illegal but we will focus on only the legal purchasing.

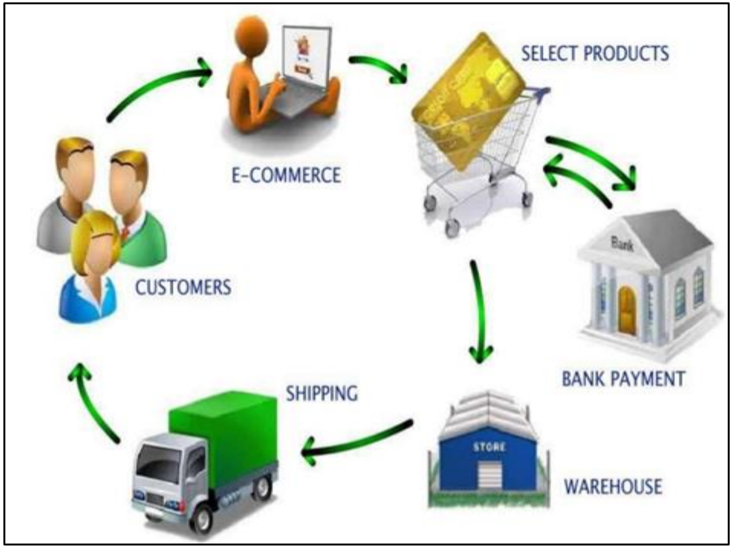
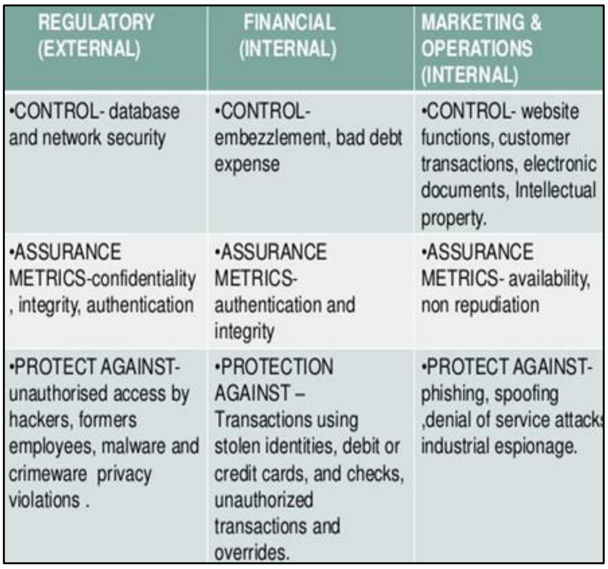


Fig. 1: E-Business cycle[10]



REGULATORY (EXTERNAL)	FINANCIAL (INTERNAL)	MARKETING & OPERATIONS (INTERNAL)
•CONTROL- database and network security	•CONTROL- embezzlement, bad debt expense	•CONTROL- website functions, customer transactions, electronic documents, Intellectual property.
•ASSURANCE METRICS-confidentiality , integrity, authentication	•ASSURANCE METRICS- authentication and integrity	•ASSURANCE METRICS- availability, non repudiation
•PROTECT AGAINST- unauthorised access by hackers, formers employees, malware and crimeware privacy violations .	•PROTECTION AGAINST – Transactions using stolen identities, debit or credit cards, and checks, unauthorized transactions and overrides.	•PROTECT AGAINST- phishing, spoofing ,denial of service attacks industrial espionage.

Fig. 2: E-commerce Security strategy[11]

According to Alexa.com a website that measures and harvests online traffic information and regularly reports rankings among popular websites, eBay and Amazon unsurprisingly, rank first and second respectively in the shopping sector. Another site, Rank.com further dissects the ranking, reporting that Amazon’s and eBay’s multiple country domains like Amazon.de, eBay.co.uk, Amazon.ca rank as the top visited websites globally. (Rank.com, 2004) [9]

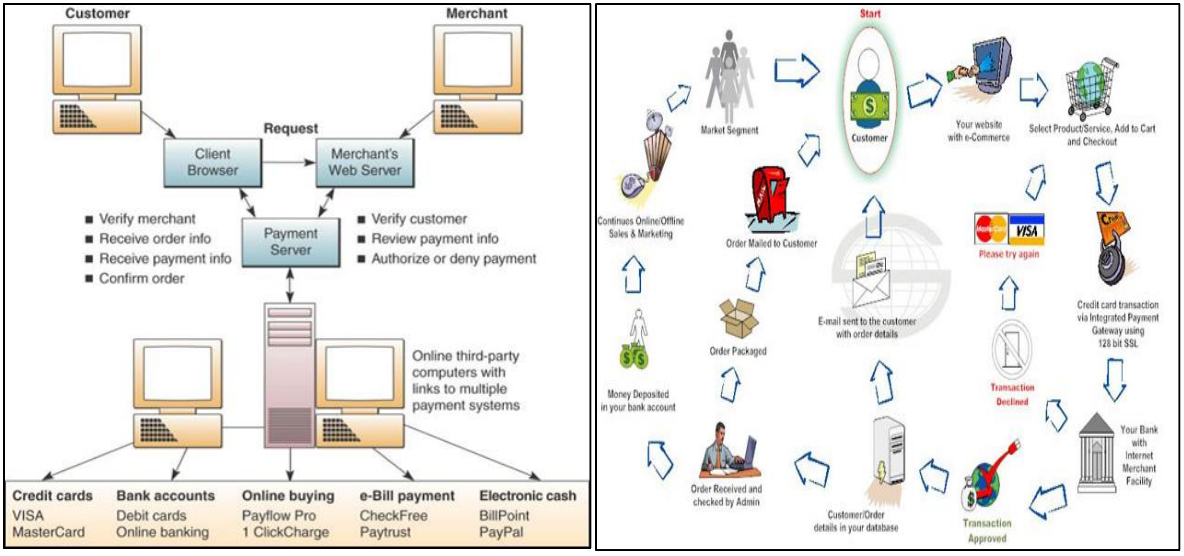

Customer
Merchant
Request
Client Browser
Merchant's Web Server
Payment Server
■ Verify merchant
■ Receive order info
■ Receive payment info
■ Confirm order
■ Verify customer
■ Review payment info
■ Authorize or deny payment
Online third-party computers with links to multiple payment systems
Credit cards
VISA
MasterCard
Bank accounts
Debit cards
Online banking
Online buying
Payflow Pro
1 ClickCharge
e-Bill payment
CheckFree
Paytrust
Electronic cash
BillPoint
PayPal
Start
Customer
Market Segment
Your website with e-Commerce
Select Product/Service, Add to Cart and Checkout
Continues Online/Offline Sales & Marketing
Order Mailed to Customer
Please try again
Credit card transaction via Integrated Payment Gateway using 128 bit SSL
E-mail sent to the customer with order details
Order Packaged
Money Deposited in your bank account
Transaction Declined
Your Bank with Internet Merchant Facility
Order Received and checked by Admin
Customer/Order details in your database
Transaction Approved

Fig. 3: E-commerce payment lifecycle[10]

V. SECURITY TOOLS

A. Public key Infrastructure (PKI):

It is a technology that can be used to establish identities, encrypt information and digitally sign documents. PKI identifies and manages relationships of parties in anelectronic exchange, serving a wide array of security needs and uses unique DigitalCertificates(DC) to secure E-commerce.

B. Proxy server:

Proxy servers are enable user privacy and anonymous surfing.It is mainlyused for facilitate security, administrative control or caching services.

C. Software of Encryption:

Encryption is the translation of electronic data into cyphertext, which can not be easilyunderstood by anyone except authorized parties.

D. Digital Certificates:

DC is a data structure that securely binds individual or entity to a public key used incryptographic operations.

E. Digital Signatures:

An Authentication mechanism that enables the creator of a message to attach a code thatworks as a signature.

F. Firewalls:

A network of computer controls access between networks and it consists of gatewaysand filters.

VI. PURPOSE OF SECURITY

A. Data Integrity

Data Integrity refers to the trustworthiness of information resources. Data Integrity ensure that the information has not been tampered and that is implemented by message digest or hashing.

B. Access Control

Access Control governs the resources. Those resources access by users on the system. Also, uses valid IDs and passwords

C. Data Confidentiality

Data Confidentiality refers to limiting information access and disclosure to authorized user and preventing access by unauthorized ones. That is provided by encryption/decryption.

D. Authentication and Identification

Ensuring that someone is who he or she claims to be is implemented with digital signatures.

E. Non-repudiation

Non-repudiation prevents either sender or receiver from denying a transmitted message which is implemented with digital signatures.

VII. SECURITY ISSUES

E-commerce is defined as online selling and purchasing of products over secure transactions such as online payments. It is mainly provide online services and facilities through electronic systems such as the Internet and to a lesser extent, other computer networks. Online privacy and security are most important part of E-commerce. privacy is linked to legal requirements and good practices regarding the management of personal data, security refers to the technical aspects of this management and protection. [3] Protecting user data from online fraud can not be achieved without proper security. E-commerce security is the protection of e-commerce assets from unauthorized access, use, alteration, or destruction. Security features are necessary to build a secure system.

A. Integrity:

Data integrity is the assurance that data transmitted is consistent and correct, that is, it has not been tampered or altered in any way during transmission.

B. Authentication:

Authentication is a means by which both parties in an online transaction can be confident that they are who they say they are and non-repudiation is the idea that no party can dispute that an actual event online took place

C. Non-repudiation:

It is a property of the transaction that positively confirms that a particular client did indeed request the transaction in question without having the ability to deny making the request.

D. Online fraud:

While doing online purchases credit card information will be stolen. Hackers target credit card files and other customer information files on merchant servers; use stolen data to establish credit under false identity.

E. Privacy:

Information exchanged must be kept from unauthorized parties.

F. Availability:

It is defined in an information security context ensures that access data or computing resources needed by the appropriate personnel are both reliable and available in a timely manner.

G. Dummy data:

- Viruses: They have ability to replicate and spread to other files; most also deliver a “payload” of some sort (destructive or benign); include macro viruses, file-infecting viruses, and script viruses.
- Worms: They are designed to spread from computer to computer.

VIII. SECURITY THREATS

Security threat is an object, person, or other entity that represents a constant danger to an asset.

Management must be informed of the various kind of threats facing the organization. By examining each threat category, management effectively protects information threw policy, education, training, and technology. There are many threats to e-commerce security. With the help of latest technology and the internet at that are still such a new phenomenon there are many issues with websites and there is still no way to make your e-commerce website completely secure without certain threats always looming.

1) E-commerce websites are vulnerable to fraud from external and internal sources. These incidents include credit card fraud, anything being entered into the system by rogue employees, hackers etc.
2) Security issues relate to internal connections between business networks and interface through transactions done by the customer and the network. Hackers can gain access to internal systems using their e-commerce website.
3) Malicious software and computer viruses are two important threats. Viruses are normally from external sources and can corrupt files on website if introduced into the internal network. Viruses can completely destroy a computer system and disrupt the operations of the website.
4) One of the greatest threats to an e-commerce is poor management. When the management is not committed to ensuring security and does not support budgets for purchase of anti-virus software licenses, that keep internal networks robust will cause pose a bid security threat. The lack of proper an anti-virus, makes the e-commerce vulnerable to viral attacks.

IX. CONCLUSION

Our study has covered the general perspective of privacy and security in e-commerce. In our study we have learnt about e-commerce and its privacy issues. E-commerce is widely considered the buying and selling of products over the internet, but any transaction that is completed solely through electronic measures can be considered e-commerce. Day by day E-commerce and M-commerce playing very good role in online retail marketing and peoples using this technology day by day increasing all over the world.

ACKNOWLEDGEMENT

– I thank to Mr. Piyush Patel, Professorof SAL Institute of Technology and Engineering Research Ahmedabad- 60 for his support and motivation.
– I thank to Mrs. TruptiPathrabe, Assistant Professor of SAL Institute of Technology and Engineering Research Ahmedabad- 60 for her support as internal guide.
– I thank to Mr. Sunay Patel, Senior employee of MICO BOSCH.LTD, Bangalore-30. for his constant support and encouragement for completing this research paper.

REFERENCES

[1] Pradnya B. Rane, Dr. B. B. Meshram. “TRANSACTION SECURITY FOR E-COMMERCE APPLICATION” VJTI, Mumbai, ISSN- 2277-1956

[2] Sokratis K. Katsikas 1, Javier Lopez 2, Günther Pernul 3. “TRUST, PRIVACY AND SECURITY IN E-BUSINESS: REQUIREMENTS AND SOLUTIONS”1Dept. of Information & Communication Systems Engineering, University of the Aegean, Greece 2Dept. of Languages and Computation Sciences, University of Malaga, Spain 3Dept. of Management Information Systems, University of Regensburg, Germany

[3] Milan Mandić. “PRIVACY AND SECURITY IN E-COMMERCE” Banja Luka, Bosnia and Herzegovina, UDK 658.8:004.738.5

[4] Santosh Kumar Maurya“CYBER SECURITY; ISSUE AND CHALLENGES IN E-COMMERCE”, NagendraPratap Bharati, Vol 5, No 1(2016)

[5] Li Xiaoming, Valon Sejdini. “PRIVACY IN E-COMMERCE”, School of Computer Science, University of Windsor, Windsor, Ontario, Canada.

[6] E. Kiountouzis: “APPROACHES TO THE SECURITY OF INFORMATION SYSTEMS”. In S. Katsikas, D. Gritzalis and S. Gritzalis (Eds.): “INFORMATION SYSTEMS SECURITY”, New Technologies Publications, Athens, Greece, 2004 (In Greek).

[7] Niranjanamurthy M 1, DR. Dharmendra Chahar 2. “THE STUDY OF E-COMMERCE SECURITY ISSUES AND SOLUTIONS” Research Scholar, Dept. of MCA, Msrit, Bangalore, India 1 HOD. Dept. of CS & IT, Seth G. B. Podar College, Nawalgarh (Jhunjhunu) -333042, India 2. ISSN (Online): 2278-1021

[8] Revathi C, Shanthi K, Saranya A.R. “A STUDY ON E-COMMERCE SECURITY ISSUES” Dhanalakshmi Srinivasan College of Arts and Science for Women, Perambalur, Tamilnadu, India. ISSN(Online): 2320-9801

[9] James Christopher “E-Commerce: Comparison of On-line Shopping Trends,Patterns and Preferences against a Selected Survey of Women”November 2004

[10] https://www.google.co.in/search?q=e+commerce+payment+cycle

[11] https://www.google.co.in/search?q=security+strategy.