International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 07 Issue: 03 | Mar 2020 www.irjet.net p-ISSN: 2395-0072

DATA PRIVACY, TRUST ISSUES AND SOLUTIONS IN ELECTRONIC COMMERCE

MEGHNA NIKAM[1] & JAGRUTI ROKADE[2]

[1]Student: Semester-II, M.Sc.(I.T)
[2]Saket College of Arts Science & Commerce Kalyan, Thane, Maharashtra, India

---

Abstract – *Privacy and Security has become an discussion topic among users. E-Commerce is a part of Information Science. If the Privacy and Security threats are not rejected, users will never trust, visit or shop at E-Commerce site. Electronic Commerce has increased dramatically in recent years, because of the revolution in Information Technology. The services provided by e-commerce companies are affected by several factors like privacy, security, trust, risks. Maintenance of users privacy online is the main concerns of E- commerce. Here will discuss about the overview of privacy, trust, risk, issues and their possible solutions.*

Key Words- E-commerce; Data privacy issues, E- commerce; security, E-commerce; risk, E-commerce; trust, Digital E-commerce Online Shopping, Security threats.

INTRODUCTION :

E-Commerce is an activity of buying and selling of products electronically. E-commerce Security is a part of Information Security framework and is applied to the components that affect e-commerce. The components that affect e-commerce includes Computer Security, Data security and other wider elements of Information Security framework. E-commerce business has became very popular now-a-days and into existence with many privacy issues solutions. E- commerce Privacy is a major issue in electronic commerce, as privacy enforcement and its monitoring is not easy to handle. Some people consider privacy as a fundamental rights and people take it as a tradable commodity.

The benefits of e-commerce includes availability, easy to access, various selection of products and services, and international reachability are attracting peoples online to join e-commerce business. The growth and trust upon E-Commerce business depends totally on the security and privacy for the development of E- Commerce. The most important factor of E-commerce is to build trust among users. A complete and secure system is required to maintain the privacy in e- commerce.

In this paper we propose a model that would consider customers privacy and security concerns and how they affect perceived risk. Here, we will study the relationship between the elements and customers trust and behavior in online business methods.

WEB SECURITY:

Web security is one of the major principal and continuing concerns that restricts customers and organizations of e-commerce. The aim of this principal is to explore the security in e-commerce B2C and C2C websites form both customers and organizations. With the rapid development of e-commerce security issues are arising from people's point of view. Web applications increasingly communicate with third party services. This introduce new security challenges due to the complexity of applications to coordinate with its state components and web client over Internet.

RESEARCH HYPOTHESIS:

The security and privacy concerns will raise the level of fear of customers' regarding proper outcomes of online transactions. The level of fear, uncertainty, and anxiety are some of risk aspects, which in return affect the level of customers' trust. Therefore, we found that it is important to explain each aspect, in distinct and try to find relationships among them.

Security:

Security threats are defined as any action that would lead to loss in network elements, or data as a result of data breach (i.e. modification, disclosure, or destruction), denial of service attacks, and scam. Therefore, security is protecting systems against such threats. The main three goals of information security are confidentiality, integrity, and availability (CIA).

Confidentiality is defined as limiting un-authorized access to confidential data. In other words, confidentiality means using encryption algorithms to safeguard transmitted data over the network and stored data in servers. Authentication methods (i.e. passwords) could be used to prevent unauthorized access to data. Integrity goal can be stated as ensuring correct transaction.

Moreover, integrity is used to guarantee data accuracy and completeness . The system availability is concerned about handling, transferring, and storing data for those who need it .

Privacy:

The concept of privacy has different definitions, which makes it challenging when trying to present components of such concept. Privacy is defined as the "right to be left alone", furthermore, being able to control the disclosure and access to personal information. Another definition of privacy is the right of individual to control what information should be disclosed and what should not. There are several definitions for privacy, privacy definitions fall into three categories: 1) Notice: Customers' right to control access to their personal data. 2) Control: The level of control that customers have over their personal data. 3) Access: Limiting access to customers' personal data to only authorized people

Trust and behavioral intention:

Trust could be seen from different perspectives (i.e. psychology, computer, marketing, science, communications, information systems, and political discipline). Due to many definitions of trust, the relationship between trust and perceived risk is not clear. Some researchers consider the risk as an outcome of trust. Additionally, we will consider the same relation between trust and behavioral intention proposed and tested in. The study suggested that level of trust that customers' have would positively affect customers' behavioral intentions.

E-Commerce Transaction Phase				
Information phase	Negotiation phase	Payment phase	Delivery phase	
Security Measures				
Confidentiality Access Control Integrity Checks	Secure Contract Identification Digital Signatures	Encryption	Secure Delivery Integrity Checks	

Chart 1: **E-Commerce Transaction Phase**

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.

DIGITAL E-COMMERCE CYCLE:

Security is very important in online shopping sites. Now days, a huge amount is being purchased on the internet, because it's easier and more convenient. Almost anything can be bought such as music, toys clothing, cars, food and even porn. Even though some of these purchases are illegal we will be focusing on all the item's you can buy legally on the internet. Some of the popular websites are eBay, iTunes, Amazon, HMV, Mercantile, dell, Best Buy and much more

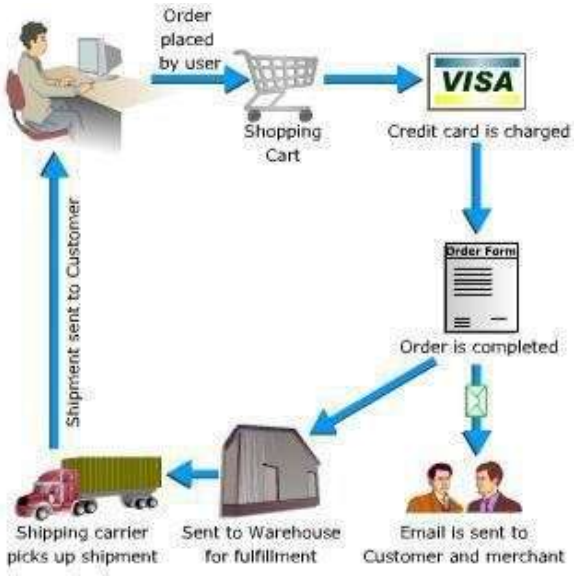

Fig -1: **Digital E-commerce cycle SECURITY ISSUES:**

E-commerce security is the protection of e- commerce assets from unauthorized access, use, alteration, or destruction. While security features do not guarantee a secure system, they are necessary to build a secure system.

Security features have four categories:

- **Authentication**: Verifies who you say you are. It enforces that you are the only one allowed to logon to your Internet banking account
- **Authorization**: Allows only you to manipulate your resources in specific ways. This prevents you from increasing the balance of your account or deleting a bill.
- **Encryption**: Deals with information hiding. It ensures you cannot spy on others during Internet banking transactions.
- **Integrity:** prevention against unauthorized data modification.

SECURE ONLINE SHOPPING GUIDELINES:

- Shop at Secure Web Sites
- Research the Web Site before You Order
- Read the Web Site's Privacy and Security Policies
- Be Aware of Cookies and Behavioural Marketing

CONCLUSIONS:

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. E- commerce security is the protection of e-commerce assets from unauthorized access, use, alteration, or destruction. Dimensions of e-commerce security; Integrity: prevention against unauthorized data modification, No repudiation: prevention against any one party from reneging on an agreement after the fact. Authenticity: authentication of data source. Confidentiality: protection against unauthorized data disclosure. Privacy: provision of data control and disclosure. Availability: prevention against data delays or removal.

Security, privacy, perceived risk, and trust issues are critical in ecommerce. Understanding the relationship between these concepts is even crucial. In this paper, we have discussed some insights for security, privacy, perceived risk and trust concepts in ecommerce. In addition, we proposed a security-privacy-perceived risk-trust preliminary theoretical model for customers in e-commerce. The model presents the relationship between privacy, security and perceived risk, and perceived risk and level of trust. The proposed model in this paper provides a basis for further research on clarifying and understanding the relationship between trust, and other concepts in e-commerce.

ACKNOWLEDGEMENT:

I would like to express my special thanks of gratitude to our guide Asst. prof "Rajeshree munde" as well as to Dr. S. K. Raju Principal Saket College of Arts science & Commerce for his valueable guidance. We precise our sincere thanks to "Praseena Biju", HOD " Information Technology", and also other employee colleagues ofthe department for his or her kind co-operation.

Secondly I would also like to thank our parents and friends who helped us a lot in finalizing this project within the limited time frame. We also precise our sincere thanks to the library staff members of the college.

REFERENCES:

[1] https://www.forbes.com/sites/marymeehan/201 9/11/26/data-privacy-will-be-the-most- important-issue-in-the-next-decade/#2f97b40c1882

[2] https://www.omicsonline.org/open-access/data- privacy-issues-and-possible-solutions-in- ecommerce-2168-9601-1000294-104325.html

[3] https://www.researchgate.net/publication/32845 7534_Data_Privacy_Issues_and_Possible_Solutions_ in_E-commerce

[4] https://www.researchgate.net/publication/31148 9590_Privacy_security_risk_and_trust_concerns_in_ e-commerce

[5] https://www.academia.edu/

[6] https://www.tutorialspoint.com/e_commerce/e_c ommerce_security.htm