

Recent Technological Trends and Security Challenges in Trust-Building in E-Commerce

Yeow Chong Larry Tan¹

¹ University of Mississippi, USA

Correspondence: Yeow Chong Larry Tan, University of Mississippi, USA. E-mail: ytan1@olemiss.edu

Received: October 14, 2019

Accepted: November 20, 2019

Online Published: November 30, 2019

doi:10.5539/ijbm.v14n12p226

URL: <https://doi.org/10.5539/ijbm.v14n12p226>

Abstract

In this research article, the researcher covers the recent trends of E-commerce and security challenges in the trusting-building process. The researcher observed that lack of trust is a consistent barrier to the adoption and implementation of E-commerce for customers in Business Industries. Prior research into the adoption of E-commerce and Internet banking has revealed many other challenges and barriers that hinder the acceptance and engagement in E-commerce transactions. In this research article, the researcher attempts to address some of the challenges, by first gaining insights into each challenge, and providing possible solutions for the difficulties faced as well as ideas for improvements, which ultimately leads to the increased adoption of E-commerce.

Keyword: E-commerce, AI, security challenges

1. Introduction

E-commerce is the process of controlling online selling and purchasing of products and services over internet. It draws on technology, mobile commerce, electronic support system and transfer, production network management, internet marketing, online exchange processing, electric data interchange(EDI) and automation control system which are responsible for controlling the information and data over internet by Joze Kuzic et.al., (2002). There are three areas of E-commerce: online retailing, electronic markets, and online sales. E-commerce is supported by electronic business. Recent trends in E-commerce rising up the business Industries and automation with the help of internet of things. The researcher focused on some of the significant research issues and usage of this technology for laymen, marketing robotization means mechanizing email marketing and scheduling web based life posts. However, marketing computerization has now become the new trend. It gives no indications of halting. It covers areas including customized points of arrival and easy-to-access shopping baskets with the help of technology and security barriers by Soliman, Youssef, M. (2003).

1.1 Background of the Study

The researcher emphasized that the research study on “Recent Technological Trends and Security Challenges in Trust-Building in E- Commerce”. The background of the research study is based on the recent trends of technological concept which are significant with respect to security challenges in trust building in E- Commerce. The Researcher stated that some of the significant factors security challenges in E-commerce for building trust of Industries.

1.1.1 Marketing Automation

Mohamed Hallowed (2017) stated that for a laymen, the marketing automation means automating the email marketing and scheduling social media by post with all possible business transactions. However the marketing automation is now become the mainstream of business transaction in daily to daily life. It is customized the business process and easy to access shopping carts. The researcher stated that some of the marketing automation attributes in business Industries.

- Send out personal E-mail to customers
- Display new products and promotion as per the visitors shopping history.
- Retarget customers for necessary products sales
- Recovers sales and reduce cart abandonment

The researcher emphasized that block chain is one of the advanced technology for security challenges to control the large markets for encouraging enough to get data through the cryptography types of money. Using this technology it is completely free for sellers and anyone to use block chain using without programming. It is model where token are generated in block chain technology to encrypt data for transparency in the use E-commerce. A block of payment is created on the block chain and displayed on the network this happens when the seller creates the item and vessels to buyer. The block is created for each cycle and it is great because of transparency, authentication and freedom for movement of transaction in between one network segment to another network segment by Ye Jun et.al. (2008).

1.1.2 Artificial Intelligent

Sachchidanand Singh and Nirmala Singh(2016) stated that in current usage of technological security parameters is business Industries the Artificial Intelligent (AI) playing a significant role for mapping the business constraints and is one of the biggest enabler for customer segmentation and identification patterns based on customers browsing history patterns in E-commerce. The artificial intelligent automatically generated the customer interest of specific products and services interests. The good news is that with the help of Artificial Intelligent (AI) the business is increasing in drastic and dramatic way in current Industries. It indicates that the Industries will tap in AI powered personalization tool in order to create personalized recommendation for each customers.

In E-commerce system security is more concern with respect to hardware, software, and environment are the essential and vulnerable focuses. E. W. T. Ngaia, and A. Gunasekaranb (2007) emphasized that hardware security includes any devices which are used in running the E-commerce websites like network devices, database server security in between clients and server network architecture. Securing the network with properly configured firewall device that is simply permitting ports needed for accessing for the E-commerce websites which are essential in every segments of the network. The web server and database server should be isolated from the other network segments using a network DMZ to reduce interruption during data transactions. In E-commerce network behind the firewall data is also secure transition in between different network including intranet, extranet, and over internet by Galanxhi-Janaqi et.al. (2004).

1.2 Need of Study

Gaffar Khan, Abdul (2019) emphasized that security challenges is one of the major concern in E- Commerce which are currently fulfill by the block chain technology to provide a secure transaction in E- Commerce and promising enough with security concern in Business Industries. E-Commerce platform on block chain technology is open BAZAR. It is P2P store where transactions are made through cryptocurRecny. It is free from merchant to setup a store without any programming knowledge.

In E-commerce, data system security for hardware and software is critical in order for shoppers to feel safe when they are doing online shopping or transactions. In recent trends hardware security is also more concern for business transactions like as network devices, web servers, database servers, and clients computers. The researcher emphasized that firewall devices, securing the networks which are allowing ports for accessing the E-commerce websites which is an essential part of network security for online transactions and significantly need in E- commerce.

2. Literature Review

Joze Kuzic et.al., (2002) have studied on E-commerce security challenges and success factors which are significant in business industries with reference to banking and finance sectors to provide secure transaction . Mohamed Halaweh (2017) stated that security is a consistent barrier for providing a secure network segments for customers and seller. Soliman, Youssef, M. (2003) emphasized that current dynamic and trends of business environment that for competing in worldwide markets to change the business standards for directing. E.W.T.Ngaia, and A.Gunasekaranb (2007) emphasized on M- commerce the offers potential opportunity for research and application for infrastructure and middleware fraud detection system in between client's machine and data base servers.

Asghar Afshar Jahanshahi et al. (2019) stated that power of wireless which are providing for secure services to customers in mobile commerce which has been entered in finance services, and internet security. Hawkins, S. et al. (2000) emphasized that internet security is a fundamental and secure data transmission and data storage, including encryption, firewall and private networks. Galanxhi-Janaqi et al. (2004) stated that E-commerce is one of the conventional and wireless .Ye Jun et.al. (2008) focused on E-commerce easy to access and secure networks resources, secure login identity and other web based services.

Murtaza, M et.al. (2004) emphasized that E-markets places and new trends in spite of failure in the E-business

new area with respect to B2B and B2C and other business Industries. Anthony Ferraro (1998) focused on simpler and more productive network that makes more secure data transmission during exchanging data between network segments...Alan D. Smith (2006) focused on E-commerce and emerging technology which are changing paradigm of data secure networks and data exchange. Gaffar Khan, Abdul (2019) emphasized that information technology playing a significant role for providing a secure network in business industries. Sachchidanand Singh and Nirmala Singh (2016) stated that The Internet of Things (IoT) given a more secure technology for developing smart devices for business opportunities and reshaping it. S. Schwiderski-Grosche and H. Knospe (2002) emphasized that Mobile commerce is noteworthy application area for secure business transaction in different network segments.

S.K. Miller (2001) emphasized that wireless technology is providing one of the secure and private network for exchanging data and information during data transmission with respect to challenging secure network and consuming low power processing power. Niranjanamurthy et al. (2013) emphasized that E-commerce is a widely used network for information security including data security and other framework of the network segments. Keng Siau et.al. (2001) stated that wireless technology is one of the advanced concept for smart development and new technological concept to implement for more secure data transmission. Md. Mahmud Hossain et.al. (2015) focused on the Internet of Things (IoT) is one of the advanced technology to manage the smart way of data transmission and security parameters the researcher presented the detailed security issues and challenges for secure data.

Mohanad Halaweh (2017) emphasized that security is one of the consistent barrier and implementation for E-commerce for customers for secure data transaction for network banking. Labuschagne, L. likewise, Eloff, J. (2000) focused on electronic commerce is one of the challenging technology in business industries over the network, in current scenario no one can trust on third part for keeping their data and information for exchanging . Kuzic Joze et.al. (2002) stated that E-commerce provides the benefits, security challenges and success factors in business industries.

3. Problem Statement and Research Objectives

Security is one of the major research topic fostering trust in E-commerce adoption. The most common security threats are phishing attacks, money thefts, data misuse, hacking, credit card frauds, and unprotected services. One of the main reasons for E-commerce threats is poor management. When the security practices is not up to the mark, it can pose a very dangerous threat to the networks and systems. Also, security threats occur when there are no proper budgets are allocated for the purchase and up keeping of security software licenses as well as services. The researcher pointed out some of the significant research issues on security and challenges on E-commerce in Business Industries.

- To study and analyze the recent technological trends of security factors on E-commerce industries.
- To study the factors of security challenges for trust-building in E-commerce.

4. Research Design and Methodology

In this researcher paper the researcher collected secondary data on recent trends on E-commerce and Security challenges in business Industries. The researcher identified some of the significant research issues on E-commerce with respect to security challenges in business Industries. The secondary data were collected from published books, journals, research papers, magazines, internet and official statistical documents. The study is qualitative in nature to show that a significant impact of security challenges on E- Commerce in business Industries. The researcher used statistical analysis tools SPSS software to analysis the data and produced the analysis report.

5. Recent Technological Trends and Security Challenges in E-Commerce

The researcher emphasized that security challenges in E-commerce is one of the significant research issues for providing a secure business transaction in finance Industries. Niranjanamurthy et al. (2013) emphasized that emphasized that block chain is one of the advanced technology which are using encryption for providing secure data transmission in business industries. Some of the research issues and security challenges which are posed by E-commerce in business industries on uncertainty with respect to security transaction and protection of online exchange that operates security and challenges issues by Keng Siau et.al. (2001) stated that:

- Denial of Service: which prevent authorized users from accessing a websites and reduced working of the websites.

- Unauthorized Access to Sensitive Information: Hackers can get intellectual property t and alter, destroy and steal data.
- Malicious: Alterations to Websites to alter website contents to negatively affect an organization.
- Damage to Computer Networks: stealing credit card information, address and personal data.
- Creation of Counterfeit Sites: Fake websites are creating a misleading statistics in business industries for stealing secure data and passwords.

The researcher emphasized that some of the significant research issues for creating major threats of security barriers for viruses, Trojan horses, and worms which are harmful software project design to damage the computers in some manners. Kuzic Joze et al. (2002) stated that viruses and worms are infected a computers, replicate, and spread data and disturbing the operational activities.

The researcher stated that some of the security parameters and awareness elements in business industries which are providing a secure network data transaction in E-commerce. Security is one of the biggest enablers to provide secure data without infected and damage the data. Labuschagne, L. likewise, Eloff, J. (2000) focused on the fraud detection system with respect to security and challenges in business industries for data storage and security parameters in business industries. In E-commerce security is one of the major concern for providing and secure and safe data during business transaction without human errors.

5.2 Data Analysis Report

Table 1. Source: Statista- E-commerce and Security Challenges' 2018

S. No	Security Factors	Share of Respondent
1	Regulatory Monitoring Online Vank Account Transaction	92.50%
2	Logout When Finished	90.30%
3	Avoiding Public or Shared Devices	86.30%
4	Avoiding Places Where one Could Potentially Watched	82.20%
5	Avoiding Providing Passwords via Email or Phone	76.60%
6	Verifying That a Secure Connection	77.30%
7	Always Typing the URL	66%
8	Using Pre-paid Cards	42.40%

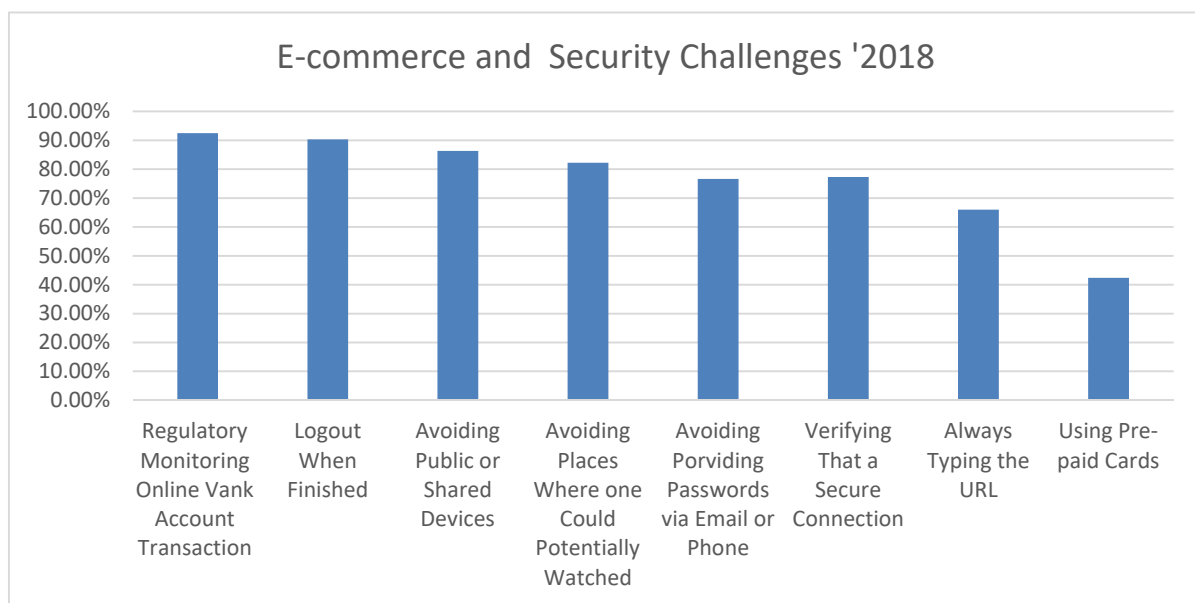


Figure 1. Security Challenges in E- Commerce'2018

The statistic presents the analysis report of E-commerce and online banking security measures employed by users during the year of 2018 which is collected from the statista. Kuzic Joze et.al. (2002) stated that during this period of time, most of the surveyed data stated that they monitor their online bank account regularly as a

security measure. In contrast, only 42.4 percent of the households used prepaid cards as a method to prevent online banking fraud.

5.3 Significance of the Research Study

Niranjanamurthy et al. (2013) emphasized that a recent analysis of the E-commerce space by Shopify identified several trends that will probably shape the fate of online deals. The absolute most critical E-commerce patterns forming its future include:

Online to Offline Growth: Notwithstanding unstable growth lately, E-commerce still speaks to just about 11.9 percent of retail deals, in spite of the fact that that is up from just 3.5 percent 10 years prior. Therefore, "online to offline" trade is a pattern to watch, as dealers endeavor to give "customers with an advanced encounter that can coordinate a particular in-store feel."

Multi-Channel E-commerce: Mobile customers are relied upon to represent \$319 billion in deals by 2020, and "multi-channel" deals, giving customers the capacity to effortlessly buy products through a variety of roads, will turn out to be always significant in the years ahead; going ahead, fruitful online traders should have a foundation that oversees and keeps up multi-channel retailing.

E-commerce Automation: As innovation keeps on developing, so too do the operational needs of online shippers. Notwithstanding satisfaction automation in the stockroom, guaranteeing that a business' site is completely in the know regarding the most recent innovation, requiring negligible human inclusion consistently, will be indispensable to proceeded with progress for E-commerce organizations. Guaranteeing that a business' site is completely fully informed regarding the most recent innovation, requiring negligible human contribution consistently, will be essential to proceeded with progress for E-commerce organizations.

Mobile E-commerce's Growing Popularity: As indicated by information from Adobe, in 2017 on both the day after Thanksgiving and The online Christmas sales extravaganza of that year, 30 percent of online deals shut through mobile gadgets. In spite of the fact that desktop is still unquestionably progressively prominent for making E-commerce buys, mobile is growing in popularity and should never again be viewed as only a strategy for enabling online customers to 'peruse'.

Opportunities in Global E-commerce: An examination by McKinsey proposes that E-commerce shippers might need to move their sights to the Asia Pacific area, when searching out universal deals openings. The investigation found that 1.4 billion individuals will join the worldwide 'working class' by 2020, with 85 percent of that growth in the Asia Pacific locale. Setting up neighborhood associations, acquainting oneself with provincial laws and customs, and guaranteeing solid, compelling showcasing will all be key components to consider as E-commerce organizations consider growing universally.

6. Conclusion

Finally, the researcher concluded data security is one of the significant factor of E-commerce in business Industries. The current technology allows for secure website design with all respect to handling secure threats when shopping online. The block chain is one of the latest security trends in business industries to provide the secure and transparent data during data transmission. The researcher also focused on the some of the significant security parameters which are growing rapidly to facilitate the proliferation of E-commerce. It is important to keep in mind that security measures do afford a good sense of protection. The researcher addressed the security audit and certain category of threats use tools to identify vulnerability that belongs to certain category of threats of E-commerce in business Industries. The primary responsibility of technology to provide the secure data transition in between different network segments. Customers must be aware of that the security issues which are still in infancy stage of the E-commerce security architecture in business Industries. The researcher emphasized that securing systems and networks available for the E-commerce systems personnel to read and implement. Educating the consumer on security issues is still in the infancy stage but will prove to be the most critical element of the E-commerce security architecture in Business Industries.

References

- Alan, D. S. (2006). Exploring m-business regarding practicality, growth and difficulties. *Worldwide Diary of Mobile Interchanges Chronicle*, 4(6), 682-703.
- Anthony, F. (1998). Electronic Business: The Issues and Difficulties to Making Trust and a Positive Picture in Purchaser Deals on the Internet. An Incredible Urban communities Activity of the College of Illinois at Chicago College Library. <https://doi.org/10.5210/fm.v3i6.601>
- Asghar, A., Jahanshahi, A. M., & Amin, A. (2019). Mobile Trade Past Electronic Business: Issue And Difficulties.

- Asian Diary of Business and The executives Sciences*, 1(2), 119-129.
- Gaffar, K. A. (2019). Electronic Business: An Examination on Advantages and Difficulties in a Rising Economy. *Worldwide Diary of The board and Business Exploration*, 16(1).
- Galanxhi-Janaqi, H., & Fui-Hoon Nah, F. (2004). U-commerce: developing patterns and research issues. *Modern Administration and Information Frameworks*, 104(9), 744-755. <https://doi.org/10.1108/02635570410567739>
- Hawkins, S., Yen, D., & Chou, D. (2000). Mindfulness and difficulties of Web security. *Data The board and PC Security*, 8(3), 131-143. <https://doi.org/10.1108/09685220010372564>
- Joze, K., Julie, F., & Angela, S. (2002). Electronic Trade Advantages, Difficulties and Achievement Factors in The Australian. Banking and Money Industry, ECIS 2002 Procedures European Meeting on Data Systems(ECIS)ECIS 2002 • June 6–8, Gdańsk, Poland.
- Keng, S., Ee-Peng, L., & Zixing, S. (2001). Mobile Trade: Guarantees, Difficulties and Exploration Motivation. *Diary of Database the executives (JDM)*, 12(3), 10. <https://doi.org/10.4018/jdm.2001070101>
- Kuzic, J., Fisher, J., & Scollary, A. (2002). Electronic Trade Advantages, Difficulties and Achievement Factors in the Australian Banking and Fund Industry. Retrieved from <http://aisel.aisnet.org/ecis2002/60>
- Labuschagne, L., & Eloff, J. (2000). Electronic trade: the information-security challenge. *Data The board and PC Security*, 8(3), 154-157. <https://doi.org/10.1108/09685220010372582>
- Md. M. H., Maier, F., & Ragib, H. (2015). Towards an Investigation of Security Issues, Difficulties, and Open Issues in the Web of Things, Distributed in: 2015 IEEE World Congress on Administrations. <https://doi.org/10.1109/SERVICES.2015.12>
- Mill, S. K. (2001). Facing the test of remote security, Distributed in: PC. <https://doi.org/10.1109/2.933495>
- Mohamed, H. (2017). Adoption of E-commerce in Jordan: Understanding the Security Challenge. <https://doi.org/10.1002/j.1681-4835.2011.tb00331.x>
- Mohanad, H. (2017). Adoption of E-commerce in Jordan: Understanding the Security Challenge. <https://doi.org/10.1002/j.1681-4835.2011.tb00331.x>
- Murtaza, M., Gupta, V., & Carroll, R. (2004). E-marketplaces and the eventual fate of store network the board: openings and difficulties. *Business Procedure The board Diary*, 10(3), 325-335. <https://doi.org/10.1108/14637150410539722>.
- Ngaia, E. W. T., & Gunasekaranb, A. (2007). An audit for mobile business research and applications. *Choice Emotionally supportive networks*, 43(1), 3-15. <https://doi.org/10.1016/j.dss.2005.05.003>
- Niranjanamurthy, K. N., Jagannath, S., & Dharmendra, C. (2013). Analysis of Web based business and M-Trade: Preferences. *Constraints and Security Issues*, 2(6), 2319-5940.
- Sachchidanand, S., & Nirmala, S. (2016). Internet of Things (IoT): Security challenges, business openings and reference design for Web based business, 2015 Universal Meeting on Green Registering and Web of Things (ICGCIoT). <https://doi.org/10.1109/ICGCIoT.2015.7380718>
- Schwiderski-Grosche, S., & Knospe, H. (2002). Secure mobile business. *Hardware and Correspondence Designing Diary*, 14(5). <https://doi.org/10.1049/ecej:20020506>
- Soliman, F., & Youssef, M. (2003)? Internet-based E-commerce and its effect on assembling and business tasks. *Modern Administration and Information Frameworks*, 103(8), 546-552. <https://doi.org/10.1108/02635570310497594>.
- Ye, J., Li, Z. S., & Mama, Y. Y. (2008). JSON Based Decentralized SSO Security Engineering in Online business, 2008 Global Symposium on Electronic Trade and Security. <https://doi.org/10.1109/ISECS.2008.171>

Copyrights

Copyright for this article is retained by the author(s), with first publication rights granted to the journal.

This is an open-access article distributed under the terms and conditions of the Creative Commons Attribution license (<http://creativecommons.org/licenses/by/4.0/>).