Contents lists available at Science-Gate

International Journal of Advanced and Applied Sciences

Journal homepage: http://www.science-gate.com/IJAAS.html

Integrated e-commerce security model for websites

Ibrahim Alfadli *

Department of Information Systems, College of Computer Science and Engineering, Taibah University, Medina, Saudi Arabia

ARTICLE INFO

Article history:
Received 28 October 2021
Received in revised form
31 January 2022
Accepted 14 February 2022

Keywords:
E-commerce
Financial attacks
Web security
Digital forensics

ABSTRACT

E-commerce is the branch of digital life that contains all economic and trade businesses conducted via the internet and commercial procedures connected to these businesses. It is considered the major and fastest-growing area in the world. It is the greatest way of purchasing goods and services done net. The old buying was changed by e-commerce only through this Covid pandemic. However, the enormous challenge of e-commerce is insider and outsider cyber-attacks, which threats the confidentiality, integrity, and availability of e-commerce. The researchers have proposed several security models and frameworks for the e-commerce field; however, there is a lack of an integrated model to secure the purchasing and selling of websites. Thus, this study presents a survey of cyberattacks that may damage e-commerce and proposes an integrated security model for e-commerce using a design science approach. The proposed model comprises three main parts: Client, e-commerce, and security. The results show that the proposed model can ensure purchasing and selling on the website and instantiate their solution models using a modeling approach.

1. Introduction

The internet plays a vital function both in individuals and in entrepreneurship. The online transaction has to be secured since there is a significant increase in cyber-crimes; as per the principles of e-commerce, some conditions are necessary to ensure the security of e-commerce mentioned below. In the network's context, security and integrity are a way to preserve customers' confidence, consistency, and accuracy with the data. It also applies to protecting data against unauthorized user change. One of the standard algorithms used to get the message authentication is an authentication code Mandatory Access Control (MAC). There are also rising risks and problems with an internet business or e-commerce. The effects of intellectual property law of commerce, customer disputes, reimbursement, product housing, and logistics. Security is the danger that any e-commerce company manager must overlook.

E-commerce security may be described as implementing the collection of protocols or regulations that carry out all e-commerce transactions safely. These safety criteria should be put in a position to protect the security of different e-commerce firms against a range of undeniable hazards. Online security during Internet transactions is one of the critical jobs (Sengupta et al., 2005). Many programs handle electronic payments that depend on web-based e-commerce. In this article, we discuss the existing security models that deal with the various forms of assaults and e-commerce risks and propose a new model that counters the security risk and increases the trustworthiness of the e-commerce systems.

This paper aims to propose a security model for e-commerce websites using the design science method. The proposed model comprises three parts: A client part, e-commerce part, and security part. The client part is used to prepare the client information before sending it to the e-commerce part. It has five activities: Sending an order, receiving it, deleting the ordering, payment, and revising it. The e-commerce part is used to handle/process the client's request. It is further made of six activities: Availability, quality, price of the order, time of order, seller, and shipping path. The security part is used to secure both parts (client and e-commerce) during sending, processing, and receiving. It consists of seven activities: Authentication, authorization, encryption, firewall, IDS, hashing, and recording. This study adapted the design science method for this purpose.

* Corresponding Author.
Email Address: ialfadli@taibahu.edu.sa
https://doi.org/10.21833/ijaas.2022.04.013
Corresponding author's ORCID profile:
https://orcid.org/0000-0002-4549-357X

The rest of this paper is structured as follows: Section 1 gives an introduction to e-commerce security. Section 2 offers the literature review. Section 3 covers the methodology, and Section 4 produces the results and discussion. Finally, Section 5 concludes the paper.

2. Literature review

This section evaluates the existing attacks statistically based on the published works between 2010 and 2021. We picked e-commerce businesses since cyber threats mainly affected them after a financial industry. Though e-commerce uses strong marketing or engaging web design, cyberattacks can damage the company. Fig. 1 shows that maximum work is done on financial fraud attacks followed by brute force attacks, bot attacks, spam attacks, etc. The minor publications are done on the distributed denial of service (DDoS) attack and SQL injection. In the coming sections, we will explain all these attacks.

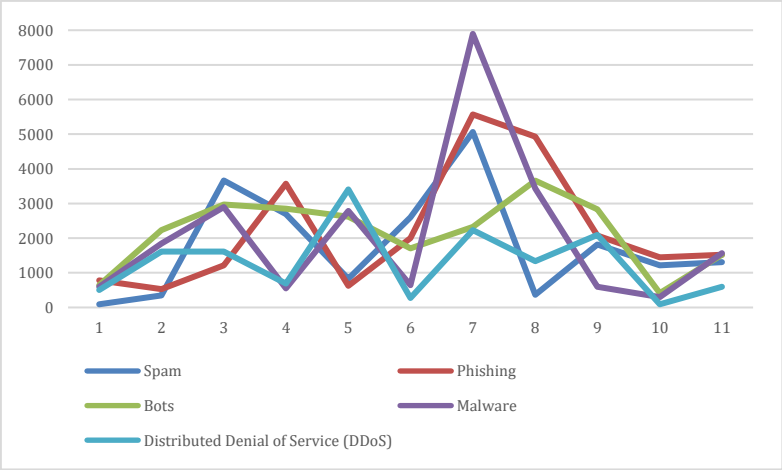

Fig. 1: Attack wise publication summary between 2010 and 2021 (Badotra and Sundas, 2021)

2.1. Financial fraud attack

Fig. 1 shows that during the past eleven years (2010-2021), publications were highest for financial fraud strikes on e-commerce sites. E-commerce fraud increases quickly, and payment methods attract cybercriminals in large portions (Fletcher, 2007). The hackers have conducted illegal transactions that lead to considerable losses for the company. The standard financial frauds include triangulation fraud (Wang et al., 2006; Hayes, 2020; Paintal, 2021), identity theft (Aïmeur and Schőnfeld, 2011; Paintal, 2021), friendly fraud (Guo et al., 2015), and affiliate fraud (Amarasekara and Mathrani, 2016; Dong et al., 2021) and clean fraud (Foley, 2016; Manohar et al., 2021). Fig. 2 shows the maximal investigation of an identity fraud followed by friendly, clean, fraudulent attacks by affiliates. Although triangulation attacks are rising nowadays, researchers have done minimal research in this area.

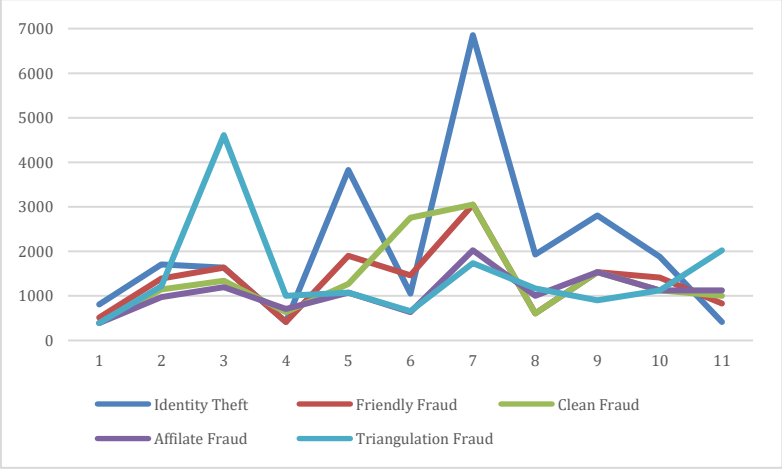

Fig. 2: Research publication summary of different types of financial fraud between 2010 and 2021(Badotra and Sundas, 2021)

2.2. Brute force attack

Hackers attempt to guess a password to breach a website's authenticated mechanism and get access to a web application's secret information. Although it is an ancient form of attack, its popularity surges because of the exponential growth in IoT devices. A brute force attack was launched on "eBay of China."

For two months, hackers hacked the accounts of 21 million consumers. In 2019, the Sucuri Firewall successfully prevented 1.3 million brute-force attempts (Badotra and Sundas, 2021).

2.3. Trojan horses attack

It's a pretty frequent sort of software that's susceptible. This program hides in the background of a computer and performs harmful activities. Unlike worms and viruses, it does not replicate itself. According to some experts, the Trojan horse introduces most viruses into a system. It may connect itself to a system's authentication mechanism, copy all authentication credentials, such as login and password, and communicate with its owner (Salomon, 2010). IcedID, SpyEye, Gootkit2, Panda, Chthonic, Zeus, Gozi, TinyNuke, and Betabot are examples of banking Trojans.

2.4. DDoS attack

DDoS assaults are one of the most severe dangers to the E-commerce sector (Bhardwaj et al., 2020). DDoS intrusions are quickly increasing, according to Kaspersky's DDoS Protection data. The number of incidents had increased to 84 percent, and they had lasted for more than 60 minutes, nearly doubling. China had risen to the top of the list of countries targeted by DDoS attacks, followed by the United States and Hong Kong (Kaspersky and Furnell, 2014).

2.5. Bot attack

Bots are used to perform e-commerce fraud such as scalping, false account creation, gift and credit card account takeover. It is one of the most common problems that an e-commerce website may encounter (Aswal et al., 2020). It may steal and leak the product's pricing and information to other e-commerce competitors for their benefit. On the other side, it tries to hack into client accounts to steal money through gift or credit card fraud. According to the most recent cyber-crime data, 210 million fraudulent attacks occurred in the first quarter of 2018, up 62 percent over 2017 (Badotra and Sundas, 2021).

2.6. Malware attack

Malware is a common cyber danger to e-commerce sites (Kashinath et al., 2021). Its major goal is to steal credit card information. These sorts of cyberattacks are on the rise; in only six months, 7,339 E-commerce sites had been compromised.

2.7. Cross-site scripting (XSS) attack

The vulnerable web applications' users are in grave danger. It's a relatively popular attack that involves injecting malicious code into a susceptible web application. It has the potential to harm a digital business's reputation and its consumer relationships. There are two forms of cross-site scripting attacks: Stored XSS and reflected XSS. XSS that is accumulated is more harmful than XSS that is reflected (Rodríguez et al., 2020). All online applications are vulnerable and have at least one risk, according to the Cisco annual security report in 2018. Web risks are getting more complex, precise, and pervasive, according to the research. It further said that 40 percent of all attempted attacks use a technique known as cross-site scripting. As a result, it is the most commonly used method (Rodríguez et al., 2020).

2.8. Spam attack

A spam attack is defined as an unsolicited mass communication transmitted by instant messaging, email, or other IoT devices (Pradeep and Kj, 2016). Advertisers typically utilize it to advertise their products without incurring any running fees. It may also be used to hack a website, allowing hackers to collect all of the information on the site, modify the website code, and upload harmful files. Furthermore, the hacked website was exploited by hackers to send spam emails to other websites (Shahapurkar, 2021).

3. Website attacks and digital forensic investigation

Several websites' attacks have been mentioned in the previous section. These attacks threaten the confidentiality, integrity, and availability of the websites. Therefore, the digital forensics investigation field is required to investigate these attacks and reveal who the attacker is, when the attack happened, and which part of the data.

Several forensics models and frameworks have been proposed to identify, collect, preserve, analyze and document websites attacks. For example, Ngadi et al. (2012), Ali et al. (2014; 2015; 2017a; 2017b), Al-Dhaqm et al. (2014; 2016; 2017a; 2017b; 2018; 2020a; 2020b; 2020c; 2020d, 2021a; 2021b; 2021c), Abd Razak et al. (2016; 2020), Onwuegbuzie et al. (2020), Kebande et al. (2020), Alfadli et al. (2021), Ghabban et al. (2021), Saleh et al. (2021), and Zawali et al. (2021) suggested several models and frameworks identify and discover these attackers.

4. Relationship between website usability and security

The security of an e-commerce site or business is highly dependent on the usability factors of the website. Therefore, a large number of researchers discussed the security and usability of the e-commerce models. The site's usability increases customer trust on one side and minimizes the attacks on the other side. Thus, a highly usable e-commerce model increases the customer base by reducing risk factors (Mohd and Zaaba, 2019).

Usable security may be described as improving the safety of a system and taking into account customers' interactions. Usability and security come together, and they are interdependent. Measuring usability also assesses security because they are not unique to each other. A highly secure system leads to a helpful system (Chandler and Hyatt, 2003). These are multidimensional subjects that are highly challenging to measure usability and security (Zaaba et al., 2011). Website usability and safety may be determined using different related criteria at the human and organizational levels (Gray and Salzman, 1998). The mixing establishes a model that shows a model in one framework of numerous factors, such as security, website quality, satisfaction, and training. Several previous assessment studies tried to assess e-commerce usability and security using models (Palmer, 2001).

4.1. Strength and weakness of the existing website usability and security models

It evaluates whether the current e-commerce methods can highlight all usability and security features in a single paradigm. Mapping the qualities assessed by the methods into usability features and security dimensions summarizes each model's advantages and disadvantages. Table 1 presents a review of the models based on the mapping to determine whether they can capture usability features and include security factors in each model's evaluation.

From all the models offered above, most of the models mainly measured only the component learnability and satisfaction. None of the models were able to capture all the features of usability and security altogether. McCloskey (2004), Al-Dwairi and Kamala (2009), and Chong et al. (2012) assessed the most significant usability and security elements. McCloskey (2004) measured learnability, efficiency, satisfaction and, security. At the same time, Chong et al. (2012) measured learnability, efficiency, satisfaction and, memorability. Al-Dwairi and Kamala (2009) measured learnability, satisfaction, privacy and, security. Only Szymanski and Hise (2000), McCloskey (2004), Pikkarainen et al. (2004), Lim et al. (2005), and Al-Dwairi and Kamala (2009) added the element security in their model.

By examining the advantages and disadvantages of each model, it is sure that there is an absence of one complete model that can assess the usability and security of an e-commerce website. Without a full model that comprises usability and security fundamentals, the assessment of the e-commerce model is not practical. It would not be able to deliver a whole vision for development. The aim of usability assessment is mostly to notice parts that sound for action and then improve the difficulties for a working package. The current assessment models do not achieve this aim. Most of the existing models only assess specific usability features rather than talking about all 5 usability elements with security fundamentals in a model. None of the current models gather all 5 usability elements and collected with the security fundamentals. While each of the models stated overhead made famous aids, there is still no one model that has combined all 5 usability features with the security fundamentals into one wide model.

Table 1: Strength and weakness of website usability and security models

Model	Usability Features					Security Feature		
	Learnability	Efficiency	Memorability	Error	Satisfaction	Privacy	Safety	Data Protection
Szymanski and Hise (2000)	✓	×	×	×	✓	✓	×	✓
McKnight et al. (2000)	✓	×	×	×	✓	×	×	✓
Devaraj et al. (2000)	✓	✓	×	×	✓	×	×	✓
McCloskey (2004)	✓	✓	×	×	×	×	✓	×
Lim et al. (2005)	✓	×	×	×	✓	×	✓	✓
Al-Dwairi and Kamala (2009)	✓	×	×	×	✓	✓	✓	×
Green and Pearson (2009)	✓	×	×	✓	✓	×	×	✓
Pikkarainen et al. (2004)	✓	✓	×	×	×	✓	×	×
Chong et al. (2012)	✓	✓	✓	×	✓	×	×	✓
Ali and Raza (2017)	✓	✓	✓	×	×	×	×	✓
Rodríguez et al. (2020)	✓	×	×	✓	×	×	×	✓

5. Methodology

This paper adopted a Design Science Research (DSR) method to develop the proposed artifact, mentioned as the E-Commerce Security Model for the Websites (Al-Dhaqm et al., 2017b; Al-Dhaqm et al., 2020b; Al-Dhaqm et al., 2021c). DSR is a investigative method used to generate original and insistent objects for a particular problem area that allows analytics to be studied (March and Smith, 1995). This specific application of DSR focuses on information technology artifacts that meaningly influence the requested location. According to (March and Smith, 1995), the making of DSR can be clarified in terms of 4 types of artifacts that contain: concepts that establish the verbal to classify difficulties and answers, artifacts that use this oral to define difficulties and answers, approaches that describe procedures that suggestion help on how to response challenges and the final artifact derive which are clear as groupings of concepts, artifacts, and techniques. The DSR life-cycle holds the repetitious assessment of produced artifacts. Therefore, authors identify, select, and group concepts, activities, and tasks of the e-commerce security domain and combine them in one abstract platform called the E-commerce security model for websites.

6. Results and discussion

The proposed e-commerce security model for the website illustrated in Fig. 3 consists of three main parts: client, e-commerce, and security. Each part has several activities. The client part is used to prepare the client information before sending it to the e-commerce part. It comprises five activities: Sending the order, receiving it, deleting the ordering, payment, and revising it. The e-commerce part is used to handle/process the client's request. It has six activities: Availability, quality, price of the order, time of order, seller, and shipping path. The security part is used to secure both parts (client and e-commerce) during sending, processing, and receiving. It contains seven activities: Authentication, authorization, encryption, firewall, IDS, hashing, and recording.

Therefore, this model allows users to derive/instantiate their models easily. Assume this scenario, "Fahad wants to buy iPhone from the Lazada website." In this scenario, Fahad and iPhone are the first part (client part), where is Lazada website is the second part (e-commerce part). Therefore, Fahad sends his order to the Lazada website. The security part is used before, during, and after sending the request. Before sending the request, the security part checks the authentication and authorization of the Fahad by inserting the user's name and password and restricting the level of approval of the Fahad against the Lazada website. During sending, the security part will use the encryption activity to protect Fahad's request from any attacks. In the e-commerce part, if the request/order is available, Fahad will check the quality, price, and shipping time. Here, Fahad can agree, delete, or change the request/order. If Fahad agrees to buy the iPhone device, he needs to pay the device's price using payment activity in the client part. The security part will protect the purchasing process using hashing and encryption activities. The firewall and IDS activities are used to protect both interests from insider or outsider threats. Finally, Fahad will receive the order details, contact the seller, and ask about the shipping path and time of delivery. Fig. 4 displays how Fahad can instantiate a real scenario to purchase iPhone derived from the e-commerce security model.

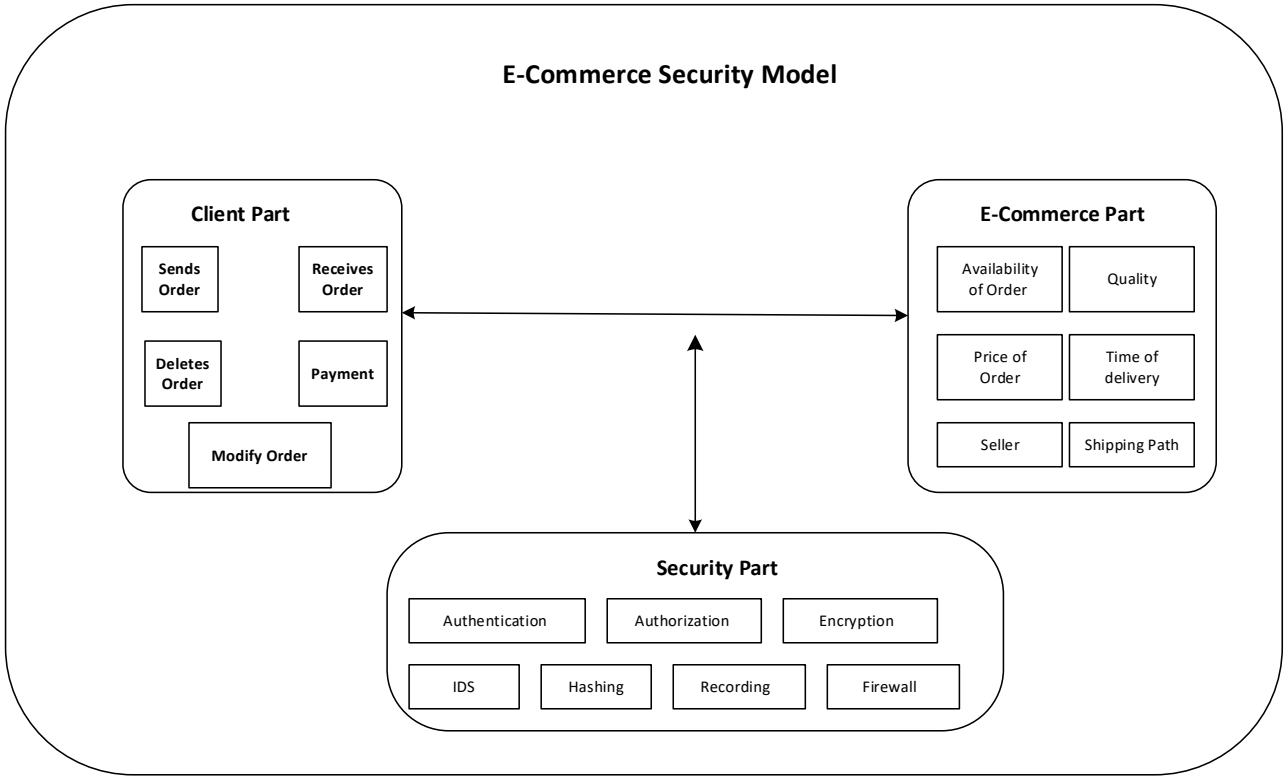

Fig. 3: E-commerce security model for website

7. Conclusion

The security and usability of the e-commerce models are working together to improve the overall performance, increase usability, and provide a secure environment for the end client. In this paper, the proposed model is simplified and improved. It served two basic purposes. The three-level security model provides improved security and serves both the merchant and the client. Secondly, it simplifies the process to improve performance. It incorporates the encryption for secure payment as check the additional parameters of order successful completion. The same model will increase the clients' experience and trust that will help in increasing the client base. Besides these improvements, the model is generalized to be used in any e-commerce scenario to serve a larger community of users.

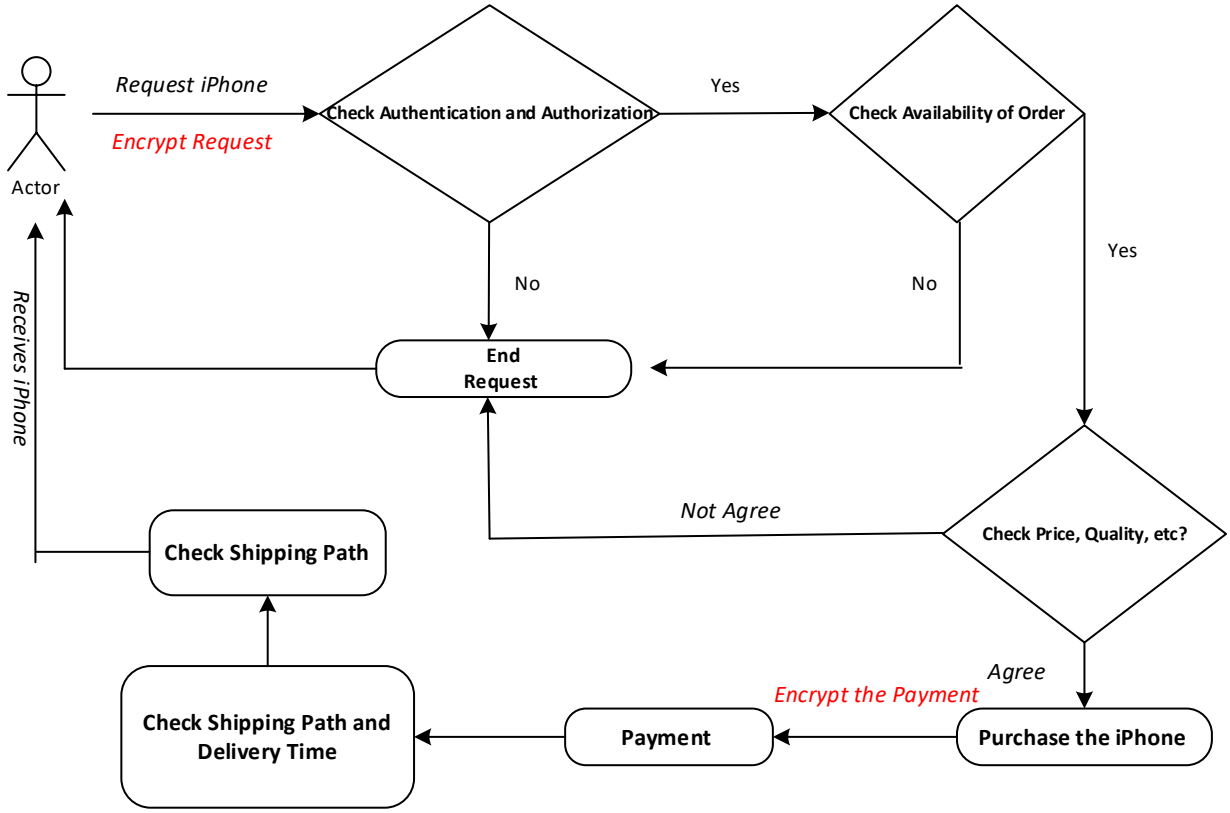

Fig. 4: Real scenario: Instantiate purchase model from the e-commerce security model

Compliance with ethical standards

Conflict of interest

The author(s) declared no potential conflicts of interest with respect to the research, authorship, and/or publication of this article.

References

Abd Razak S, Nazari NHM, and Al-Dhaqm A (2020). Data anonymization using pseudonym system to preserve data privacy. IEEE Access, 8: 43256-43264. https://doi.org/10.1109/ACCESS.2020.2977117

Abd Razak S, Othman SH, Aldolah AA, and Ngadi MA (2016). Conceptual investigation process model for managing database forensic investigation knowledge. Research Journal of Applied Sciences, Engineering and Technology, 12(4): 386-394. https://doi.org/10.19026/rjaset.12.2377

Aïmeur E and Schőnfeld D (2011). The ultimate invasion of privacy: Identity theft. In the 19th Annual International Conference on Privacy, Security and Trust, IEEE, Montreal, Canada: 24-31. https://doi.org/10.1109/PST.2011.5971959

Al-Dhaqm A, Abd Razak S, Dampier DA, Choo KKR, Siddique K, Ikuesan RA, and Kebande VR (2020b). Categorization and organization of database forensic investigation processes. IEEE Access, 8: 112846-112858. https://doi.org/10.1109/ACCESS.2020.3000747

Al-Dhaqm A, Abd Razak S, Ikuesan RA, Kebande VR, and Siddique K (2020a). A review of mobile forensic investigation process models. IEEE Access, 8: 173359-173375. https://doi.org/10.1109/ACCESS.2020.3014615

Al-Dhaqm A, Abd Razak S, Othman SH, Ali A, Ghaleb FA, Rosman AS, and Marni N (2020c). Database forensic investigation process models: A review. IEEE Access, 8: 48477-48490. https://doi.org/10.1109/ACCESS.2020.2976885

Al-Dhaqm A, Abd Razak S, Othman SH, Nagdi A, and Ali A (2016). A generic database forensic investigation process model. Journal Teknologi, 78(6-11): 45-57. https://doi.org/10.11113/jt.v78.9190

Al-Dhaqm A, Abd Razak S, Siddique K, Ikuesan RA, and Kebande VR (2020d). Towards the development of an integrated incident response model for database forensic investigation field. IEEE Access, 8: 145018-145032. https://doi.org/10.1109/ACCESS.2020.3008696

Al-Dhaqm A, Ikuesan RA, Kebande VR, Razak S, and Ghabban FM (2021c). Research challenges and opportunities in drone forensics models. Electronics, 10(13): 1519. https://doi.org/10.3390/electronics10131519

Al-Dhaqm A, Ikuesan RA, Kebande VR, Razak S, Grispos G, Choo KKR, and Alsewari AA (2021a). Digital forensics subdomains: The state of the art and future directions. IEEE Access, 9: 152476-152502. https://doi.org/10.1109/ACCESS.2021.3124262

Al-Dhaqm A, Razak S, and Othman SH (2018). Model derivation system to manage database forensic investigation domain knowledge. In the IEEE Conference on Application, Information and Network Security, IEEE, Langkawi, Malaysia: 75-80. https://doi.org/10.1109/AINS.2018.8631468

Al-Dhaqm A, Razak S, Ikuesan RA, Kebande VR, and Hajar Othman S (2021b). Face validation of database forensic investigation metamodel. Infrastructures, 6(2): 13. https://doi.org/10.3390/infrastructures6020013

Al-Dhaqm A, Razak S, Othman SH, Choo KKR, Glisson WB, Ali A, and Abrar M (2017a). CDBFIP: Common database forensic

investigation processes for Internet of Things. IEEE Access, 5: 24401-24416. https://doi.org/10.1109/ACCESS.2017.2762693

Al-Dhaqm A, Razak S, Othman SH, Ngadi A, Ahmed MN, and Ali Mohammed A (2017b). Development and validation of a database forensic metamodel (DBFM). PLOS ONE, 12(2): e0170793. https://doi.org/10.1371/journal.pone.0170793 **PMid:28146585 PMCid:PMC5287479**

Al-Dhaqm AMR, Othman SH, Abd Razak S, and Ngadi A (2014). Towards adapting metamodelling technique for database forensics investigation domain. In the International Symposium on Biometrics and Security Technologies, IEEE, Kuala Lumpur, Malaysia: 322-327. https://doi.org/10.1109/ISBAST.2014.7013142

Al-Dwairi RM and Kamala MA (2009). An integrated trust model for business-to-consumer (b2c) e-commerce: Integrating trust with the technology acceptance model. In the International Conference on CyberWorlds, IEEE, Bradford, UK: 351-356. https://doi.org/10.1109/CW.2009.34

Alfadli IM, Ghabban FM, Ameerbakhsh O, AbuAli AN, Al-Dhaqm A, and Al-Khasawneh MA (2021). CIPM: Common identification process model for database forensics field. In the 2nd International Conference on Smart Computing and Electronic Enterprise, IEEE, Cameron Highlands, Malaysia: 72-77. https://doi.org/10.1109/ICSCEE50312.2021.9498014

Ali A, Abd Razak S, Othman SH, and Mohammed A (2017b). Extraction of common concepts for the mobile forensics domain. In the International Conference of Reliable Information and Communication Technology, Springer, Johor Bahru, Malaysia: 141-154. https://doi.org/10.1007/978-3-319-59427-9_16

Ali A, Abd Razak S, Othman SH, Mohammed A, and Saeed F (2017a). A metamodel for mobile forensics investigation domain. PLOS ONE, 12(4): e0176223. https://doi.org/10.1371/journal.pone.0176223 **PMid:28445486 PMCid:PMC5433730**

Ali A, Al-Dhaqm A, and Razak SA (2014). Detecting threats in network security by analyzing network packets using wire shark. In the International Conference of Recent Trends in Information and Communication Technologies, IEEE, Chennai, India.

Ali A, Razak SA, Othman SH, and Mohammed A (2015). Towards adapting metamodeling approach for the mobile forensics investigation domain. In the 1st International Conference on Innovation in Science and Technology, Kuala Lumpur, Malaysia: 364-367.

Ali M and Raza SA (2017). Service quality perception and customer satisfaction in Islamic banks of Pakistan: The modified SERVQUAL model. Total Quality Management and Business Excellence, 28(5-6): 559-577. https://doi.org/10.1080/14783363.2015.1100517

Amarasekara BR and Mathrani A (2016). Controlling risks and fraud in affiliate marketing: A simulation and testing environment. In the 14th Annual Conference on Privacy, Security and Trust, IEEE, Auckland, New Zealand: 353-360. https://doi.org/10.1109/PST.2016.7906986

Aswal K, Dobhal DC, and Pathak H (2020). Comparative analysis of machine learning algorithms for identification of BOT attack on the Internet of Vehicles (IoV). In the International Conference on Inventive Computation Technologies, IEEE, Coimbatore, India: 312-317. https://doi.org/10.1109/ICICT48043.2020.9112422

Badotra S and Sundas A (2021). A systematic review on security of E-commerce systems. International Journal of Applied Science and Engineering, 18(2): 1-19.

Bhardwaj A, Mangat V, and Vig R (2020). Hyperband tuned deep neural network with well posed stacked sparse AutoEncoder for detection of DDoS attacks in cloud. IEEE Access, 8: 181916-181929. https://doi.org/10.1109/ACCESS.2020.3028690

Chandler K and Hyatt K (2003). Customer-centered design: A new approach to Web usability. Prentice-Hall Professional, Hoboken, USA.

Chong X, Zhang J, Lai KK, and Nie L (2012). An empirical analysis of mobile internet acceptance from a value–based view. International Journal of Mobile Communications, 10(5): 536-557. https://doi.org/10.1504/IJMC.2012.048886

Devaraj S, Fan M, and Kohli R (2002). Antecedents of B2C channel satisfaction and preference: Validating e-commerce metrics. Information Systems Research, 13(3): 316-333. https://doi.org/10.1287/isre.13.3.316.77

Dong Y, Jiang Z, Alazab M, and Kumar P (2021). Real-time fraud detection in e-market using machine learning algorithms. Journal of Multiple-Valued Logic and Soft Computing, 36(1-3): 191-209.

Fletcher N (2007). Challenges for regulating financial fraud in cyberspace. Journal of Financial Crime, 14(2): 190-207. https://doi.org/10.1108/13590790710742672

Foley C (2016). E-commerce fraud: A guide to prevention. Ph.D. Dissertation, Utica College, Utica, USA.

Ghabban FM, Alfadli IM, Ameerbakhsh O, AbuAli AN, Al-Dhaqm A, and Al-Khasawneh MA (2021). Comparative analysis of network forensic tools and network forensics processes. In the 2nd International Conference on Smart Computing and Electronic Enterprise, IEEE, Cameron Highlands, Malaysia: 78-83. https://doi.org/10.1109/ICSCEE50312.2021.9498226

Gray WD and Salzman MC (1998). Damaged merchandise? A review of experiments that compare usability evaluation methods. Human–Computer Interaction, 13(3): 203-261. https://doi.org/10.1207/s15327051hci1303_2

Green DT and Pearson JM (2009). The examination of two web site usability instruments for use in B2C e-commerce organizations. Journal of Computer Information Systems, 49(4): 19-32.

Guo Y, Le-Nguyen K, Jia Q, and Li G (2015). Seller-buyer trust in cross-border e-commerce: A conceptual model. In the Twenty-first Americas Conference on Information Systems, San Juan, Puerto Rico: 1-7.

Hayes JK (2020). Cyber security and corporate fraud. In: Baker HK, Purda-Heeler L, and Saadi S (Eds.), Corporate fraud exposed: 279-298. Emerald Publishing Limited, Bingley, UK. https://doi.org/10.1108/978-1-78973-417-120201018

Kashinath SA, Mostafa SA, Mustapha A, Mahdin H, Lim D, Mahmoud MA, and Yang TJ (2021). Review of data fusion methods for real-time and multi-sensor traffic flow analysis. IEEE Access, 9: 51258-51276. https://doi.org/10.1109/ACCESS.2021.3069770

Kaspersky E and Furnell S (2014). A security education Q&A. Information Management and Computer Security, 22(2): 130-133. https://doi.org/10.1108/IMCS-01-2014-0006

Kebande VR, Ikuesan RA, Karie NM, Alawadi S, Choo KKR, and Al-Dhaqm A (2020). Quantifying the need for supervised machine learning in conducting live forensic analysis of emergent configurations (ECO) in IoT environments. Forensic Science International: Reports, 2: 100122. https://doi.org/10.1016/j.fsir.2020.100122

Lim K, Lim J, and Heinrichs JH (2005). Structural model comparison of the determining factors for e-purchase. Seoul Journal of Business, 11: 119-143.

Manohar GV, Bhattacharjee B, and Pratap M (2021). Preventing misuse of discount promotions in e-commerce websites: An application of rule-based systems. International Journal of Services Operations and Informatics, 11(1): 54-74. https://doi.org/10.1504/IJSOI.2021.114111

March ST and Smith GF (1995). Design and natural science research on information technology. Decision Support Systems, 15(4): 251-266. https://doi.org/10.1016/0167-9236(94)00041-2

McCloskey D (2004). Evaluating electronic commerce acceptance with the technology acceptance model. Journal of Computer Information Systems, 44(2): 49-57.

McKnight DH, Choudhury V, and Kacmar C (2002). Developing and validating trust measures for e-commerce: An integrative typology. Information Systems Research, 13(3): 334-359. https://doi.org/10.1287/isre.13.3.334.81

Mohd NA and Zaaba ZF (2019). A review of usability and security evaluation model of ecommerce website. Procedia Computer Science, 161: 1199-1205. https://doi.org/10.1016/j.procs.2019.11.233

Ngadi M, Al-Dhaqm R, and Mohammed A (2012). Detection and prevention of malicious activities on RDBMS relational database management systems. International Journal of Scientific and Engineering Research, 3(9): 1-10.

Onwuegbuzie IU, Abd Razak S, Fauzi Isnin I, Darwish TS, and Al-Dhaqm A (2020). Optimized backoff scheme for prioritized data in wireless sensor networks: A class of service approach. PLOS ONE, 15(8): e0237154. https://doi.org/10.1371/journal.pone.0237154 **PMid:32797055 PMCid:PMC7428073**

Paintal S (2021). Ecommerce and online security. International Journal of Management, 12(1): 682-687.

Palmer G (2001). A road map for digital forensic research. In the First Digital Forensic Research Workshop, Utica, USA: 27-30.

Pikkarainen T, Pikkarainen K, Karjaluoto H, and Pahnila S (2004). Consumer acceptance of online banking: An extension of the technology acceptance model. Internet Research, 14(3): 224-235. https://doi.org/10.1108/10662240410542652

Pradeep P and Kj S (2016). Detection of SPAM attacks in the remote triggered WSN experiments. In: Kim K and Joukov N (Eds.), Information science and applications: 715-727. Springer, Singapore, Singapore. https://doi.org/10.1007/978-981-10-0557-2_70

Rodríguez GE, Torres JG, Flores P, and Benavides DE (2020). Cross-site scripting (XSS) attacks and mitigation: A survey. Computer Networks, 166: 106960. https://doi.org/10.1016/j.comnet.2019.106960

Saleh MA, Othman SH, Al-Dhaqm A, and Al-Khasawneh MA (2021). Common investigation process model for internet of things forensics. In the 2nd International Conference on Smart Computing and Electronic Enterprise, IEEE, Cameron Highlands, Malaysia: 84-89. https://doi.org/10.1109/ICSCEE50312.2021.9498045 **PMid:34022883 PMCid:PMC8140497**

Salomon D (2010). Elements of computer security. Springer Science and Business Media, Berlin, Germany. https://doi.org/10.1007/978-0-85729-006-9

Sengupta A, Mazumdar C, and Barik MS (2005). E-commerce security—A life cycle approach. Sadhana, 30(2-3): 119-140. https://doi.org/10.1007/BF02706241

Shahapurkar A (2021). A survey of data driven methodologies for mitigating cyber attack in online environment. Turkish Journal of Computer and Mathematics Education, 12(10): 3345-3353.

Szymanski DM and Hise RT (2000). E-satisfaction: An initial examination. Journal of Retailing, 76(3): 309-322. https://doi.org/10.1016/S0022-4359(00)00035-X

Wang JH, Liao YL, Tsai TM, and Hung G (2006). Technology-based financial frauds in Taiwan: Issues and approaches. In the IEEE International Conference on Systems, Man and Cybernetics, IEEE, Taipei, Taiwan, 2: 1120-1124. https://doi.org/10.1109/ICSMC.2006.384550

Zaaba ZF, Furnell S, and Dowland P (2011). End-user perception and usability of information security. In the Fifth International Symposium on Human Aspects of Information Security and Assurance, London, UK: 97-107.

Zawali B, Ikuesan RA, Kebande VR, and Furnell S (2021). Realising a push button modality for video-based forensics. Infrastructures, 6(4): 54. https://doi.org/10.3390/infrastructures6040054