E-Commerce Website System Security Improvement Strategy Using AHP and FAHP Methods

Farras Hafizh Zidane
Computer Science Faculty
UPN "VETERAN" Jawa Timur
Surabaya, Indonesia
21082010057@student.upnjatim.ac.id

Mochammad Yusuf Pratama
Computer Science Faculty
UPN "VETERAN" Jawa Timur
Surabaya, Indonesia
21082010063@student.upnjatim.ac.id

Dhiya' Ulhaq Ahmad Ramsi
Computer Science Faculty
UPN "VETERAN" Jawa Timur
Surabaya, Indonesia
21082010066@student.upnjatim.ac.id

Moh. Azzam Priyanto
Computer Science Faculty
UPN "VETERAN" Jawa Timur
Surabaya, Indonesia
21082010068@student.upnjatim.ac.id

Eristya Maya Safitri
Computer Science Faculty
UPN "VETERAN" Jawa Timur
Surabaya, Indonesia
maya.si@upnjatim.ac.id

***Abstract*—Security of e-commerce websites becomes one of the factors to develop e-commerce services. A secure e-commerce website can protect the personal information and transactional data of the user. However, in its everyday use, there is some problem that appears related to security. The purpose of this writing is to establish a security strategy for an e-commerce website based on the result of AHP and FAHP measuring. The research method used in this writing is Analytic Hierarchy Process (AHP) and Fuzzy Analytic Hierarchy Process (FAHP) to take a decision. AHP is used as a tool to analyze decision-making that comes close to a real-life situation and is used a lot in various fields, like evaluation, assessment, forecasting, and others. Meanwhile, fuzzy logic is used for a vague variable. The results of the research that has been done are that several e-commerce websites get low scores on system security measurements using the AHP and FAHP measurement methods. Therefore a strategy is needed to increase the security of the e-commerce website system so that users' personal information can be properly maintained.**

Keywords—E-Commerce; AHP; FAHP; Security

I. INTRODUCTION

According to Siregar, Irmawati explained that "e-commerce (e-commerce) is the process of buying, selling or exchanging products, services, and information through computer networks." E-commerce is part of electronic business, where the scope of electronic business is wider, not only trading but also cooperation with business partners, customer service, job offers, etc. E-commerce sites are currently experiencing significant development to their initial use. Customers can view products and services and can make purchases online. In building e-commerce, it should be noted that there are three factors that we must pay special attention to when we want to build an online store, namely: variety, visibility, and speed [1]. However, there is another important factor that needs attention, which is security. All e-commerce activities, from transactions to payments are carried out online, therefore data security is very important to protect consumer rights and build customer trust, so security issues are essential in e-commerce.

Through the results of research conducted by Eza Rahmanita et al in their journal article entitled "USE OF THE AHP AND FAHP METHODS IN MEASURING THE QUALITY OF E-COMMERCE WEBSITE SECURITY", this journal article attempts to discuss strategies to improve the quality of e-commerce system security that can be carried out by e-commerce vendors mentioned in the referenced journal article.

The advantages of research conducted on reference journal articles are that the security factor of electronic commerce consists of 27 security criteria and uses a rather complex method, namely a combination of AHP, dempster-shafer, and fuzzy TOPSIS methods, while the weakness is that it is difficult to find experts from e-commerce security sources [2].

II. METHODOLOGY

The methodology used in this research is the literature review method by examining data found from journals, articles, and other reference sources that are relevant to the research. Literature Review is a systematic, clear, and repeatable method

for identifying, evaluating, and synthesizing research articles and ideas from researchers and practitioners [3]. We use library sources from several journal sources through international and national journal websites such as Google Scholar, Science Direct, Elsevier, and Garba Digital Referrals (Garuda). By using this method, we can analyze the implementation of strategies to improve and maintain e-commerce website security so that it has good security. This analysis is supported by data from previous research, namely "Measuring the Quality of E-Commerce Website Security Using the AHP and FAHP Methods" by Rahmanita Eza, et al. From these data, further analysis can be carried out regarding implementation strategies to improve e-commerce website security.

III. Results and Discussion

A. Accuracy Analysis Tools

Before conducting an assessment of various e-commerce, it is better to analyze the accuracy of the tools first. To measure the accuracy of tools, the consistency ratio is used in the measurement. Consistency ratio scores are declared consistent when CR ≤ 0.1. The following is the accuracy of each tool used in this study:

1) Secure Web Test

Table I shows the result from the Secure Web Test tool. This tool gives a consistent result because it has a Consistency Ratio of less than 0.1.

TABLE I. Consistency Ratio Tools Secure Web Test

1	Eigen Value	5.187
2	Consistency Index	0.05
3	Consistency Ratio	0.04
4	Keputusan	Konsisten

2) Asafa Web

Table II shows the result from the Asafa Web tool. This tool gives a consistent result because it has a Consistency Ratio of less than 0.1.

TABLE II. Consistency Ratio Tools Asafa Web

1	Eigen Value	12.01053
2	Consistency Index	0.00096
3	Consistency Ratio	0.00061
4	Keputusan	Konsisten

3) Observatory by Mozilla

Table III shows the result from the Asafa Web tool. This tool gives a consistent result because it has a Consistency Ratio of less than 0.1.

TABLE III. Consistency Ratio Tools Observatory by Mozilla

1	Eigen Value	11.02193
2	Consistency Index	0.00219
3	Consistency Ratio	0.00148
4	Keputusan	Konsisten

Table I, II, and III shows the results from tools that are going to be used to measure an e-commerce security quality. Those three tools give a consistent result because the Consistency Ratio is less than 0.1.

B. Analysis of FAHP Method Results

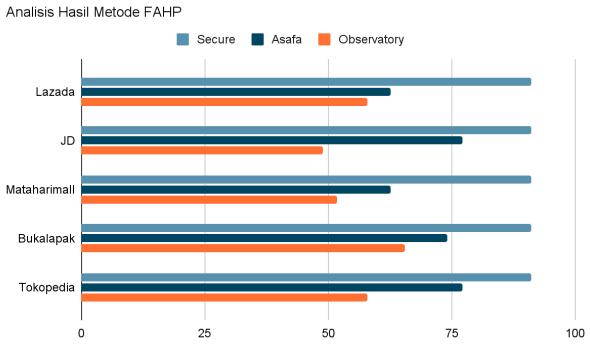

Fig. 1. Analysis of FAHP Method Results

C. FAHP Ranking Method

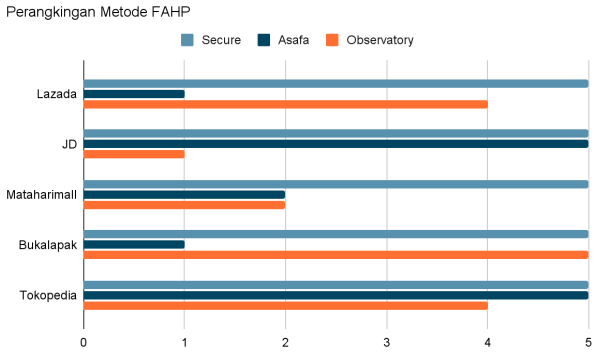

Fig. 2. FAHP Ranking Method

These are the the ranking model. Each rank has its own value. E-Commerce that rank first will get 5 points, rank 2 will get 4 points, rank 3 will get 3 points, rank 4 will get 2 points, and last rank will get 1 point. Based on the result above, Tokopedia topping up the chart in the first place, followed by Bukalapak and JD.ID in 2nd place, Lazada in 3rd place, and the last rank with the lowest score is MatahariMall.

Figure 2 shows the result from each e-commerce from the measurement. Tokopedia.com topping up the list, followed by Bukalapak.com and jd.id in the second place, Lazada in the fourth place, then MatahariMall.com in the last place.

D. Analysis of AHP Method Results

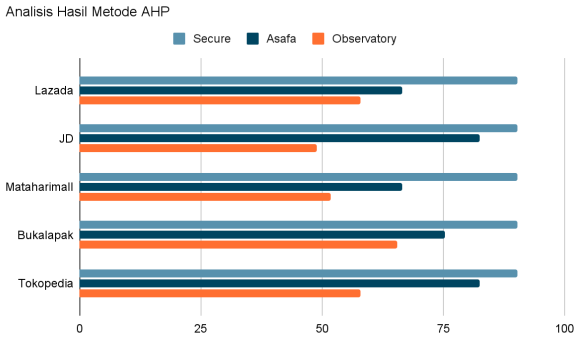

Fig. 3. Analysis of AHP Method Results

E. AHP Ranking Method

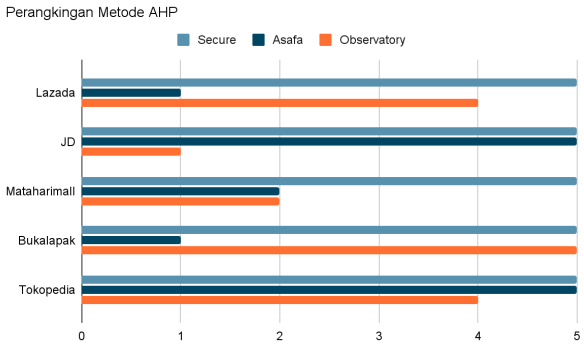

Fig. 4. AHP Ranking Method

These are the the ranking model. Each rank has its own value. E-Commerce that rank first will get 5 points, rank 2 will get 4 points, rank 3 will get 3 points, rank 4 will get 2 points, and last rank will get 1 point. Based on the result above, Tokopedia topping up the chart in the first place, followed by Bukalapak and JD.ID in 2nd place, Lazada in 3rd place, and the last rank with the lowest score is MatahariMall.

Figure 4 shows the result from each e-commerce from the measurement. Tokopedia.com topping up the list, followed by Bukalapak.com and jd.id in the second place, Lazada in the fourth place, then MatahariMall.com in the last place.

F. E-Commerce Security Improvement Strategy

Based on the results of the ranking of e-commerce security levels above, several websites get low scores, therefore a strategy is needed that can improve the quality of website security, but companies need to identify overall security requirements in their systems [4]. E-commerce vendors also need to know the categories and types of threats in the world of e-commerce, so that the planned security strategy or improvement uses the right technology, so that the security improvement plan is successful, the threat categories that lurk in e-commerce are as follows:

1) Fraud

Fraud is an attempt to trick customers into stealing important data that is useful for hackers or fraudsters, such as usernames, passwords, and credit card data. Phishing is one of the methods included in this category, the way the phishing method works is by sending messages in the form of fake e-commerce web links, then asking the customer to fill in and send important customer data, such as usernames, passwords, and so on.

2) Data theft through a network connection

Because almost all e-commerce activities are carried out online, all data exchange in e-commerce is carried out over the network, but threats lurk in this data exchange process because when transferring data, data will pass through many connections or networks, making it very possible for hackers to steal customer's personal data during this process.

3) Web server attack

This threat category is usually carried out by attacking the server by flooding the server with requests so that the server goes down and e-commerce services are disrupted. DOS and DDOS are examples of attack methods that fall into this category.

To prevent the above threats, companies need strategies that can improve the security of their websites, some of the strategies that can be carried out by e-commerce companies are as follows:

1) Secure Socket Layer (SSL)

SSL is an encryption protocol that is invoked via a web server using HTTPS and SSL as well as server and client intermediaries so that the network becomes more secure [5]. HTTPS or HTTP with SSL data can be protected before being sent to the destination. The difference is that before using SSL, data worked in such a way that data was sent directly in text format without additional protection. SSL also has several protocol components, such as handshake protocols, storage protocols, alerts, and certificates. In addition, the SSL protocol is a secure protocol from the dangers of sniffing [6].

2) Using the Best Firewall Application To Prevent DDOS attacks

Distributed Denial Of Service (DDOS) is a type of server attack by fulfilling server network traffic with computers that have been manipulated in large numbers to exceed the capacity of the server, this causes the system to be unable to serve requests from users or down [7]. This attack takes a long time to recover, if e-commerce is hit by a DDOS attack, various services on the website or application will be disrupted, and this attack can cause huge losses to e-commerce. Using a good Firewall Application can be a solution to prevent DDOS attacks, one of the best Application Firewalls to prevent this DDOS attack is AWS Shield. AWS Shield has always-on detection features and automatic inline mitigations that can reduce server down time, with these features e-commerce vendors can take early prevention against DDOS attacks.

3) Using Layered Security

As technology develops, e-commerce vendors continue to improve the security of their e-commerce websites, but on the other hand, hackers are also getting more creative in

developing their hacking methods, one of the hacking methods used is by attacking communication channels, this is done so to get the data, or messages in a communication channel to use for its own sake, one of the communication channel attack methods is Spoofing. Spoofing is a method of attacking communication channels, by posing as a trusted entity to get data that is useful for hackers, therefore it needs layered security in activities involving customer data, such as logins. one layered security method is to apply OTP (One Time Password). One Time Password (OTP) is a password that can only be used once and can only be valid for a few minutes, so hackers have little time to crack the code [8].

4) Backup Data Regularly

Backing up a website is something that must be done for online business owners from small to large scale. If an e-commerce website gets a cyber attack and the website loses a lot of data. Doing so can cause the website to go down making it inaccessible. Based on a survey of IT professionals in 2018, "80% OF SMALL AND MIDSIZE BUSINESSES (SMBS) HAVE EXPERIENCED DOWNTIME AT SOME POINT IN THE PAST, WITH COSTS RANGING FROM $82,200 TO $256,000 FOR A SINGLE EVENT." Website data backup is capable of copying all site data on the web and ensures that the e-commerce website is fully protected, and the data backed up must include products, themes, categories, customer data, orders, pages, posts, and more. 4 things must be considered in backing up data including regular data backups, comprehensive data backups, stored on a separate location or server from the website, easy to access, and restore when you need it [9].

5) Using Asymmetrci Key Encription in Exchanging Customer Data

Asymmetric Key Encryption is a more modern and complex type of encryption than Symmetric Key Encryption, this encryption is more complex because this type of encryption requires its own key in the encryption and decryption process, a public key for encryption and a private key for decryption [10]. The use of 2 keys in this type of encryption makes data sent using this encryption only accessible to certain users, so this encryption offers better data security than symmetric key encryption. This encryption can be applied to activities related to customer data in e-commerce, such as payments and orders. Some of the algorithms that can be used in this encryption are as follows:

a) RSA

b) Diffie-Hellman

c) DSA

IV. Conclusion

Based on the results of research that has been done, the use of the AHP and FAHP methods to measure security quality, some e-commerce doesn't have a very good system security quality. Therefore it is necessary to apply several strategies or solutions that can be used by e-commerce vendors to improve the security quality of e-commerce systems, including SSL, Using the Best Application Firewall, Using Layered Security, Backing up data regularly, and Using Asymmetric Key Encryption. This research is expected to provide new insights to improve the quality of e-commerce security.

References

[1] D. Irmawati, "Pemanfaatan e-commerce dalam dunia bisnis," *Jurnal Ilmiah Orasi Bisnis–ISSN,* vol. 2085, no. 1375, pp. 161-171, 2011.

[2] S. Ongkowijoyo, R. Gernowo, S. T. Rizal Isnanto and M. MT, "MODEL PENILAIAN KEAMANAN SITUS WEB E-COMMERCE MENGGUNAKAN KOMBINASI METODE AHP, DEMPSTER-SHAFER DAN FUZZY TOPSIS," *Doctoral dissertation, Diponegoro University,* 2013.

[3] T. Rahayu, S. Syafril, I. S. Wekke and R. Erlinda, "Teknik Menulis Review Literatur Dalam Sebuah Artikel Ilmiah," *INA-Rxiv,* 2019.

[4] H. Matbouli and Q. Gao, "An overview on web security threats and impact to e-commerce success," in *International Conference on Information Technology and e-Services*, Tunisia, 2012.

[5] M. S. Bhiogade, "Secure socket layer," in *Computer Science and Information Technology Education Conference*, 2002.

[6] H. Pranata, L. A. Abdillah and U. Ependi, "Analisis Keamanan Protokol Secure Socket Layer (SSL) Terhadap Proses Sniffing di Jaringan," *arXiv,* 2015.

[7] Microsoft, "What is a DDoS attack?," Microsoft, [Online]. Available: https://www.microsoft.com/id-id/security/business/security-101/what-is-a-ddos-attack. [Accessed 1 1 2023].

[8] K. I. Santoso, "Dua Faktor Pengamanan Login Web Menggunakan Otentikasi One Time Password Dengan Hash SHA," *Semantik,* vol. 1, p. 3, 2013.

[9] S. Rally, "Why Website Backups Can Save Your Business," Big Commerce, 2003. [Online]. Available: https://www.bigcommerce.com/blog/website-backups/. [Accessed 31 12 2022].

[10] A. Chaudhary, K. Ahmad and M. A. Rizvi, "E-commerce security through asymmetric key algorithm," in *Fourth International Conference on Communication Systems and Network Technologies*, Bhopal, 2014.