The Threats and Dimensions of Security Systems in Electronic Commerce

[1]Waheeb Abu-ulbeh, [2]Yazeed Al Moaiad, [3]Abdilahi Liban, [4]Mazen Mohammed Farea, [5]Wafa Abdulkarem Al-Haithami, *[6]Yousef A.Baker El-Ebiary

[1]Asst. Prof. Dr., Cybersecurity Department, Al-Istiqlal University, Jericho, 10, Palestine
w.abuulbeh@pass.ps
[2]Asst. Prof. Dr., Faculty of Computer and Information Technology, MEDIU, Malaysia
yazeed.alsayed@mediu.edu.my
[3]Dr., Faculty of Computer and Information Technology, MEDIU, Malaysia,
abdilahi.liban@hotmail.com
[4]Assoc. Prof. Dr., Faculty of Finance & Administrative Sciences, Al-Madinah International University, Malaysia
mazen.farea@mediu.edu.my
[5]Faculty of Finance and Administrative Sciences, Al-Madinah International University, Malaysia
fafikareem2017@gmail.com
[6]Assoc. Prof. Ts. Dr., Faculty of Informatics and Computing, UniSZA University, Malaysia,
*(Corresponding Author) yousefelebiary@unisza.edu.my
https://orcid.org/0000-0002-4392-8015

Abstract

E-commerce is a buying and selling platform via the internet, and the transaction of money also must be made online. This platform needs to have good security to ensure the trust of customers. Trust from consumers is needed to continue this business, because of that security system must be constantly improved and upgraded to a better version. The security system of e-commerce must be tightly secure to ensure all consumers' privacy and personal information do not get leaked by hackers. E-commerce offers a great opportunity to the online banking and online shopping industry, but also has a high risk of security threats. This article shows the difficulties of asset and transaction security in e-commerce components and operations. Because substantial sums of public money are involved in the transactions, the importance of data security and privacy is not overstated in this industry. The article goes on to highlight the security requirements of e-commerce systems from potential threats and weaknesses after looking at the technologies utilized in e-commerce. The challenge of e-commerce security is then considered as one of engineering management, and a lifecycle solution is proposed. This report will discuss the threats in E-commerce and all dimensions of e-commerce. Besides that, this report will explain the advantages and disadvantages of e-commerce, and also the solution on how to counter the threats to the security system of E-commerce. A lot of issues discussed here are important for online shopping or e-commerce platform users because they will educate them to be more careful when making an online transaction. This report also persuades customers to be more confident in the e-commerce security systems.

Keywords—E-commerce, security system, threats, dimensions

I.Introduction

In the late 1970s, the capacity to employ E-Commerce technology became available. E-Commerce at the time meant the electronic execution of business transactions using Electronic Data Interchange (EDI) and Electronic Funds Transfer (EFT) (EFT). The Internet was first made available for commercial use in 1991, and it gained popularity in 1994. (E-Commerce Land, 2004). As a result, security protocols such as HTTPS took nearly four years to create. One of the earliest E-Commerce companies to build a safe market was Amazon.

Information privacy and security, according to Miyazaki and Fernandez (2001), will be the biggest obstacles in the growth of consumer-related e-commerce.

There are five major types of e-commerce which are business to consumer(B2C), business to business(B2B), consumer to consumer(C2C), business to government(B2G), and mobile commerce(m-commerce). The retail or sale side of e-commerce is where Business to Consumer focuses. It is the exchange of products and services between businesses and consumers, and it entails customers obtaining information, purchasing physical commodities such as clothes or furniture, or information goods such as downloading digital material content such as software, online games, or electronic books. In the business-to-consumer (B2C) market, one example is Shopee which is more relatable to an online shopping mall due to its largest range in Malaysia.[5]

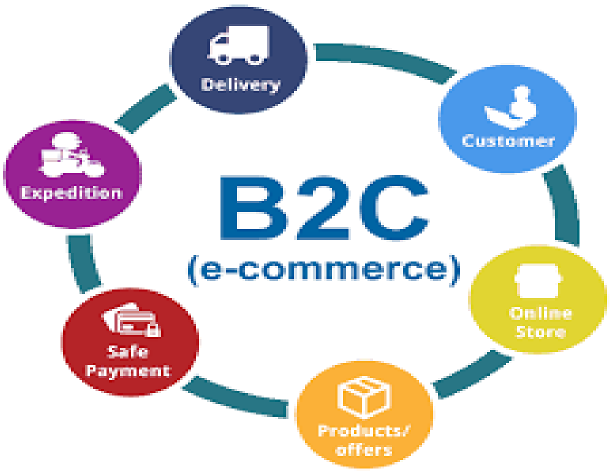

Fig. 1. Example of Business to Consumer e-commerce

When e-commerce is expanded to include supply chain management between and among firms, a new concept known as business-to-business forms (B2B). Companies can handle various supply chain elements such as manufacturers, distributors, and dealers. E-commerce between two or more businesses is known as business to business e-commerce. In business to business e-commerce, the main focus is on procurement, but in business to consumers, the main focus is on selling and marketing.

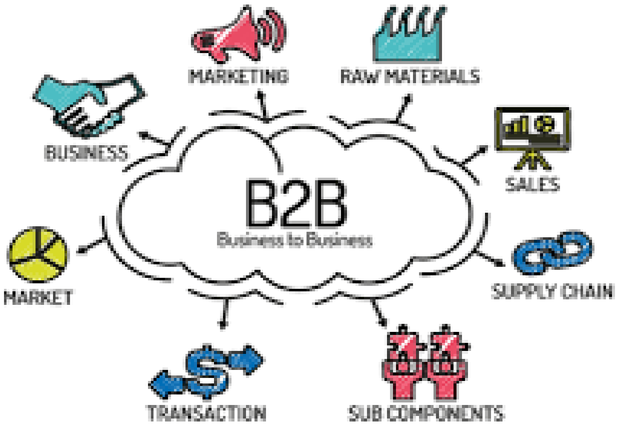

Fig. 2. Example of Business to Business ecommerce

Consumer to consumer e-commerce happened between private individuals and consumers. There are a lot of example of consumer to consumer e-commerce such as portals like Chilindo which allows online real time bidding on products for sale on the internet. Next, Peer-to-peer (P2P) systems which allows private individuals to share files containing many types of data. It is unlawful in Finland to transfer any copyrighted information using peer-to-peer networks.The last example is individuals can sell or purchase garbage or commodities on different advertising platforms such as Corousell. On internet, there are also forums where users may post classified ads for buying or selling employees relating to the forum's topic.

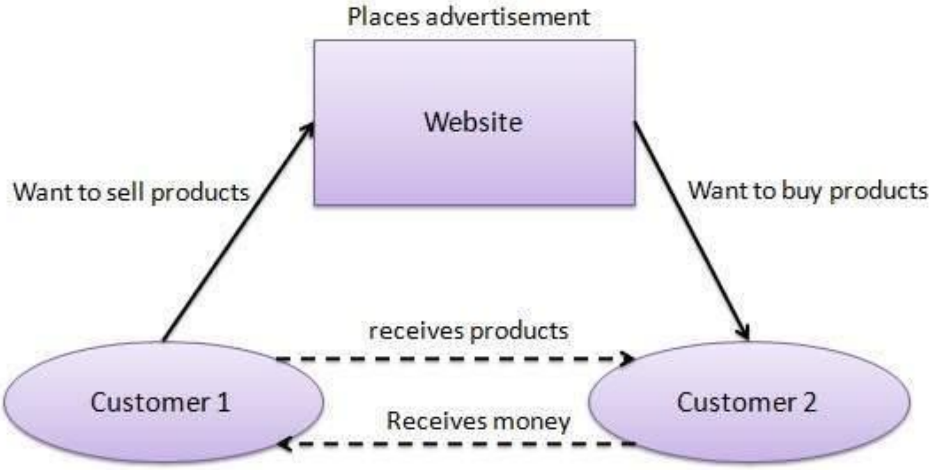

Fig. 3. Example of consumer to consumer cycle

Business-to-government e-commerce refers to e-commerce between businesses and the government. For example, this involves using the internet for licensing,public procurement, and other government-related tasks. In business to government e-commerce, the government plays a key role in creating e-commerce.

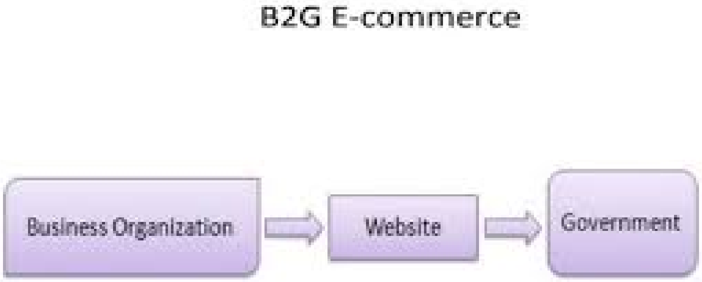

Fig. 4. Example of business to government cycle

The practise of buying and selling products or services through wireless technology is known as mobile e-commerce. The most significant advantage of m-commerce is that the terminal is portable, and large cities have radio coverage. In addition, the number of services offered in m-commerce is growing.[5] For example, data and information services such as automatic reminders or notification of news, bill or stocks market.[6]

Fig. 5. Example of mobile e-commerce

E-commerce security is a protection to customers of e-commerce from any hackers, unauthorized access to personal information and scammers. E-commerce is a platform that includes all business activities such as investment, shopping and online transactions.[7] E-commerce also is a part of the Information Security framework that applied to elements that affected e-commerce security such as Computer Security, Data Security and other components of the Information Security framework. (The Study of E-Commerce Security Issues and Solutions) This platform needs to have a tight security to ensure the trust given by customers. This is because e-commerce involves with a lot of customers' money and also their personal information. This will attract the bad people to gain money by scamming and hacking customer's money and bank information.[8]

Online shopping platforms such as Shopee, Lazada and Amazon has the terms and conditions that customers must follow to protect their personal information and privacy. This is also to make sure customers can buy a product with safe and secure transactions. Online shopping users also need to educate themselves to not give any bank information to any people on online websites.[9]

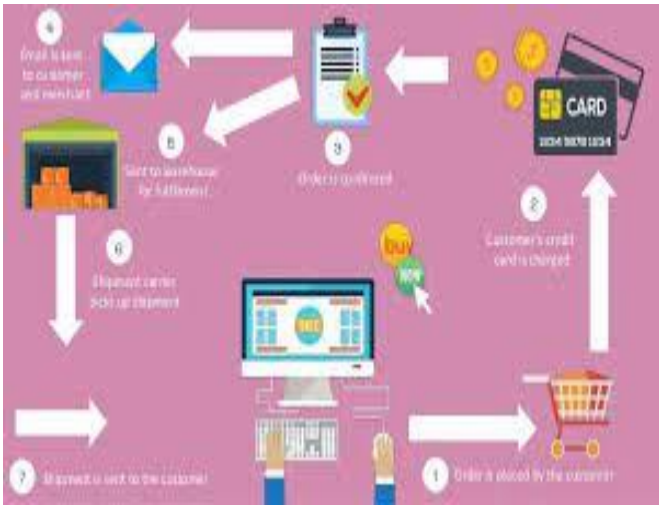
4
Email is sent to customer and merchant
CARD
3
Order is confirmed
5
Sent to warehouse for fulfilment
2
Customer's credit card is charged
6
Shipment carrier picks up shipment
buy
now
7
Shipment is sent to the customer
1
Order is placed by the customer

Fig. 6. Example of E-commerce process cycle

There is a way how e-commerce ensures the security of their customers' information. For example, Shopee did not allow their customers to do a transaction outside the applications to avoid any money scamming.[10] Privacy has become a major concern, not just to customers but also to the e-commerce provider, because of that people need to give more attention to e-commerce security. In the minds of consumers, security risks appear as the most pressing worry. Besides, e-commerce faces other dangers, including server threats, communication channel threats, client threats, virus threats, and intellectual belonging threats. In order to overcome these attacks, security is very crucial for anyone.[11]

Fig. 7. Example of e-commerce platform

II.Related Works

Security is not just about the safety of ourselves but security also should be provided in our today's lifestyle such as security on the internet that we use nowadays to do something online. In addition, many of our jobs today required the use of the internet to solve problems like making an appointment with a doctor or some company should have an online appointment.[12]

Security is an important part of any transactions that use the internet. People will lose their faith in e-commerce platforms when there is too much scam on the internet and do not have any securities on the internet page.[13]

Nowadays, a lot of things are done on the internet such as buying and selling goods using online websites or online applications like Shopee and Lazada. These applications consist of their own safety that safeguards people who take care and observe their clients online when they do their selling or buying using those applications. These applications have gained people's trust and it is because of the security internet on the website works well [14].

E-commerce security is to provide protection of e-commerce assets from being hacked or used by unauthorized persons. E-commerce security is one of the most important in nowadays life because it has dimensions of e-commerce such as integrity, non-repudiation, authenticity, confidentiality, privacy, and availability.[15] E-commerce also has its own threats like intellectual property threats, client computer threats, communication channel threats, and server threats. Also, e-commerce has its advantages and disadvantages.

In my opinion, e-commerce security should be upgraded on websites to avoid something bad like scammers and illegal servers. E-commerce has their trust in people because it helps people to provide online websites and online transactions such as keeping the personal information on the website.[16] Without trust, many people would forget about the use of the internet and maybe revert back to using the traditional methods. In my opinion, we should know more about e-commerce so that we can provide our internet website or information from being scammed or hacked.[17]

III.Purpose Of Study

- To learn the important of e-commerce.
- Discuss a deeper understanding of customers perceived privacy and security.
- Study of maintaining a high perception of security.
- Explore the security concerns of online IT users.
- Explore the perception of security in e-commerce from both customer and organizational perspectives.
- Analyze the improvement of environment for the advancement of e-commerce.
- Understanding of customer needs and priorities on the subject security.
- To discuss the overview of E-commerce security system.
- To know how to place an order for online shopping.
- To know the purpose of security system in E-commerce.
- To discuss the disparate security issues in E-commerce.
- To gain knowledge on how to secure online shopping guidelines.
- Discuss how to increase operational efficiency by using different security measures.

IV.Threats In E-Commerce

Based on figure 8. above, we can see how the hackers are doing their job to make the businesses lose and take the payment of a customer. It starts when the attacker injects a malicious script to an e-commerce platform to get into the web server. After that, they attack the front-end online store by loading the malicious script to confuse them in order to access the web server. Meanwhile, the users who do not know anything about the malicious script just use it and this way would affect the businesses of the store because the hacker may have their details information. However, it not only makes the store lose profit but also the customer can be hacked because the malicious script that the users use may make the payment information of users be sent to the attacker's server. At last, the attacker got all the payment info and causes huge losses to either the businesses or the customers money. Thus, businesses should have more knowledge about security systems in e-commerce so that they can adapt the malicious script that will affect their business.

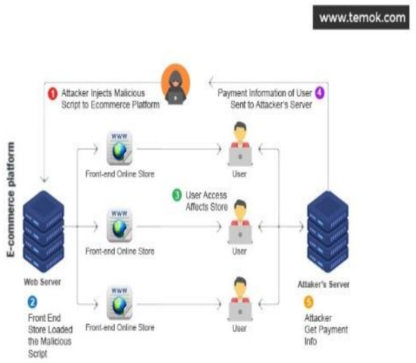
www.temok.com
1 Attacker Injects Malicious Script to Ecommerce Platform
Payment Information of User Sent to Attacker's Server 4
E-commerce platform
Front-end Online Store
User
3 User Access Affects Store
Front-end Online Store
User
Web Server
2 Front End Store Loaded the Malicious Script
Front-end Online Store
User
Attaker's Server
5 Attacker Get Payment Info

Fig. 8. The flow chart of security threats in e-commerce

Security threats can be referred to as a risk in security e-commerce which can harm computer data and organization. This is because someone can steal our data from the computer that is called a hacker. The hacker can gain unauthorized access to a computer system. E-commerce threat also can be defined as using the internet for something unfair because of the intention of stealing and fraud. Also, there are various types of threats such as accidental, some are purposeful and some are due to human error. But the most common threats are electronic payments that use e-cash or credit and debit card frauds.[18]

Threats can be classified into two categories that are physical threats and non-physical threats. As for physical threats, it may cause an incident that will risk loss or physical damage to our computer systems.

Physical threats can be classified into three main categories which are internal, external, and human. Internal physical threats are like fire or unstable power supply.

For external physical is more like lightning, floods, and earthquakes. The last one is a physical threat of humans like theft, vandalism of the infrastructure, or intentional errors.

The non-physical threat is known as a logical threat. This threat may cause many incidents such as corruption of the system data, business operations that use the computer may disrupt, loss of sensitive information, and cyber security breaches. The common types of non-physical threats are likes spyware, keyloggers, and unauthorized access to the computer system resources.[19]

Other than that, the threats that involve credit and debit card fraud are called financial fraud. Most cases involve financial fraud because of online selling and buying. As a credit card, it happens when cybercriminals steal the credit card data and used it to buy products. Usually, this case can be detected because the shipping and billing addresses vary.

Also, there is a case of fake return and refund fraud. This is because the hacker can make unauthorized transactions that can make the businesses loss[20]. Some of them also do cybercrimes about refund fraud like they file a fake case that requests a refund. Most of the victims came from old people because they easily believe something without investigating it first.[21]

Other than that, there is also a threat called phishing which happens when the hacker in disguise as a police or other agency that sent a message, email and even used a call to lie about something like you get sued or some fraudulent retrieval of goods in certain places.[22] For example, the authentic email from the bank asking to provide our details and such a thing.[23]

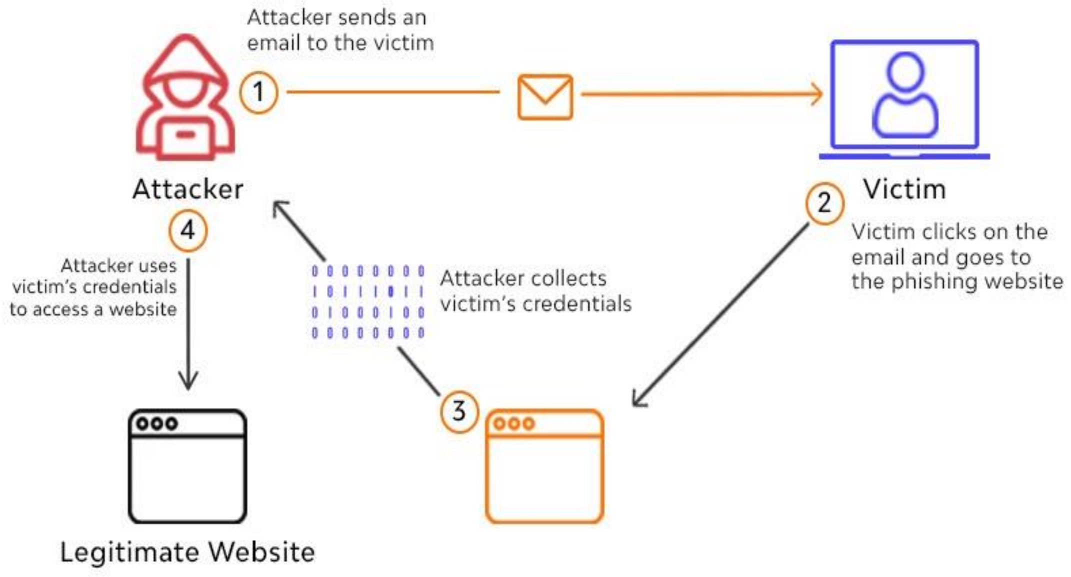
Attacker sends an email to the victim
1
Attacker
Victim
2
Victim clicks on the email and goes to the phishing website
4
Attacker uses victim's credentials to access a website
Attacker collects victim's credentials
3
Legitimate Website

Fig. 9. Example of phishing attacks

This phishing attack happens to the customer who does not realize the via email that is sent to them is not illegal and it is how the attackers use email for the victim clicks and give all the details in that email. This way could make the attacker collect the victim's credentials. The attacker uses the details that the victim gives to access a legitimate website.

Besides, there are also cases of spamming. This happens when the hacker will send a link via email or social media inboxes. Not just that, they also put the link in comment forms and once someone clicks the link, all of the data will directly arrive at them. Then, someone may end up being a victim of spamming. So, that is why we should put an e-commerce security system in order to have safe privacy online.[24]

A threat called a man in the middle also happens when the attacker uses the wi-fi or network to listen to the communication. Some businesses have experienced this case. This is because of the man in the middle that contains the details and uses them for other harm like scamming. These threats can make some of the businesses incur a loss. So, in order to ensure safety, the business should have security like a password in order to use the wi-fi. This may help even a little from being scammed by hackers. It is better if we just use the direct way from using other people to get the information like the figure shows how the man in the middle works to get the information of businesses. [25]

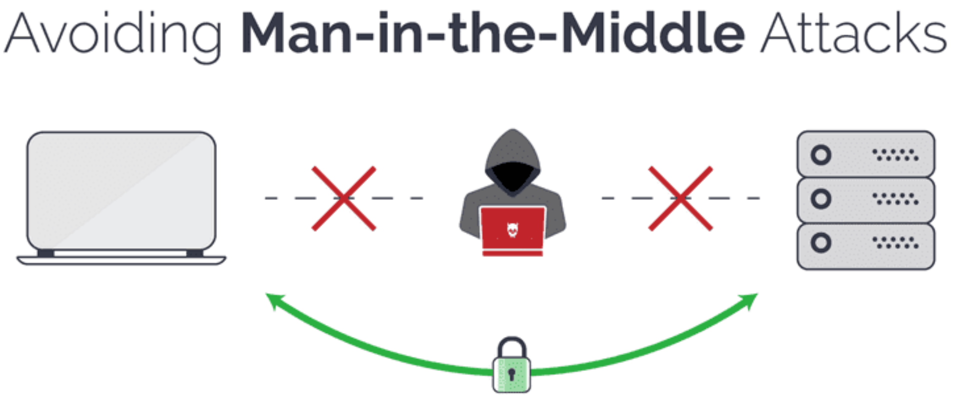

Fig. 10. Example of Man in the Middle

There are more threats but the case above keeps receiving reports of people being scammed. In conclusion, the security system of e-commerce is very important for online users so that it will lessen the danger of a hacker scamming people. Also, all of us from all ages should have more knowledge about security systems and e-commerce and should be aware of something that happened suddenly. We should investigate it first or ask others that have more knowledge about it.[14]

V. Dimensions Of E-Commerce Security

Nowadays, cyber-attacks are often prevalent on the internet and most businesses are facing significant losses. So, the websites that are used by users need to be protected and have high security. There are six dimensions of e-commerce security which are integrity, non-repudiation, authenticity, confidentiality, privacy, and availability.[13]

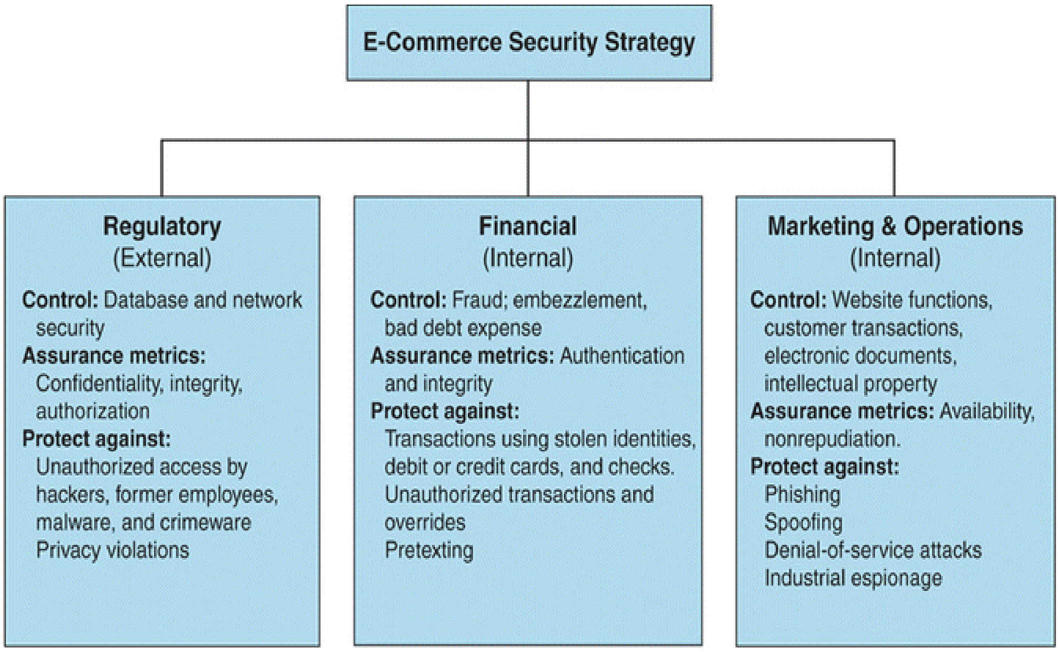
E-Commerce Security Strategy
Regulatory
(External)
Control: Database and network security
Assurance metrics:
Confidentiality, integrity, authorization
Protect against:
Unauthorized access by hackers, former employees, malware, and crimeware
Privacy violations
Financial
(Internal)
Control: Fraud; embezzlement, bad debt expense
Assurance metrics: Authentication and integrity
Protect against:
Transactions using stolen identities, debit or credit cards, and checks.
Unauthorized transactions and overrides
Pretexting
Marketing & Operations
(Internal)
Control: Website functions, customer transactions, electronic documents, intellectual property
Assurance metrics: Availability, nonrepudiation.
Protect against:
Phishing
Spoofing
Denial-of-service attacks
Industrial espionage

Fig. 11. E-commerce security strategy

The first dimension is integrity. Integrity includes the accuracy of data, trustworthiness, and keeping consistency over its whole lifecycle. It means that integrity can make sure all of the crucial information and data on the internet are safe and have not been stolen by any unauthorized or unknown parties. So, the issues that are raised by the customers and merchants whether they presented the data and information that were published on the website has been altered, or not or the information that is sent from customers are valid or not can be solved with integrity.[26]

Second is non-repudiation. Non-repudiation can be defined as the assurance that the sender of information is given with the proof of delivery and the recipient is offered with proof of the sender's identity, so neither can later deny having prepared or processed the information. Once the customers or sellers agreed that there would not be any repudiation, they should not deny facts, rules, or regulations.[27] Furthermore, non-repudiation verifies that all of the information and data transferred between two parties which are customers and sellers has been successfully received or not.

Next is authenticity. It means the assurance that any transactions, messages, and other reciprocity of information are from authorized sources. The authenticity also includes the evidence of identity and can affirm the authenticity through authentication. In e-commerce, the customers and sellers need to give or provide accurate and correct proof of their native identities in order to have a secure transaction between them in the platform. In addition, e-commerce platforms used authenticity as a tool to make sure people are not faking their identities. As an illustration, people can use their fake phone numbers and email address to access any e-commerce platform.

Confidentiality is also one of the dimensions of e-commerce security. This dimension makes sure the private information and data are secured from any unauthorized parties. So, the private information and data are only available or can be accessed by authorized people and they can use any sensitive or restricted data or modify them. As we can see, when people cannot log in to their e-commerce website account, they will reset their password and change with the new password. In order to change their new password, e-commerce websites will send the one-time password to their email or phone number to avoid any disruption from third parties.

The fifth dimension of e-commerce security is privacy. Privacy can be defined as possessing the capability to secure the restrictive or sensitive information of personally recognizable data. In short, privacy is the protection of the usage of information or data between the customers and sellers. Moreover, privacy is a vital threat to any online transaction as private data is revealed and there is no method to disclose them. For example, if third parties or hackers breach the e-commerce websites, they can access any information on credit card details of customers.

Lastly, availability. It means the affirmation that a computer system is available or can be accessed by an authorized user whenever it is needed. This dimension strengthens site traffic, search engine rankings, and online visibility. The data and information in the websites should always be secured and available to the customers and sellers.

VI. Advantages Of Security System In E-Commerce

In an e-commerce system security, software, environment, and hardware are the main critical issues which are crucial in the system[21]. There are many advantages of the security system in e-commerce. First, the security system in e-commerce is crucial in order to protect the customer’s data and privacy on a website. In this age of technological advancement, people make sales and purchases online to facilitate their daily affairs without having to go out to a physical store. Therefore, e-commerce platforms are very important as it assists them to purchase the trusted online products. So, when there are a lot of transactions done on this platform, the security system plays an even more important role to secure the customer’s data and privacy such as personal details, address, bank account, and more.[28]

Furthermore, the security system can prevent any payment scams and financial fraud which is likely to occur to customers when they make an online purchase transaction. Financial fraud has been prevalent on various websites especially online purchase websites. As an illustration of payment scams and financial fraud, hackers have quietly made unauthorized transactions and the trail has been wiped out and indirectly the customers and sellers have to bear big losses. Some scammers also file requests for fake refunds or returns. Thus, with the existence of this security system, it helps to detect the dubious transactions made by scammers or hackers and allows the customers to make payments securely and safely.[29]

The next advantage is gaining the trust of customers. The security system manages to earn the trust of customers when frequent scams are reduced. Moreover, when the customers are buying products from the sellers on e-commerce such as Shopee, Lazada, and Zalora, they will feel safe and confident that their privacy and data of transaction will be fully protected by the security system. In addition, the customers will not be willing to recommend other people to buy online products on e-commerce if there is no data protection even if it is a loyal customer.

VII. Disadvantages Of Security System In E-Commerce

However, there are also many disadvantages of the security system in e-commerce. First, there is a chance of vulnerability to viruses and malware. It will appear when the sellers inconsistently upgrade the store's software from the updates issued by the software providers. Furthermore, if the customers are using old or outdated HTTP protocols, they will face cyber-attack and fraud.

In addition, the security system may require a huge technological cost. The software, network, and any arising security issues need to be renewed and improved from time to time as it will affect the e-commerce website to be able to run smoothly. So, the e-commerce website will invest more costs on the security system and that is one of the disadvantages of having a security system.

VIII. Discussion

We choose e-commerce as e-commerce is the system that most people use for their business even a small business can use it to increase their sales. They can find a buyer in this system and do not have to waste their energy and time because they only need an internet connection to access e-commerce. For us, we think e-commerce is an easy platform as we can search any product and service online with just using an internet connection.[30]

Some applications or websites will have a problem with security privacy issues which are becoming more prevalent in our country. This is the same as the e-commerce system. E-commerce systems also have a security and privacy issue that is very serious and hackers usually targeted e-commerce platforms using a myriad of malicious techniques.[31] An e-commerce security threat that occurs is financial fraud. In online business, financial fraud always happens such as credit card fraud and fake return and refund fraud. Credit card fraud happens when a cybercriminal uses stolen credit card data to buy a product from your store and sometimes it can happen when they steal your information details for them to get a new credit card. And for the fake return and refund fraud, it happens when the hackers make a fake file to request returns.[32]

Second, the security threat that happen in E-Commerce is phishing. This happened because a fraudster makes copies of your website to trick the users to believe them. The fraudster used this trick to get money from the customers. Then, another threat is spamming. This is a bad trick where they send you a link via email or social media inbox and if you click it, you may be a victim of them.

Among the security and privacy issues that happen in e-commerce is the security threat. Security threats are risk that can potentially harm computer systems and organizations. The security threats that happen in e-commerce are fraudulent use of credit cards, computer viruses, spam messages on email, theft on computers or information, and others.

The security and privacy issues with e-commerce can be minimized with a few solutions. First, you should make a review on features or services offered by your web hosting service, internet service provider, web design, and software company. It is very crucial for you to double-check before you download something from any website as if not, your privacy will be exposed to the hacker or someone that will manipulate your information. You should pay serious attention to security alerts about any websites or links that should not be pressed and you must install security patches as needed.[33]

Besides that, you should regularly update the software in your computer and scan the spyware and viruses. This is very important to reduce vulnerabilities and make sure that your database is not exposed to security threats. If you do not update your software, it is the same that you give a chance for your computer to be infected. Besides that, it is important to update the software to fix bugs and crashes on your computer. Crashes and bugs always happen when someone or the company wants to update the version of a program. If you do not update the software, you cannot avoid the problems that will be affecting your computer. So, to make your computer better, you should update the software to ensure that you are running the most current and bug-free version.[34]

Other than that, you should back up the system and information regularly. This is very crucial to make sure that information from your computer is not missing or exposed to the threats that will use your information in the wrong way. Do not let your information to be exposed to hackers because of your negligence.[35]

Furthermore, before you want to do online shopping, it has a few guidelines for you to follow. First of all, as a buyer of online shopping, you should shop at a guaranteed safe website that uses encryption technology to transfer your information to the online merchant's computer. You could know whether the site is secure or not on the website address, if the website has 's' after the HTTP, that means the website is secure. Another way to know if the website is secured or not, you can see the padlock on the address bar at the upper of the screen. If it is open, that means it is not a secured website. So, before you want to open a website, remember to read a merchant's privacy and security policies to learn how it saves your information on its computer.

Second, the guidelines for you to follow is to do research about the website before you make an order. This is important for you to know whether the website is owned by the company that you are already or not. If you are not familiar with the company, you should not buy anything from the websites. You can call the number on the websites or you can check through the Better Business Bureau.

Thirdly, you should never give your social security number because the merchant will not need it. If a website asks for your social security number, do not give it to them. It is the same that you give your private data to them. Next, you must keep your password private. Usually, when you make an order, you need a username and a password. You should not make a password that is related to common information such as your birthdate, or another date that is related to your family. You also should not use the same password for another website because some of that is associated with sensitive information.

Lastly, you must be aware of the identity of the theft or hackers. Nowadays, there are many fraudulent cases which is identity forgery that is always occurred over the internet. They used the low tech such as dumpster diving, mail theft, or workplace access to SSNs. They use the credit cards of the victims to buy a service or goods from the websites. If you want to shop online you should be careful with this theft and must ensure that you use a credit card instead of a debit card. And then, you must check your credit card for several months after you do online shopping. If there is something wrong with your credit cards, you can contact the credit card company and file a dispute claim. You should check the reports of your credit card at least once a year to see if your credit cards were used without your permission.

IX. Conclusion

In conclusion, in this sophisticated age, people must be careful in using technologies such as gadgets especially in this Covid-19 pandemic season as during this time, our work, expenses, and payment are mostly online. E-commerce has become one of the important platforms for people to use. Because of that, users need to be careful before using e-commerce as this platform normally needs to use our private data such as bank account number, identification certificate number, phone number, and others.

Besides that, e-commerce also has many threats for users. For example, financial frauds, phishing, spamming, man in the middle which is a hacker, and others. To prevent these issues, an e-commerce security system has been established to make sure that users' privacy data is strictly controlled. Users need to know about the dimensions of e-commerce security to prevent leakage of personal information. The list of dimensions of e-commerce security is integrity, non-repudiation, authenticity, confidentiality, privacy, and availability. [36]

The security system in e-commerce also has advantages and disadvantages. Advantages obviously bring benefits to users but disadvantages will bring consequences to users. To prevent this from happening, users need to make sure that any gadgets used, free from viruses and always update the software, if not, our gadgets will have the chance to get infected. Last but not least, the existing or new users must take note of all these issues to prevent them from becoming the next victim.

Day by day, this e-commerce platform plays an important role in our society. This concludes with a great advertisement about the product in e-commerce that can attract interest with different ages which are children, teenagers, adults, and elders. But they must be careful before buying a product as nowadays, there are many scammers that will take the opportunity to cheat on the community, especially students and the elderly. Simple steps that we can use before buying a product online are to check the product ratings and reviews, read the product's specifications, understand the return and refund policy, and others.

Apart from customers who need to be careful, the sellers that are involved in e-commerce platforms also need to play an appropriate role such as being honest on the product that you want to sell and choosing a trusted courier.

Other than that, the sellers must also keep the customer's personal information from other parties such as name, address, and phone number. Sellers must provide the best security e-commerce system to gain customers' trust. Nowadays, transaction authorization code (TAC) and I-access code (IAC) is very important thing that we must request before making an online payment but we cannot share that code with others. Last but not least, everyone has their own responsibility before using an e-commerce platform to prevent losses.

References

[1] R. C. Marchany and J. G. Tront, "E-Commerce Security Issues," 2002, Accessed: Nov. 22, 2021. [Online]. Available: www.cultdeadcow.com,.

[2] F. Kamoun and M. Halaweh, "A fuzzy classification approach to assess e-commerce security perception," Int. J. Bus. Inf. Syst., vol. 9, no. 1, pp. 108–126, Dec. 2012, doi: 10.1504/IJBIS.2012.044457.

[3] Y. Zhang, X. Deng, D. Wei, and Y. Deng, "Assessment of E-Commerce security using AHP and evidential reasoning," Expert Syst. Appl., vol. 39, no. 3, pp. 3611–3623, Feb. 2012, doi: 10.1016/J.ESWA.2011.09.051.

[4] A. Sengupta, C. Mazumdar, and M. S. Barik, "e-Commerce security — A life cycle approach," Sadhana 2005 302, vol. 30, no. 2, pp. 119–140, 2005, doi: 10.1007/BF02706241.

[5] A.Koponen, "E-Commerce, Electronic Payments," Proc. Res. Semin. Telecommun. Bus., 2006, [Online]. Available: http://www.tml.hut.fi/Opinnot/T-109.7510/2006/Proceedings_2006.pdf.

[6] "Proceedings of the International Multiconference on," 2008.

[7] M. Warren and W. Hutchinson, "A security risk management approach for e-commerce," Inf. Manag. Comput. Secur., vol. 11, no. 5, pp. 238–242, 2003, doi: 10.1108/09685220310509028/FULL/XML.

[8] T. A. Kraft and R. Kakar, "E-Commerce Security," 2009, Accessed: Nov. 22, 2021. [Online]. Available: https://www.researchgate.net/publication/281976555.

[9] H. Kim, Y. Han, and S. Kim, "A Curriculum Design for E-commerce Security - ProQuest." https://www.proquest.com/openview/129dfe6fa02127e630a42dca2ea17393/1?pq-origsite=gscholar&cbl=25848 (accessed Nov. 22, 2021).

[10] P. Prisha, H. F. Neo, T. S. Ong, and C. C. Teo, "E-Commerce security and identity integrity: The future of virtual shopping," Adv. Sci. Lett., vol. 23, no. 8, pp. 7849–7852, Aug. 2017, doi: 10.1166/ASL.2017.9592.

[11] S. Muthaiyah, J. A. J. Ernest, and C. K. Wai, "Review Of E-Commerce Issues: Consumers Perception On Security And Privacy," Int. Bus. Econ. Res. J., vol. 3, no. 9, Feb. 2011, doi: 10.19030/IBER.V3I9.3724.

[12] M. S. Ackerman and D. T. Davis, "Privacy and Security Issues in E-Commerce."

[13] M. Niranjanamurthy and D. Chahar, "The study of E-Commerce Security Issues and Solutions," International Journal of

Advanced Research in Computer and Communication Engineering, 2013. .

[14] V. Jinson, “Ecommerce Security: Importance, Issues & Protection Measures.” https://www.getastra.com/blog/knowledge-base/ecommerce-security/ (accessed Nov. 22, 2021).

[15] S. Furnell, “E-commerce security: a question of trust,” Comput. Fraud Secur., vol. 2004, no. 10, pp. 10–14, Oct. 2004, doi: 10.1016/S1361-3723(04)00122-8.

[16] M. P. Gupta and A. Dubey, “International Journal of Computer Science and Mobile Computing E-Commerce-Study of Privacy, Trust and Security from Consumer’s Perspective,” Int. J. Comput. Sci. Mob. Comput., vol. 5, no. 6, pp. 224–232, 2016, Accessed: Nov. 22, 2021. [Online]. Available: www.ijcsmc.com.

[17] S. R. Nallamothu, “Individual Paper - INTUITION OF PRIVACY AND SECURITY IN E-COMMERCE Intuition of Privacy and Security in E-Commerce Sasi Rekha Nallamothu University of | Course Hero.” https://www.coursehero.com/file/12474234/Individual-Paper/ (accessed Nov. 23, 2021).

[18] W. Lawrence, “Potential Security Threats To Your Computer Systems.” https://www.guru99.com/potential-security-threats-to-your-computer-systems.html (accessed Nov. 22, 2021).

[19] A. K. Ghosh, “E-Commerce Security: No Silver Bullet,” Database Secur. XII, pp. 3–16, 1999, doi: 10.1007/978-0-387-35564-1_1.

[20] P. B. Rane and B. B. Meshram, “Transaction Security for E-commerce Application,” vol. 2, no. 1, Accessed: Nov. 22, 2021. [Online]. Available: www.ijecse.org.

[21] J. Singh, “Review of e-Commerce Security Challenges,” Int. J. Innov. Res. Comput. Commun. Eng. (An ISO, vol. 3297, no. 2, 2007, Accessed: Nov. 22, 2021. [Online]. Available: www.ijircce.com.

[22] D. Kaushik, A. Gupta, and S. Gupta, “E-Commerce Security Challenges: A Review,” Accessed: Nov. 23, 2021. [Online]. Available: https://ssrn.com/abstract=3595304.

[23] W. Yuanqiao, Z. Chunhui, M. Juan, and L. Kezhong, “Research on E-commerce security issues,” 2008 Int. Semin. Bus. Inf. Manag. ISBIM 2008, vol. 1, pp. 186–189, 2008, doi: 10.1109/ISBIM.2008.168.

[24] S. M. Rahman, “E-Commerce Systems Security for Small Businesses PhD Learners at Capella View project OAuth-SSO: A Framework to Secure the OAuth-based SSO Service for Packaged Web Applications View project,” doi: 10.5121/ijnsa.2013.5215.

[25] J. Bytnar and K.-P. Anna, “The Study of E-Commerce Security Issues and Solutions,” Int. J. Eng. Res. Technol., vol. 4, no. 27, pp. 269–275, Apr. 2018, Accessed: Nov. 23, 2021. [Online]. Available: https://www.researchgate.net/publication/224370553.

[26] K. Haseeb, M. Arshad, and S. Ali, “Secure E-Commerce Protocol.”

[27] S. Chari, P. Kermani, S. Smith, and L. Tassiulas, “Security Issues in M—Commerce: A Usage—Based Taxonomy,” E-Commerce Agents, pp. 264–282, Nov. 2001, doi: 10.1007/3-540-45370-9_16.

[28] O. Rababah and F. Masoud, “Key Factors for Developing a Successful E-commerce Website,” Commun. IBIMA, pp. 1–9, Jan. 2010, doi: 10.5171/2010.763461.

[29] “Prof .Waghmare G.T. - Isrj.net.” https://www.yumpu.com/en/document/view/9847621/prof-waghmare-gt-isrjnet (accessed Nov. 23, 2021).

[30] N. Kuruwitaarachchi, L. R. P.K.W. Abeygunawardena, and S.W.I.Udara, “View of A Systematic Review of Security in Electronic Commerce- Threats and Frameworks,” Global Journal of Computer Science and Technology: ENetwork, Web & Security. https://computerresearch.org/index.php/computer/article/view/1794/1778 (accessed Nov. 22, 2021).

[31] R. J. Langdon, P. D. Yousefi, C. L. Relton, and M. J. Suderman, “Effective management and policy in e-business security,” Clin. Epigenetics, pp. 750–765, 2001, doi: 10.2/JQUERY.MIN.JS.

[32] [7]. Yousef A.Baker El-Ebiary, Samer Bamansoor, Waheeb Abu-Ulbeh, Wan Mohd Amir, Syarilla Iryani A. Saany, M. Hafiz Yusoff. “A Prognosis of Chinese E-Governance” Vol. 68, Editor’s Issues, Oct. 2020, pp. 86-89, IJETT, doi: 10.14445/22315381/CATI1P215.

[8]. Yousef A.Baker El-Ebiary, Waheeb Abu-Ulbeh, Najeeb Abbas Al-Sammarraie, M. Hafiz Yusoff , W. M. Amir Fazamin W. Hamzah, Syarilla Iryani A. Saany. “The Role of ICT in Special Educational Needs – A Case Study of Malaysia” Vol. 68, Editor’s Issues, Oct. 2020, pp. 90-93, IJETT, doi: 10.14445/22315381/CATI1P216.

[9]. W. M. Amir Fazamin W. Hamzah, Waheeb Abu-Ulbeh, Najeeb Abbas Al-Sammarraie, Yousef A.Baker El-Ebiary, M. Hafiz Yusoff, Syarilla Iryani A. Saany, Azliza Yacob. “The Integration of Learning Management Systems with PLE – a Review Paper” Vol. 68, Editor’s Issues, Oct. 2020, pp. 94-96, IJETT, doi: 10.14445/22315381/CATI1P217.

[10]. Syarilla Iryani A. Saany, Waheeb Abu-Ulbeh, Najeeb Abbas Al-Sammarraie, Yousef A.Baker El-Ebiary, M. Hafiz Yusoff, W. M. Amir Fazamin W. Hamzah, Yanty Faradillah. “A New E-Learning Technique Using Mobility Environment” Vol. 68, Editor’s Issues, Oct. 2020, pp. 97-100, IJETT, doi: 10.14445/22315381/CATI1P218.

[11]. Hazem M Bani Abdoh, Syarilla Iryani A. Saany, Hamid H. Jebur, Yousef El-Ebiary. “The Effect of PESTLE Factors on E-Government Adoption in Jordan: A Conceptual Model” Vol. 68, Editor’s Issues, Oct. 2020, pp. 19-23, IJETT, doi: 10.14445/22315381/CATI3P203.

[12]. Y. A. B. El-Ebiary, "The Effect of the Organization Factors, Technology and Social Influences on E-Government Adoption in Jordan," 2018 International Conference on Smart Computing and Electronic Enterprise (ICSCEE), Shah Alam, Malaysia, 2018, pp. 1-4. IEEE Xplore, Scopus: 19 November 2018, DOI: 10.1109/ICSCEE.2018.8538394.

[13]. Y. A. Baker El-Ebiary et al., "Blockchain as a decentralized communication tool for sustainable development," 2021 2nd International Conference on Smart Computing and Electronic Enterprise (ICSCEE), 2021, pp. 127-133, doi: 10.1109/ICSCEE50312.2021.9497910.

[14]. Y. A. Baker El-Ebiary et al., "Track Home Maintenance Business Centers with GPS Technology in the IR 4.0 Era," 2021 2nd International Conference on Smart Computing and Electronic Enterprise (ICSCEE), 2021, pp. 134-138, doi: 10.1109/ICSCEE50312.2021.9498070.

[15]. S. I. Ahmad Saany et al., "Exploitation of a Technique in Arranging an Islamic Funeral," 2021 2nd International Conference on Smart Computing and Electronic Enterprise (ICSCEE), 2021, pp. 1-8, doi: 10.1109/ICSCEE50312.2021.9498224.

[16]. J. A. Jusoh et al., "Track Student Attendance at a Time of the COVID-19 Pandemic Using Location-Finding Technology," 2021 2nd International Conference on Smart Computing and Electronic Enterprise (ICSCEE), 2021, pp. 147-152, doi: 10.1109/ICSCEE50312.2021.9498043.

[17]. Y. A. Baker El-Ebiary et al., "E-Government and E-Commerce Issues in Malaysia," 2021 2nd International Conference on Smart Computing and Electronic Enterprise (ICSCEE), 2021, pp. 153-158, doi: 10.1109/ICSCEE50312.2021.9498092.

[18]. Y. A. B. El-Ebiary et al., "Determinants of Customer Purchase Intention Using Zalora Mobile Commerce Application," 2021 2nd International Conference on Smart Computing and Electronic Enterprise (ICSCEE), 2021, pp. 159-163, doi: 10.1109/ICSCEE50312.2021.9497995.

[19]. S. Bamansoor et al., "Efficient Online Shopping Platforms in Southeast Asia," 2021 2nd International Conference on Smart Computing and Electronic Enterprise (ICSCEE), 2021, pp. 164-168, doi: 10.1109/ICSCEE50312.2021.9497901.

[20]. S. Bamansoor et al., "Evaluation of Chinese Electronic Enterprise from Business and Customers Perspectives," 2021 2nd International Conference on Smart Computing and Electronic Enterprise (ICSCEE), 2021, pp. 169-174, doi: 10.1109/ICSCEE50312.2021.9498093.

[21]. Altrad et al., "Amazon in Business to Customers and Overcoming Obstacles," 2021 2nd International Conference on Smart Computing and Electronic Enterprise (ICSCEE), 2021, pp. 175-179, doi: 10.1109/ICSCEE50312.2021.9498129.

[22]. Y. A. Baker El-Ebiary et al., "Mobile Commerce and its Apps - Opportunities and Threats in Malaysia," 2021 2nd International Conference on Smart Computing and Electronic Enterprise (ICSCEE), 2021, pp. 180-185, doi: 10.1109/ICSCEE50312.2021.9498228.

[23]. M. B. Mohamad et al., "Enterprise Problems and Proposed Solutions Using the Concept of E-Commerce," 2021 2nd International Conference on Smart Computing and Electronic Enterprise (ICSCEE), 2021, pp. 186-192, doi: 10.1109/ICSCEE50312.2021.9498197.

[24]. P. R. Pathmanathan et al., "The Benefit and Impact of E-Commerce in Tourism Enterprises," 2021 2nd International Conference on Smart Computing and Electronic Enterprise (ICSCEE), 2021, pp. 193-198, doi: 10.1109/ICSCEE50312.2021.9497947.

[25]. K. Aseh et al., "The Future of E-Commerce in the Publishing Industry," 2021 2nd International Conference on Smart Computing and Electronic Enterprise (ICSCEE), 2021, pp. 199-205, doi: 10.1109/ICSCEE50312.2021.9498175.

[26]. S. M. S. Hilles et al., "Latent Fingerprint Enhancement and Segmentation Technique Based on Hybrid Edge Adaptive DTV Model," 2021 2nd International Conference on Smart Computing and Electronic Enterprise (ICSCEE), 2021, pp. 8-13, doi: 10.1109/ICSCEE50312.2021.9498025.

[27]. S. M. S. Hilles et al., "Adaptive Latent Fingerprint Image Segmentation and Matching using Chan-Vese Technique Based on EDTV Model," 2021 2nd International Conference on Smart Computing and Electronic Enterprise (ICSCEE), 2021, pp. 2-7, doi: 10.1109/ICSCEE50312.2021.9497996.

[28]. Y. M. A. Tarshany, Y. Al Moaiad and Y. A. Baker El-Ebiary, "Legal Maxims Artificial Intelligence Application for Sustainable Architecture And Interior Design to Achieve the Maqasid of Preserving the Life and Money," 2022 Engineering and Technology for Sustainable Architectural and Interior Design Environments (ETSAIDE), 2022, pp. 1-4, doi: 10.1109/ETSAIDE53569.2022.9906357.

[29]. W. A. H. M. Ghanem et al., "Cyber Intrusion Detection System Based on a Multiobjective Binary Bat Algorithm for Feature Selection and Enhanced Bat Algorithm for Parameter Optimization in Neural Networks," in IEEE Access, vol. 10, pp. 76318-76339, 2022, doi: 10.1109/ACCESS.2022.3192472.

[30]. Iswanto, A., Gustina Zainal, A., Murodov, A., A. Baker El-Ebiary, Y., & G. Sattarova, D. (2022). Studying the role of Islamic religious beliefs on depression during COVID-19 in Malaysia. HTS Teologiese Studies / Theological Studies, 78(4), 6 pages. doi: https://doi.org/10.4102/hts.v78i4.7567.

[31]. Partono Prasetio, A., Duc Tai, T., Jade Catalan Opulencia, M., Abbas, M., A. Baker El-Ebiary, Y., Fadhil Abbas, S., Bykanova, O., Samal, A., & Iswanto, A. (2022). Impact of the COVID-19 pandemic on religious tourism amongst Muslims in Iraq. HTS Teologiese Studies / Theological Studies, 78(4), 6 pages. doi: https://doi.org/10.4102/hts.v78i4.7565.

[33] R. Yazdanifard, N. Al-Huda Edres,

and A. P. Seyedi, “Security and Privacy Issues as a Potential Risk for Further E-commerce Development.”

[34] M. Halaweh and Y. J. Kim, “Integration of Grounded Theory and Case Study: An Exemplary Application from e-Commerce Security Perception Research,” vol. 13, no. 1, pp. 31–51, 2012, Accessed: Nov. 22, 2021. [Online]. Available: www.groundedtheory.com/.

[35] M. Umar, N. Uddin, and O. Shopping, “Consumers’ Attitude towards Online Shopping : Factors influencing Gotland consumers to shop online,” 2011, Accessed: Nov. 23, 2021. [Online]. Available: http://urn.kb.se/resolve?urn=urn:nbn:se:hgo:diva-914.

[36] “(PDF) Information Secuirty Awareness as Management Decisions: A Conceptual Application.” https://www.researchgate.net/publication/332118308_Information_Secuirty_Awareness_as_Management_Decisions_A_Conceptual_Application (accessed Nov. 23, 2021).