International Journal of Research in Finance and Marketing (IJRFM)
Available online at: http://euroasiapub.org
Vol. 13 Issue 05, May – 2023
ISSN: 2231-5985 | Impact Factor: 8.132
(An open access scholarly, peer-reviewed, interdisciplinary, monthly, and fully refereed journal.)

RELATED TO E-COMMERCE AND SECURITY

Dr. Sameer Singhal

Assistant Professor, Accountancy and Business statistics

Government College Tonk

ABSTRACT

In stark contrast to this trend is Ramachandran's (2004a) comprehensive investigation on the effects of DPEP, which was conducted both in the lab and in the field. She draws attention to a variety of resources, some of which include the reports produced in addition to the Joint Review Missions (formerly known as will be responsible for the evaluation. You may obtain all of this information by logging into the District Information System for Education. which is abbreviated as DISE for short. Regrettably, the capabilities that are now available impose considerable limits on the imaginative use of such data. To be more specific, the disaggregation of gender has not resulted in the creation of methods that are reasonable and sensible for dealing with the intricacies of gender disparity in a range of settings. The underrepresentation of women in positions of power is a significant element that contributes significantly to the existence of these inequities.

Keywords: - *ecommerce has security, digital e commerce*

INTRODUCTION

E-commerce The supporting infrastructure of online commerce is subject to all aspects of information security, including computer security, data security, and other components of the information security architecture. that are more comprehensive. When discussing "Information Security," the term "security" refers to a component that falls under the wider umbrella term. E-commerce security is unlike any other type of security because of the complexity of its problems, and it is one of the most obvious parts of security that has an effect on the end user because of the daily payment contacts that the firm has with the client. The protection of an online shopper's financial information is essential to the success of any transaction they attempt to carry out in an online environment. The protection of users' personal information and safety is of the utmost importance in the field of contemporary electronic technology. Concerns about privacy and safety are also raised by other developments in this area, such as mobile commerce. It has been discovered that customers

International Journal of Research in Finance and Marketing (IJRFM)
Available online at: http://euroasiapub.org
Vol. 13 Issue 05, May – 2023
ISSN: 2231-5985 | Impact Factor: 8.132
(An open access scholarly, peer-reviewed, interdisciplinary, monthly, and fully refereed journal.)

are concerned about their privacy in a variety of contexts, including social networking platforms, online commerce, electronic medical records, and electronic recruiting tools. This lack of belief has been connected to the scepticism that has been expressed. Both consumers and companies have been hesitant to engage in e-commerce due to the persistent worry that their private information, including financial details and identification details, may become public.

The term "online shopping" refers to the activity of making purchases of products or services from an online store by accessing the services of such a business. Typically, an online store will have its own set of protocols for assuring the safety and security of the customer. The e-commerce sector is beginning to handle security concerns on its internal networks in a methodical yet consistent manner. The individuals who are in charge of ensuring the safety of e-commerce platforms can study up on and put into practise the available standards for the protection of computer systems and networks. Even if the security of online commerce is still in its infancy, the education of customers on various security concerns will prove to be the most important component. The most significant threat to online business comes from malicious software known as Trojan horses. These programmes are designed to infiltrate client computers and are able to spoof or go around the majority of the authentication and authorization processes that are required for an online purchase. The most straightforward approach to installing software on a distant computer is to include it as an attachment to an email. Consumers' worries about their privacy have moved to the forefront as a direct result of the rise in the number of instances involving identity theft and impersonation. When it comes to managing an online business, it is imperative that the requirements of the customer come first at all times.

OBJECTIVES

1. To do research about online business Information security includes security as one of its components
2. To conduct a historical investigation of the development of online business.

International Journal of Research in Finance and Marketing (IJRFM)
Available online at: http://euroasiapub.org
Vol. 13 Issue 05, May – 2023
ISSN: 2231-5985 | Impact Factor: 8.132
(An open access scholarly, peer-reviewed, interdisciplinary, monthly, and fully refereed journal.)

Web security

Customers and businesses are discouraged from engaging in electronic commerce due to one of the primary and ongoing concerns, which is the security of the web. The purpose of this seminar is to investigate the customer and organizational perceptions of the level of security present on business-to-consumer (B2C) and business-to-business (C2C) websites. As a result of the lightning-fast growth of e-commerce, individuals are becoming increasingly concerned about security risks. The safety of the transaction is the most fundamental and important a problem that requires resolution as the volume of internet commerce increases. This seminar explored the security challenges of activities associated to e-commerce and provided solution strategies from two different angles: technology and system. The goal of the conference was to enhance the environment for the expansion of electronic commerce and to support its further growth. A large number of today's online applications make use of services that are provided by third parties. Integration brings up additional security considerations due to the difficulty of synchronising the internal states of an application with those of the component services and the web client via the internet. When making a purchase online, there is always an additional layer of safety that is built in.

E-commerce Transaction Phases			
Information Phase	Negotiation Phase	Payment Phase	Delivery Phase
Security Measures			
Confidentiality Access Control Integrity Checks	Secure Contract Identification Digital Signatures	Encry-ption	Secure Delivery Integrity Checks

Figure: 1 software and other products that are functionally comparable

Internet companies face an annoying and sometimes damaging annoyance in the form of viruses. Since they cause legitimate online firms to experience disruption, they are most

International Journal of Research in Finance and Marketing (IJRFM)
Available online at: http://euroasiapub.org
Vol. 13 Issue 05, May – 2023
ISSN: 2231-5985 | Impact Factor: 8.132
(An open access scholarly, peer-reviewed, interdisciplinary, monthly, and fully refereed journal.)

accurately referred to as a denial of service (DoS) weapon. The most significant danger to business conducted via the internet is posed by Trojan horse remote control software and other products that are functionally comparable. On a customer's computer, a Trojan horse is a piece of malicious software that seems to be genuine software in order to get access to sensitive data and launch fraud and other types of attacks. Once they have established a presence in a network, it may be difficult to completely remove them from the system. The computer of the victim may be hacked and used by an attacker to place fraudulent orders, and the server of the online retailer would have no means to check whether or not these transactions were legitimate. Because the hacker can see everything in clear text before it is encrypted, It is possible for the code of the Trojan horse to circumvent any existing security measures, such as the protection provided by passwords, encrypted client-server.

well as an increase in the number of online customers who are aware of the risks associated with conducting business online. The potential of doing business online has been hindered as a result of the convergence of these factors. Customers frequently refrain from transacting business via the internet because they either do not have faith in the system or are concerned that the security of their personal information will be breached.

Digital E-Commerce Cycle

Online retail platforms must prioritize customer safety above anything else. Due to the fact that it is less difficult and more convenient, a significant proportion of shopping is done on the internet these days. Almost everything, even pornographic material, may be purchased, including music, toys, clothing, vehicles, food, and even food. Despite the fact that some of these transactions are unlawful, we are going to concentrate on all of the items that may be bought lawfully via the internet. There are several prominent websites, but some of the most well-known ones include.

International Journal of Research in Finance and Marketing (IJRFM)
Available online at: http://euroasiapub.org
Vol. 13 Issue 05, May – 2023
ISSN: 2231-5985 | Impact Factor: 8.132
(An open access scholarly, peer-reviewed, interdisciplinary, monthly, and fully refereed journal.)

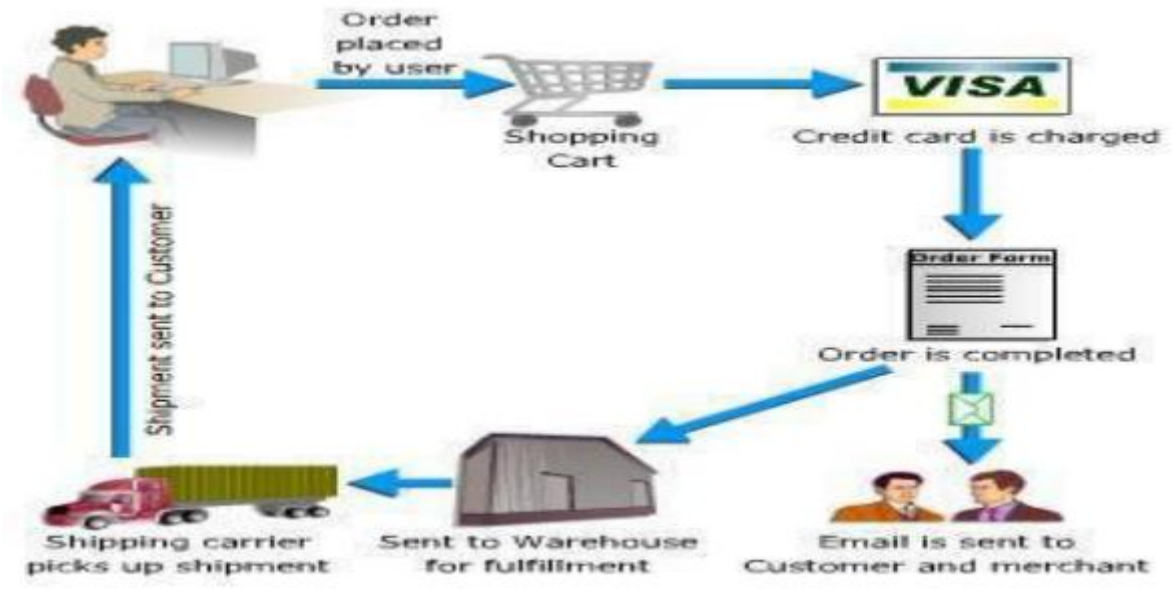

Figure 2: Digital E-Commerce Cycle

In this particular illustration, the user types information into a computer; if all of the information is accurate, the procedure moves on; otherwise, the user is required to submit payment information before the purchase can be processed, such as a credit card or debit card. The subsequent order is then processed by the firm, and after email notifications are sent to both the buyer and the seller, the company eventually delivers the product to the buyer's residence.

Purpose Of Security

1. Encrypting and decrypting data allows for the data to be kept confidential, which is one of the benefits of using these two methods.
2. The functions of authentication and identification can both be accomplished with the help of digital signatures. This makes it possible to verify that the person with whom one is communicating is, in fact, the person that they claim to be.
3. Third, Access Control determines which components of the system a user may access and how that access can take place for that user. There are genuine credentials being used for the login.

International Journal of Research in Finance and Marketing (IJRFM)
Available online at: http://euroasiapub.org
Vol. 13 Issue 05, May – 2023
ISSN: 2231-5985 | Impact Factor: 8.132
(An open access scholarly, peer-reviewed, interdisciplinary, monthly, and fully refereed journal.)

4. The information has not been altered in any way, as evidenced by the fact that the data's integrity has been preserved. This objective can be accomplished through the use of hashing or message digestion.
5. Non-repudiation, also known as the promise not to contest a purchase or transaction, was made possible with the use of digital signatures, which were used in the process. A communication that can be read by humans is referred to as being in plaintext or cleartext. Ciphertext is encrypted in such a way that it cannot be deciphered by humans. Decryption is the process that is directly opposed to encryption. The term "algorithm" is sometimes abbreviated to "cypher" when referring to cryptography. It is a piece of mathematical software known as a "function." The majority of assaults have the primary objective of stealing the key.

Security Issues

When we talk about we are referring to what we mean by "e-commerce security." Even while the presence of security measures is required for the construction of a secure infrastructure, this alone is not enough to ensure the system's integrity. You have the option of selecting from the following four different levels of safety: Authentication is the process of confirming that your identity is exactly what you claim it to be.

- If you enable this function, you can be certain that no one, not even dishonest hackers, will be able to access your online banking account. You may do so with complete peace of mind. You will find the open-access, professionally reviewed International Journal of Engineering Research and Technology (IJERT) on its website, which is located at www.ijert.org. Number assigned to the magazine by the ISSN is 2278-0181. NCRIT 2016 Conference Proceedings, Volume 4, Number 27, Special Issue, 2016 3 is cited as the following: [Proceedings of the NCRIT Annual Conference for the Year 2016] Provides you, and only you, with the ability to make changes to your
- The utilization of resources in certain ways. This stops you from adding more money to your account balance or removing a bill from your account. Encryption is a technique for concealing information.

International Journal of Research in Finance and Marketing (IJRFM)
Available online at: http://euroasiapub.org
Vol. 13 Issue 05, May – 2023
ISSN: 2231-5985 | Impact Factor: 8.132
(An open access scholarly, peer-reviewed, interdisciplinary, monthly, and fully refereed journal.)

- During Internet banking transactions, it is impossible to listen in on other people's conversations. Auditing is the process of maintaining a record of activities. Merchants
- You should conduct an audit to demonstrate that you purchased a certain item. Integrity is the protection against the introduction of illegal data.
- Modification Non-repudiation: protection against action taken by any one party
- Refrain from backpedaling on a deal after it has already been made Availability: the protection of data against delays or loss.
- elimination. – Distributed denial of service assaults, often known as DDOS, are carried out by cybercriminals who install software agents on a number of computers that belong to third parties and then command those systems to make requests to the desired target simultaneously.
- Sniffers are pieces of software that get unauthorized access to data that is moving over a network.
- Theft of software by the unauthorized copying of files from the company's servers.
- Theft of hardware, most notably laptops.

Understand E-Commerce Services

What types of services are available to us through the medium of online commerce? The list is rather large, and some of the services are brand new and ground-breaking in their respective fields. For instance, several organizations are now offering paid memberships to various forms of information. In the past, there existed an option for this kind of service; but, it was always somewhat pricey, and it typically necessitated the use of a specialized dial-in line. These services are now available to everyone worldwide via the internet. Another way for the service provider to boost income is to reduce the price of the information they supply to their customers.

The development of electronic commerce via the Internet has also resulted in the emergence of a new type of service: the provision of electronic library services for material that may be deemed sensitive or secret. A service that saves and makes organizations' own digital information accessible to them can be subscribed to by the organizations themselves. Internet

International Journal of Research in Finance and Marketing (IJRFM)
Available online at: http://euroasiapub.org
Vol. 13 Issue 05, May – 2023
ISSN: 2231-5985 | Impact Factor: 8.132
(An open access scholarly, peer-reviewed, interdisciplinary, monthly, and fully refereed journal.)

is used to send the information back to the organization after it has been processed. As an illustration, Organization A maintains a contractual relationship with Vendor V in order to archive and store electronic information. A data center that has a significant quantity of storage is established by Vendor V, which also accepts delivery of Organization A's files. After that, these files are uploaded to the appropriate systems so that personnel from Organization A may access them in a safe manner. Organization A is assessed a price by Vendor V based on the total volume of data that will be stored.

There are a variety of other services that may be obtained through the utilization of electronic commerce. Some of these services include activities that businesses have traditionally carried out but which can now perhaps be carried out at a lower cost. One excellent illustration of This is one method of the exchange of information. Wholesalers and other reseller networks, for instance, need that manufacturers provide them with access to product information and price. In the past, manufacturers have provided distributors with two alternatives for accessing this data. Either the manufacturer would print out copies and distribute them, or the firm would set up intricate and expensive private networks that wholesalers were required to utilise in order to connect to the manufacturer and acquire the data. E-commerce makes it possible for a manufacturer to set up a central website on the internet, which then enables the company's distributors and resellers to communicate with one another online and get the relevant information. The service is not only more affordable but also more prompt.

Buying things through an online marketplace is most likely the type of e-commerce service that comes to mind first. Even in this very conventional service, there are signs of innovation all around us. Some businesses have begun offering digital versions of books as well as music in the form of MP3 files. The time-honored activity of trading items also takes place at this location. The opportunity to shop online is available at a wide variety of locations, and consumers have plenty of options. The ordering process begins with the consumer, who is ultimately the recipient of the delivered items.

Examples of E-Commerce Services

When considering how to implement security precautions for e-commerce services, it may be helpful to utilise as a guide the four key It is also possible for us to presume that accessibility

International Journal of Research in Finance and Marketing (IJRFM)
Available online at: http://euroasiapub.org
Vol. 13 Issue 05, May – 2023
ISSN: 2231-5985 | Impact Factor: 8.132
(An open access scholarly, peer-reviewed, interdisciplinary, monthly, and fully refereed journal.)

is a problem for all forms of online business. The concerns associated with the other three types of e-commerce services will also change according to the sort of e-commerce service that you make use of. make available to your customers. The three examples that are provided in the following sections illustrate three different ways in which security may be required for e-commerce services.

Communications Security

The PC belonging to the customer and the server belonging to the online retailer both need to have their information protected while it is in transit. This is what communications security for e-commerce apps protects. This may include sensitive information such as the digits from a credit card or the password to a website. It is also possible for it to include sensitive information that is transmitted from the server to the client's PC, such as files associated with the customer.

Encryption is the only viable option for dealing with this problem. The ability to encrypt communication is built into the majority of common web browsers. If HTTPS is used instead of HTTP, this is the approach that will be implemented by default. When secure HTTP (HTTPS) is utilized, a connection known as a Secure Socket Layer (SSL) is established between the client and the server. All of the data that is sent and received via this connection is encrypted.

As more people become aware of the risks associated with providing personal information such as credit card numbers over the internet, the use of HTTPS has become mandatory. In the event that a customer's card number is compromised, the consumer will be responsible for no more than fifty dollars' worth of charges.

Advantages of e-commerce

The following is a condensed list of the benefits that business organizations can derive from engaging in e-commerce: E-commerce has the potential to boost revenue while simultaneously cutting expenses. Through the usage of e-commerce, a company is able to penetrate niche markets that are dispersed across a large geographic area. The internet and the

International Journal of Research in Finance and Marketing (IJRFM)
Available online at: http://euroasiapub.org
Vol. 13 Issue 05, May – 2023
ISSN: 2231-5985 | Impact Factor: 8.132
(An open access scholarly, peer-reviewed, interdisciplinary, monthly, and fully refereed journal.)

world wide web are very helpful tools for developing virtual communities that may function as excellent target customers. A meeting of people who have a common interest might be described as a virtual community. However, rather than taking place in the real world, this gathering takes place on the internet.

E-commerce creates more potential for sales for merchants, but it also creates more options for consumers to shop online. E-commerce provides companies with the opportunity to discover new business partners and suppliers as part of their purchasing procedures. Because of the efficiency with which the web can supply information on rival bids, it is much simpler to negotiate pricing and delivery terms when conducting business online. The speed and precision with which firms may share information is significantly improved by the use of e-commerce, which results in cost savings on both sides of the transaction.

Customers are able to explore a greater variety of goods and services from a greater number of vendors while conducting business online, giving them access to a greater number of available options than they would have in traditional retail settings. The advantages of online business extend all the way to the improvement of society as a whole. When sent through the internet, electronic payments for things like tax refunds, public retirement, and welfare support have lower issuance costs, come more promptly and securely, and don't take as much time. In addition, auditing and monitoring electronic payments can be simpler than auditing and monitoring check payments, which can be helpful in reducing the risk of financial loss due to theft and fraud. Through the use of e-commerce, formerly inaccessible regions can get access to goods and services. For instance, the advent of distance learning has made it feasible for people to acquire new knowledge and achieve degrees regardless of the location in which they reside or the number of hours in the day that they have free to devote to academic pursuits.

Security

If you knew that unauthorized parties might potentially tap your transmission of your credit card number, would you still want to transfer it? Integrity problem: how do you tell whether information that has been given to you has been changed by a hacker? Authentication

challenge: how can you determine whether or not the organization that is going to get your information is a legitimate company? Problem with non-repudiation: how can one legally demonstrate that a message was transmitted? These questions cover four of the key conditions that must be met in order for a transaction to be effective and secure. In this part, we will examine how these requirements may be met by utilizing a variety of well-known procedures for the security of online commerce transactions.

Everyone who uses the Internet for online business has a responsibility to be concerned about the safety of their own personal information. Secure Sockets Layer (SSL) and Secure Electronic TransfersTM (SETTM) are two examples of the many protocols that may be used to ensure the safety of a transaction. These security mechanisms, together with public-key cryptography, digital signatures, and digital certificates, will be the topic of discussion in the next few sections. In addition to this, we will offer case studies on organizations like as VeriSign and CyberCash that use these technologies to assist e-businesses in overcoming the issues that they face with regard to security.

CONCLUSION

When most people hear the term "e-commerce," the first thing that comes to their mind is traditional commercial transactions that take place over the internet. However, the term "e-commerce" refers to any type of company that is performed wholly online. Both e-commerce and mobile utilising these platforms continues to skyrocket at an alarming rate all over the world. With regard to the prevention of losses caused by burglary, tampering, inappropriate use, or destruction of e-commerce assets, we are referring to what we mean by "e-commerce security." Concerns regarding the safety of electronic transactions for payments; Integrity is the protection of data from being altered without authorization, No repudiation refers to the prevention of any one party from backtracking on an agreement after it has already been made. Authenticity involves verifying the credibility of the data source. A safeguard against the leaking of confidential information to unauthorized parties. Privacy may be defined as the provision of control over data as well as disclosure. Availability refers to the protection against the deletion or delay of data. Online customers are more vulnerable to being taken advantage of by con artists because they are more likely to make rookie mistakes. People

frequently put themselves in danger by making careless decisions like buying on unprotected sites, exposing an excessive amount of personal information, or failing to maintain adequate privacy safeguards. systems protected from malware.

REFERENCES

1. Niranjanamurthy M, Research Scholar, Dept. of MCA, MSRIT, Bangalore, INDIA1
2. DR. Dharmendra Chahar, HOD. Dept. of CS & IT, Seth G. B. Podar College, Nawalgarh (Jhunjhunu) -333042, INDIA2
3. MohanadHalaweh, Christine Fidler - " Security Perception in Ecommerce:Conflict between Customer and Organizational Perspectives". Proceedings of the International Multiconference on Computer Science and Information Technology, pp. 443 – 449, ISBN 978-83-60810-14-9- 2008- IEEE
4. Yuanqiao Wen, Chunhui Zhou "Research on E-Commerce Security Issues". 2008 International Seminar on Business and Information Management.
5. ShaziaYasin, Khalid Haseeb. "Cryptography Based E-Commerce Security: A Review". IJCSI-Vol. 9, Issue 2, No 1, March 2012
6. Schneider G P, Perry J T 2001 Electronic commerce. Course Technology, Cambridge, MA SSE-CMM 2003 Systems security engineering capability maturity model. SSE-CMM, Model Description Document Version 3.0, June 15, 2003
7. Rashad Yazdanifard, Noor Al-Huda Edres "Security and Privacy Issues as a Potential Risk for Further Ecommerce Development"International Conference on Information Communication and Management - IPCSIT vol.16 (2011)
8. Seyyed Mohammad Reza Farshchi "Study of Security Issues on Traditional and New Generation of E-commerce Model" International Conference on Software and Computer ApplicationsIPCSITvol.9(2011).
9. Rui Wang, Shuo Chen "How to Shop for Free Online Security Analysis of Cashier-as-a-Service Based Web Stores". IEEE S&P‘11 proceedings.
10. V.SRIKANTH "ECOMMERCE ONLINE SECURITY AND TRUST MARKS". IJCET ISSN 0976 – 6375, Volume 3, Issue 2, July- September (2012),
11. Randy C. Marchany, Joseph G. Tront, "E-Commerce Security Issues"Proceedings of the 35th Hawaii International Conference on System Sciences - 2002