

# Data Privacy in E-Commerce

Prashant Bhat, Mullapudi Hari Prasad, Deepshikha Sinha, Madhulika Mailin Sagorkar, Sephora Fernandes

Department of Computer Science and IT, Garden City University, Bengaluru, Karnataka, India

Department of Marketing & HR, Christ Institute of Management, Lavasa, Maharashtra, India

## ABSTRACT

The internet has been flourishing since its invention. The retailers as well as the whole sellers are now shifting their premise from brick to mortar. This paper showcases how the e-commerce websites are flourishing and how they are conducting the day-to-day transactions as well as reaching out to vast customer database with the help of the ERP systems. The main concern that has been faced by these sites is how well they can protect the data provided by the customers, ensuring that the information provided by them stays confidential as well as doesn't get transferred and taken advantage of. The paper deals with how to have data privacy in E-Commerce sites as well as how to face and prevent them from happening.

**Keywords:** Electronic Commerce, Data Privacy, Internet transactions, Customers Trust.

## I. INTRODUCTION

One of the most complex legal issues facing e-commerce ventures today is privacy. Many sites have little interest in actively profiling their users or discovering personal information about them. However, these sites will often collect significant amounts of personally recognizable data that may trigger liability risks.

Some of this material is effectively provided by clients. For instance, the WGU site gathers names, physical and email locations, and MasterCard data through structures. Clients may likewise intentionally supply individual data in their strung discourse messages, which are filed on the site. Some of this information is inactively gathered again. Routine data about each visit is recorded by the crowd server. A portion of the place's flag advancements enable outsider sponsors to track clients' perusing propensities. (NORJIHAN ABDUL & ZAILANI, 2009)

The main task is to assess the liability risk of a site's information collection practices. We can separate this assignment into four fundamental advances. To begin with, we should figure out what data is gathered by the site. Evaluation the potential liability for those information collection practices. Third, we must choose whether to develop a privacy policy to disclose those practices. And fourth, we must verify our compliance with statutes or regulations.

The emergence of e-commerce has brought about many benefits to a country's economy and individuals, but the openness of the Internet has given rise misuse of personal data. A few nations have instituted statutes and strategies to ensure the data protection of their natives and partnerships. Be that as it may, numerous creating nations, for example, Nigeria are yet to establish any methodology, regardless of the abnormal state of wholesale fraud and online extortion. Distinctive ways to deal with information security and assurance are found in various nations. These can be by and large delegated the self-direction approach, as

utilized as a part of the United States and the administration approach.

E-commerce security is the protection of e-commerce assets from unauthorized access, destruction, alteration, or use so its dimensions to be studied are- Integrity, Privacy, Non-repudiation, Authenticity, Confidentiality, and Availability. This paper would throw light on E-commerce privacy, security, its purpose, different security issues and how consumer's trust and purchasing behaviour is affected by it. (Joseph A, Andrew S, & Dinesh S, 2008)

## II. LITERATURES REVIEW

Internet business is an effective device for business change that enables organizations to upgrade their production network task, achieve new markets, and progress administrations for clients and in addition for suppliers. Actualizing the E-business applications that give these advantages might be outlandish without a sound, steady way to deal with E-business security. Internet business has exhibited another method for doing exchanges everywhere throughout the world utilizing web. Associations have changed their method for working together from a customary way to deal with grasp E-business forms. As people and organizations increment data sharing, a worry with respect to trade of cash safely and helpfully finished the web increments. Security is a need in an E-business exchange. The motivation behind this paper is to clarify the significance of E-business security and will examine quite great protection, secure internet business convention, open key framework, computerized mark and declaration-based cryptography methods in online business security. In this paper various approaches have presented that increases the level of security. (Mihir, Ran, & Hugo, 1998)

The online platform is a place where in everything is seen but not touched and felt. It's also intangible except for the seen part as the main part of online

selling and buying is based on the attractiveness of the product as well as the way it is projected. The validity of these sellers is the thing that these e-commerce sites have to prove. Along with e-commerce companies even general public size up regarding the security obligations and ingress possible scientific way out and also, they must approach, analyze and rectify the threat included (Ms. Palak & Dr. Akshat, 2016). For all that electronic commerce is proliferating globally, public are even now antipathetic to trade with it for the reason that of the certainty and seclusion concerns. Intrinsically, there are countless research papers have been brought out during the past years on different concerns connected to electronic commerce. Concerning on the internet data safety affairs, at most 10.6 percent of the assenters seems completely secured for filling the confidential data regarding oneself on the net but many (around 57.7 percent) doesn't agree with regards and almost 31.8 percentage of them linger on this concern (Thaw, Mahmood, & Dominic, 2009).

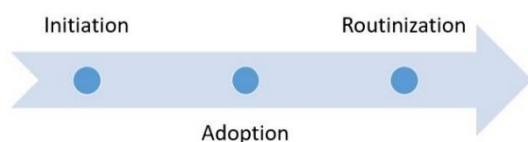
There is some categorization based on predecessors which will affect the buyer belief and buyers' discerned threat so as to approach online commerce operations, that are:

- I. Skill-based
- II. Perception-based
- III. Character bearings
- IV. Influence-based

Consumers through online provide product information and recommendations on the e-commerce sites where in the reviews are sometimes negative which lead to bringing down the market share as well as the ratings of the app. A recent example of this would be: the feud of snap deal and snap chat. People confused between these two websites, which lead to the falling of the ratings of snap deal. The negative reviews on the websites are sometimes, forged. In order to solve and identify

between the genuine and fake reviews, an algorithm is designed where in the reviews are calculated and depending on it, the genuine ratings of the website is determined. (KYUNG-AH, BYUNG-RAE, & TAI-YUN, 2002)

Evolution is the only thing that pushes the boundaries for getting better and more advanced. The same thing has happened with e-commerce websites where in an idea to sell products to customers as well as reach a large number of the consumers at the same time. Researchers are faced with thousands of e-business adoption articles to find when seeking and reviewing those most relevant to their own projects. (Chen & Holsapple, 2013). They have manually check and coded the article for the validity as well as how well is it to design as well as analyze the secondary data that has been collected.



The e-commerce sites have two major things: buying and selling of products/services. The benefits of the e-commerce are:

- ✓ People can buy goods with a click of a button
- ✓ People can buy these goods without moving
- ✓ Services such as: Banking, ticket booking etc., can be possible.

#### The opportunities are:

- ✓ The investment has been made by Indian Venture Capitalist are over \$5 million in 7 e-commerce infrastructures.
- ✓ Critical mass of internet users
- ✓ Rising middle class with disposable income

#### The challenges are:

- ✓ Cash on delivery
- ✓ High cash burn rate
- ✓ High inventory poor supply chains
- ✓ Ethical issues

#### ✓ Security concerns

The world is in the era of evolution and is moving towards e-commerce application for the completion of their daily work. E-commerce has become one of the medium of people to work and complete their daily tasks. Such as paying bills, shopping can be done in one click. Online Shopping has reduced the conventional purchase approach. People at present do rely on internet for their work and it has become an integral part of their life. The internet exerts an increasingly strong influence of people's everyday life. The wide range of using cyberspace for the activities has become a threat to information privacy and it gives bad result on personal information privacy. (NORJIHAN ABDUL & ZAILANI, 2009)

With parallel to financial disclosure, privacy disclosure in e-commerce is also considered to be an essential unregulated environment. In order to help accountants and security regulators to project the consequences of a competitive regime with the support of study of privacy standards, disclosure practices and demanded audit. This research paper has set up a framework for such type of study, by gathering data from field and analyse privacy standards and the effectiveness of opt-out practices of some high-traffic e-commerce web sites. They have explored the implication of these results for the consequences of a competitive regime for regulation of reporting.

Authentication measure design model for ecommerce systems. Its effectiveness was reflected and with the help of a SET integrated ecommerce system. (KARIM, MICHAEL, & SHYAM, 2003)

Authentication measures design model and methodology for e commerce systems:

- ✓ Authentication security requirements at system time should be captured and satisfied.
- ✓ Provide measures in s chronological order.

- ✓ Contain effective countermeasures against the set of all known security attacks related to authentication.
- ✓ Block malicious user requirements at system design time.
- ✓ Can be directly incorporated into high level design documents of ecommerce systems.
- ✓ Provide guidelines for avoiding security pitfalls and also can be used with security aware technology like CORBA or can be implemented as a stand-alone module for EC systems.

Thus, converting the model into a flow chart for implementation needs is straightforward and easily can be done.

Security is clearly a very important factor governing the size of the e-commerce market. E-commerce security concerns include payment confidentiality, payment integrity, and payment authorisation for Internet transactions. Currently, many potential e-commerce participants are reluctant to participate in Internet e-commerce because of these concerns, not least because many users perceive. (Shazia, Khalid, & Rashid Jalal, 2012)

Internet shopping as the riskiest shopping method by comparison with other methods of payment. In this paper we consider the influence of the mass media, including television and newspapers, on e-commerce consumer perceptions. Given that cases of security breaches are often sensationalised by these media, we observe that the mass media may actually be unduly increasing e-consumer concerns, and thereby adversely affecting the e-commerce marketplace.

### III. RESULTS AND DISCUSSION

In the recent years data privacy has always been an issue faced by the population. To collect the primary data, we conducted a survey on a sample population. Population were asked some general questions about

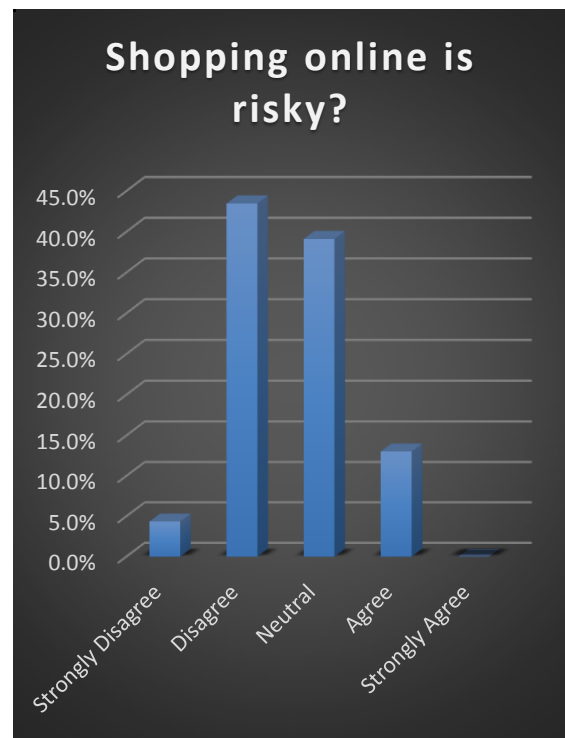
what they think of the online transactions and its security.

The first question asked to them to know about their perspective on risk in online shopping.

So, from the following data collected we can interpret that around 43.5% of the respondents disagreed with the statement that “Shopping online is risky”.

**Table 1**

Shopping online is risky?	
Strongly Disagree	4.3%
Disagree	43.5%
Neutral	39.1%
Agree	13.0%
Strongly Agree	0.0%



**Figure 1**

The next question asked to them was to know about the customer behaviour about letting out their credit card details online without any assurance of the safety of the details.

The following data collected shows that around 34.8% of the population are not hesitant to share their credit card details online.

**Table 2**

While shopping online, I hesitate to give my credit card number	
Strongly Disagree	8.7%
Disagree	34.8%
Neutral	26.1%
Agree	26.1%
Strongly Agree	4.3%



**Figure 2**

**IV. CONCLUSION**

From the survey conducted that the public is not trusting the e-commerce sites to 100%. So, there are

ways to increase the trust among the customers who shop online:

- ✓ Develop well-polished web design.
- ✓ Build civilized things like “About Us” page.
- ✓ Provide the contact information of the e-commerce site.
- ✓ Provide a separate page in website on privacy policies.
- ✓ Secure check-in and check-out options.

Security Plan:



**Figure 3**

**V. REFERENCES**

- [1]. Chen, L., & Holsapple, C. W. (2013). E-Business Adoption Research: State of the Art, VOL 14.
- [2]. J. C., A. J., & D. D. (2008, February). The Impact of consumer perceptions of information privacy and security risks on the adoption of residual RFID technologies. Communications of the Association for Information Systems, 22, 1-32.
- [3]. K. J., M. M., & S. S. (2003, May). Privacy in E-commerce: Development of Reporting Standards, Disclosure, and Assurance Services in an Unregulated Market. Journal of Accounting Research, 41(2), 285-309.
- [4]. K.-A. C., B.-R. L., & T.-Y. K. (2002). Open Authentication Model Supporting Electronic Commerce in Distributed Computing. Electronic Commerce Research, 2, 135-149.
- [5]. M. B., R. C., & H. K. (1998, March 13). A Modular Approach to the Design and Analysis of Authentication and Key Exchange Protocols.

30th Annual Symposium on the Theory of Computing, pp. 1-26.

- [6]. M. G., & D. D. (2016, June). E-Commerce-Study of Privacy, Trust and Security from Consumer's Perspective. *International Journal of Computer Science and Mobile Computing*, 5(6), 224-226,231.
- [7]. N. G., & Z. M. (2009, March). Personal Information Privacy Protection in E-commerce. *WSEAS TRANSACTIONS on INFORMATION SCIENCE and APPLICATIONS*, 6(3), 407-416.
- [8]. S. Y., K. H., & R. Q. (2012, March). Cryptography Based E-Commerce Security. *International Journal of Computer Science Issues*, 9(2), 132-137.
- [9]. Thaw, Y. Y., Mahmood, A. K., & Dominic, P. D. (2009). A Study on the Factors That Influence the customers' Trust on E-commerce Adoption. *International Journal of Computer Science and Information Security*, 4(1,2), 153,154,157.
- [10]. Vikram, A. (n.d.). E-commerce: opportunities and challenges. E-commerce: opportunities and challenges.