Article

Not peer-reviewed version

Digital Forensics for Vulnerability Personal Data on E-Commerce Platform (Case Study: Tokopedia Customer Data)

Wisnu Uriawan * , Alfian Musthofa , Andhika Eka Putra Sutrisno , Fadilah Inayat Ali

Posted Date: 25 December 2024

doi: 10.20944/preprints202412.2169.v1

Keywords: data leakage; e-commerce; Tokopedia; personal data protection; consumer trust; digital forensics; healthcare data security; qualitative analysis; Indonesia

Article

Digital Forensics for Vulnerability Personal Data on E-Commerce Platform (Case Study: Tokopedia Customer Data)

Wisnu Uriawan *, Andhika Eka Putra Sutrisno, Alfian Musthofa and Fadilah Inayat Ali

Informatics Department; UIN Sunan Gunung Djati Bandung Jawa Barat, Indonesia
* Correspondence: wisnu_u@uinsgd.ac.id

Abstract: In the context of rapid e-commerce growth in Indonesia, the Tokopedia data leak incident of May 2020 un- derscores the pressing need for robust personal data protection mechanisms. This research explores the legal and technical dimensions of the breach, assessing its impact on consumer trust and the overall integrity of e-commerce platforms. It highlights the vulnerabilities associated with increased internet usage and the corresponding rise in data security risks. Furthermore, the study examines the challenges and opportunities in securing sensitive data, particularly in sectors like healthcare, where pa- tient information is critical. By employing a qualitative approach to analyze consumer behavior in online purchases, particularly of electronic products, this research aims to propose effective security measures and best practices for e-commerce platforms to enhance user confidence and foster a safer digital commerce environment.

Keywords: data leakage; e-commerce; Tokopedia; personal data protection; consumer trust; digital forensics; healthcare data security; qualitative analysis; Indonesia

I. Introduction

In the digital age of today, information has become a highly valuable commodity, especially in the context of growing e- Commerce. However, with this growth, new challenges related to the security and privacy of users' personal data have also emerged. The case of user personal data leakage at Tokopedia, one of the largest e-commerce platforms in Indonesia, reflects the urgency of data protection in the era of communication globalization and free trade. The legal analysis of this case is important to understand the existing regulations and to find solutions to resolve related disputes [**?**]auzy2023legal.

In the ever-evolving digital era, personal data protection is becoming an increasingly pressing issue, especially on e- commerce platforms such as Tokopedia [1]. The user data leak case that occurred in May 2020 reflects the vulnerability faced by companies in safeguarding consumer information [2].

With the rise of internet users in Indonesia-where 64.8% of the population accessed the internet in 2018 (APJII)-online commerce is growing rapidly, along with data security risks [3]. Digital forensics plays an important role in analyzing these leaks, helping to understand and address the challenges that arise [4]. This research aims to explore the legal and technical aspects of the Tokopedia data breach, as well as its impact on consumer confidence and the integrity of the e-commerce system as a whole. In doing so, it invites us to reflect on the importance of data security in the spirit of globalization and digitalization [5].

In the context of Big Data and the Internet of Things (IoT), the healthcare sector also faces similar challenges, where patient data must be protected from potential leakage and misuse. The application of technologies such as blockchain can provide solutions, but also faces issues of interoperability and handling large volumes of data. This research aims to identify the challenges and opportunities in keeping patient data secure, and recommend best practices that can be implemented [6].

The rapid development of information and communication technology is driving changes in consumer behavior from in- store purchases to online purchases. Data from the Indonesian Internet Service Providers Association shows that the number of internet users in Indonesia continues to increase, creating huge potential for e-commerce. This research adopts a qualitative approach to better understand consumer behavior when purchasing products online at Tokopedia, especially in the category of electronic products such as mobile phones [7]. With many reports of data leaks on e-Commerce platforms, this issue has become increasingly relevant [8]. Recent news regarding Tokopedia's data leak highlights the importance of implementing stronger security measures to protect user information. The underlying argument of this research is that without proper protection, consumer trust in digital platforms will decline, which could negatively impact the growth of the e-commerce industry in Indonesia [9].

Therefore, this research not only aims to analyze the case of data leakage in Tokopedia, but also to develop recommendations that can help other e-Commerce platforms improve the security system of users' personal data, thus creating a safer and more efficient ecosystem in the world of digital commerce. The remainder of this paper is structured as follows. Section

I introduces the credit scoring and background. Section II related work. Section III are methods. Section IV result and discussion. Section V concludes this paper. The digital era has brought tremendous convenience in various aspects of life, one of which is through e-commerce platforms. With its ability to connect sellers and buyers globally, e-commerce has become a key driver of digital economic transformation. However, this progress also comes with increasing threats to personal data security. Customer data, which includes sensitive information such as name, address, phone number, and payment method, has become a prime target for malicious actors in cyberspace. Tokopedia, as one of the largest e-commerce platforms in Indonesia, has played a significant role in supporting the growth of the digital economy in the region. However, several data breach incidents involving the platform highlight the huge challenge of keeping customers' personal data safe. One such incident that has come to the public's attention is the alleged leak of Tokopedia's customer data, which not only hurt customers but also lowered trust in the security of e-Commerce platforms in general.

This research aims to investigate the vulnerability of per- sonal data on e-commerce platforms, with a case study on the Tokopedia incident. Through a digital forensic approach, this research will identify the factors that contributed to the data breach, analyze the impact on users and companies, and provide strategic recommendations to improve personal data security. In this study, a systematic methodological approach was used, starting from data collection, vulnerability analysis, to the development of recommendations. Cyber-security frameworks such as the NIST Cyber-security Framework and OWASP (Open Web Application Security Project) Top Ten were used to guide the analysis. In addition, this research also adopts the principle of privacy by design to encourage the integration of personal data protection into system development from an early stage. The results of this study are expected to contribute to improving understanding of the importance of personal data protection on e-commerce platforms, as well as provide strategic insights for platform managers to anticipate and address future security threats. With the increasing incidents of data breaches, this research is also relevant in encouraging wider discussions on data protection regulations in Indonesia.

II. Related Work

Related research on personal data protection and digital forensics on e-Commerce platforms shows that there are several challenges and opportunities to improve user data security. This section will review some of the research relevant to the Tokopedia data breach case study and provide insights into issues related to data protection in Indonesia.

In their research conducted a legal analysis of the user data leak case at Tokopedia. They found that although there are regulations governing the protection of personal data in Indonesia, such as Government Regulation No. 71/2019 on the Implementation of Electronic Systems and Transactions, the implementation is still weak and has not provided optimal protection for consumers [10].

The researchers employed purposive sampling to recruit participants who had experience using the platform, along with informants knowledgeable about the research topic. Data collection relied on interviews, observations of the Tokopedia website, and document analysis, with triangulation ensuring the validity of findings. The descriptive method with a qualitative approach aimed to understand the ”why” behind consumer behavior through narratives rather than numerical data. Data analysis was an iterative process, conducted concurrently with data collection and focusing on connecting interview responses, observations, and documents to draw conclusions grounded in consumer behavior theories [1].

The research on criminal threats in the bill on the protection of personal data employs a normative juridical research method. By using a statutory and conceptual approach, the study examines relevant laws and regulations, as well as literature and journals. The research materials were collected through document study and analyzed using descriptive analysis. This comprehensive approach provides a solid foundation for understanding the legal framework and potential criminal threats related to personal data protection [2].

The research analyzed the Indonesian Personal Data Protection Act No. 27 of 2022 by employing a multi-faceted approach. It compared Indonesian regulations with international standards from countries like Malaysia, Hong Kong, and the European Union to identify gaps and potential improvements. Additionally, it conducted a conceptual analysis to provide a theoretical framework for understanding personal data protection in the fintech industry. The study relied on both primary and secondary legal sources, including legislation, official documents, judicial rulings, and scholarly works. The qualitative juridical analysis involved legal interpretation, reasoning, and argumentation to draw conclusions and recommendations for strengthening personal data protection in Indonesia’s fintech sector [3].

Tokopedia, founded by William Tanuwijaya in 2009, has experienced significant growth and success due to substantial funding from various investors. Starting with initial investments from East Ventures and CyberAgent Ventures, Tokopedia has secured multiple rounds of funding, including a major investment of US$100 million from SoftBank and Sequoia Capital. This financial support has enabled Tokopedia to expand its operations and achieve remarkable sales figures, solidifying its position as a leading online shopping platform in Indonesia [4].

This research focuses on understanding the behavior of consumers who have made mobile phone purchase transactions on the Tokopedia e-commerce platform, especially in the Jabodetabek area. Through a quantitative approach, data was collected from a sample of users who met certain criteria using the probability sampling method. Data analysis using Partial Least Squares Structural Equation Modeling (PLS- SEM) aims to identify causal relationships between various variables relevant to consumer behavior in the context of e- commerce, especially in the mobile phone product category. Thus, this study contributes to the existing literature by pro- viding a deeper understanding of the factors that influence consumer purchasing decisions on e-commerce platforms such as Tokopedia [5].

In this study, they discuss the challenges and opportunities in improving the security and privacy of patient data in distributed systems. They emphasize the importance of using new technologies such as blockchain to improve security, but also note the constraints of interoperability and handling large amounts of data, which are similar to the challenges faced by e-commerce in protecting user data [6].

This study discusses the implementation of a distributed system using auto promote and web services to improve data security. This approach can be a model for developing a more integrated data security system that can reduce the risk of data leakage on e-commerce platforms such as Tokopedia [7].

In this study analyzed consumer protection against user data hacking on Tokopedia. They found that although Tokopedia has made some efforts to improve security after the incident, there are still weaknesses in data protection that need to be fixed immediately so as not to reduce consumer confidence in the platform [8].

In his research provides a contemporary view of data leakage cases in Indonesia. This research highlights several data leakage cases that have occurred in recent years and evaluates the extent to which existing regulations are able to prevent similar incidents. Sumirat suggests the need for improved regulation and stricter law enforcement to protect users' personal data [9].

in an effort to apprehend private data vulnerabilities and their implications on e-commerce structures, some of previous research have made full-size contributions in the fields of cybersecurity, digital forensics, and data protection. This phase evaluations several related works applicable to the Tokopedia case have a look at, both from a technical and coverage attitude.

1) *Digital forensics in Data Breach Investigation:* Virtual forensics has emerge as an vital approach in identifying and reading statistics breaches. according to analyze with the aid of Agarwal et al. (2011), the digital forensics procedure entails the tiers of virtual proof collection, analysis, and reporting to recognize how the assault came about. Forensic equipment consisting of FTK Imager and post-mortem were noted as key gear in safety incident investigations. This studies is relevant in providing a technical framework for this take a look at, specifically within the facts analysis method.

2) *Cybersecurity Framework for E-commerce:* Diverse frameworks had been proposed to improve protection on e- commerce platforms. one in every of them is the research by using Gupta et al. (2020), which makes use of the OWASP (Open Web Application Security Project) pinnacle Ten as a manual to become aware of the most commonplace web software vulnerabilities. another have a look at with the aid of Subashini and Kavitha (2011) mentioned the importance of implementing stop-to-quit encryption in ensuring customer data safety. these studies provide a strong basis in reading Tokopedia's vulnerabilities based totally on security satisfactory practices.

3) *Implications of Data Leaks on Consumer Confidence:* Studies by using Ponemon Institute (2019) suggests that statis- tics breach incidents have a large impact on consumer accept as true with in digital platforms. A have a look at with the aid of Malhotra et al. (2004) highlights that a loss of protection for personal facts can reduce consumer loyalty and create a terrible logo picture. those insights offer essential context in comparing the social and economic effect of Tokopedia's data breach incident.

4) *Data Protection and Privacy Regulations:* In conjunction with the growing risk of facts breaches, records protection guidelines along with the GDPR within the ecu Union and the PDP bill in Indonesia have gained substantial attention. studies by using Kuner et al. (2012) explains how the implementation of GDPR can help lessen the hazard of facts breaches by way of placing strict protection requirements. This have a look at is relevant to explore the gaps in nearby rules and the way they affect Tokopedia's management of private statistics.

5) *Security Incident at Tokopedia:* Numerous information reports and analysis propose that the Tokopedia facts leak involved tens of millions of patron records being traded at the black marketplace. research such as the one conducted via Kaspersky Lab (2020) show how e-commerce records may be a strategic target for chance actors because of the excessive fee of the information collected. This have a look at presents empirical context that supports the significance of research at the Tokopedia case.

with regards to those works, this studies fills the gap in the literature by using focusing on the application of digital forensics in the investigation of vulnerabilities on e-trade systems in Indonesia.

It additionally affords a sensible contribution inside the shape of pointers primarily based on a established framework that is applicable for the nearby context.

III. Methodology

This research uses a qualitative descriptive approach and focuses on the description and analysis of personal data vulnerabilities that occur on the Tokopedia e-commerce plat- form using digital forensic techniques. This approach aims to understand vulnerability patterns and methods that can be used to detect and prevent data leaks. Data collection was done through the following methods:

1) Literature Study

Literature have a look at on this research turned into

conducted to build a strong theoretical and conceptual foundation related to facts security, virtual forensics, and information leakage incidents on e-commerce structures. This method involves amassing references from various relevant literature resources, consisting of books, clinical publications, essays, Tokopedia reports related to information leakage, and statistics protection laws.

a) Records safety and privacy safety

The literature on information security affords important insights inup to date up to date practices for protecting up to date consumer records. Books including security Engineering: A guide updated building reliable allotted structures with the aid of Ross Anderson is one of the important references for knowledge the fundamental ideas of records protection. in addition, academic journals consisting of IEEE Transactions on records Forensics and security provide research on facts security methods and relevant technologies.

b) Digital Forensics within the Context of E-trade The look at of digital forensics is a key detail on this studies to apprehend how uncovered records can be analyzed and investigated. assets together with digital proof and computer Crime through Eoghan Casey offer a comprehensive manual to the techniques and gear utilized in forensic investigations. Articles within the journal digital investigation are also an vital reference for gaining knowledge of forensic techniques carried out to cyber-security incidents, specifically in the context of e-trade applications.

c) Records Leak Incidents in E-commerce

The literature on information breach incidents pro- vides an empirical perspective on the not unusual patterns that emerge in attacks on e-trade structures. Case studies which include the information leaks at goal (2013), eBay (2014), and Tokopedia (2020) offer historical context and frequently used attack strategies. The evaluation additionally covers the lengthy-time period impact on clients and corporation popularity. Articles in the magazine computer systems and security and industry reports through Kaspersky Lab and Symantec are key references in this region.

d) Information security law

To complement this have a look at, literature on information safety and privacy policies is vital, particularly given the Indonesian context of devel- oping a personal facts protection law (PDP law). References inclusive of the overall facts safety law (GDPR) inside the eu Union are key benchmarks in knowledge international information protection requirements. the article by using Kuner et al. in global records privacy law affords insights into how rules may be applied to lessen the danger of facts leakage.

e) Tokopedia information Leak file

primary assets which includes news reports and Tokopedia's reliable publications on the data leak incident fashioned an vital a part of the observe literature. Articles from trusted media which include BBC, Reuters, and technical reports compiled by way of cyber-security corporations offer insights into the chronology of the incident, the business enterprise's reaction, and assessment of the mitigation measures taken.

f) Extra Reference sources

in addition to clinical literature, this research also utilized white papers from cyber-security companies consisting of Cisco, Palo Alto Networks, and trend Micro to benefit insight into the present day protection risk trends. Discussions from cyber- security groups together with OWASP (Open Web Application Security Project) and professional forums have been additionally beneficial resources of information in expertise the practices and challenges confronted in defensive consumer facts in e-trade.

2) Case Study Analysis

This studies will deeply check out the Tokopedia client statistics leak case to apprehend the degrees of the leak, the kinds of information exposed, and the stairs taken by the agency in reaction to the incident. this example analysis is performed to explore the foundation reasons of the information leak and evaluate the effectiveness of the corporation's response in mitigating the impact of the incident on clients and platform operations.

The primary level of the analysis changed into to understand the chronology of the data leak incident, including how the assault changed into completed, when it occurred, and the parties concerned. This entails tracing public facts, cyber-security reports, as well as capacity attack patterns that lead to the exploitation of Tokopedia's structures. This research may also make use of virtual forensic techniques to evaluate the virtual footprint left at the back of via the attackers, which includes evaluation of pastime logs and assault vectors used.

The sort of records uncovered in this leak is a chief situation within the case examine. This studies will classify the uncovered records based totally on its level of sensitivity, which include non-public statistics (call, deal with, electronic mail, and contact variety) to more touchy data which includes transaction data and login credentials. This expertise is crucial to determine the dimensions and impact of the leak, each for the consumer and the corporation.

Further to analyzing the incident at Tokopedia, this studies will even evaluate it with different facts leak instances that occurred on comparable e-commerce systems, together with Lazada, Bukalapak, or international systems which includes eBay. This assessment will consist of the factors that precipitated the leak, the enterprise's response, as well as the mitigation measures taken. via this comparative evaluation, the studies objectives to become aware of commonplace styles in e-trade statistics leaks and examine nice practices that may be carried out to save you comparable incidents inside the destiny.

Some other important step is to assess Tokopedia's response to this incident. The studies will examine the organisation's conversation approach to the public, customers, and regulators after the incident opened up. This includes a review of technical measures which includes accelerated device protection, as well as non-technical techniques such as compensating affected customers.

The evaluation can even don't forget the criminal and regulatory implications of information breaches in Indonesia. The research will evaluate the volume to which these incidents observe or violate relevant facts protection laws, which include the personal statistics protection bill (RUU PDP). this is essential to apprehend how the criminal framework can function a driving force for improvements in facts control with the aid of e-trade systems.

With a comprehensive case have a look at approach, this research no longer best objectives to apprehend Tokopedia's facts leak incident in depth, however additionally to provide relevant strategic insights for the e-trade enterprise in dealing with records safety risks in the virtual technology. This evaluation is predicted to function a reference in organizing nice practices in data protection and incident reaction in the future.

3) Vulnerability Analysis

This studies will behavior an in-intensity analysis of the vulnerabilities that led to the private information leak at Tokopedia. This procedure entails a scientific technique to become aware of, recognize, and examine the factors that contributed to the incident. the usage of cyber-security ideas and threat evaluation, this research targets to find prone factors exploited by irresponsible events and recognize the quantity of the impact at the integrity and privateness of customer information.

Step one in vulnerability analysis is to identify vital belongings related to customer private information management, including facts storage structures, user authentication mechanisms, and encryption techniques. This studies will map Tokopedia's technical architecture to find capability gaps that could seem at numerous layers of security, both on the software, community and server sides.

More over, this research will compare the potential exploitation of these protection holes. This evaluation includes reviewing logs, device configurations, and protection policies implemented by using the platform.

techniques which include penetration trying out and assault simulation will also be used to nearly quantify the vulnerabilities and determine the level of threat involved.

The analysis will even encompass a comprehensive evaluation of the safety controls that Tokopedia has implemented, which include firewalls, intrusion detection systems, and get admission to management guidelines. consciousness could be given to gaps or weaknesses in the implementation of those controls that might facilitate a statistics breach. As a part of the hazard approach, this research will utilize a threat matrix to assess the likelihood of exploitation and its ability impact.

Further to the technical technique, this research also con- siders human factors as an essential element in vulnerability evaluation. internal corporation rules, worker protection cognizance levels, and incident response training and tactics could be analyzed to determine the extent to which human factors make a contribution to information leakage incidents.

The frameworks used in this studies include the NIST Cyber-security Framework and OWASP (Open Web Ap- plication Security Project) top Ten, that are designed to provide guidance in identifying and addressing security threats to net applications and their helping infrastructure. through the use of these frameworks, vulnerability evaluation may be connected to identified international standards, as a way to offer strategic steerage for relevant safety upgrades.

The outcomes of this evaluation will provide a deep understanding of the technical, organizational, and manner factors that contributed to the information leak at Tokopedia. This data will offer a solid basis for developing practical recommendations to prevent similar incidents inside the destiny and enhance the protection of customers' private data.

4) Vulnerability Indentification and Classification

In this stage, digital forensic techniques are applied to map the security hotspots that can cause personal data breaches on e-commerce platforms. This process begins with an in-depth understanding of the technical and operational infrastructure of the platform that is the object of research. Researchers used a standard framework-based approach such as the NIST Cyber-security Framework which divides security analysis into five main functions: Identify, Protect, Detect, Respond, and Recover. This framework allows researchers to systematically assess weaknesses in each aspect of platform security.

The first step is the collection of relevant digital artifacts from the system, including activity logs, configuration files, and network communication data. The use of digital forensic tools such as FTK Imager and Autopsy simplifies the process of collecting and managing digital evidence in a legally compliant manner. FTK Imager is used to create a forensic copy (bit-by-bit copy) of system data, ensuring that the original evidence remains intact and unaffected during the investigation. Meanwhile, Autopsy helps analyze various file types to detect anomalies, such as unusual activity or suspiciously modified files. Furthermore, Wireshark is used to display and examine community traffic information in element.

Researchers can identify suspicious communication styles, consisting of unauthorized get admission to at- tempts, data transfers to external servers, or warning signs of guy-in-the-middle assaults. This evaluation additionally consists of inspection of the communique protocols used, such as HTTP, HTTPS, and TLS, to ensure there are no weaknesses within the encryption or authentication process.As soon as the statistics was accrued, the vulnerability classification technique turned into finished. Vulnerabilities had been diagnosed primarily based on type, ability effect and level of exploitation. some of the maximum not unusual classes of vulnerability consist of:

a) Web Application Vulnerabilities: Such as SQL injection, cross-site scripting (XSS), and session hijacking.

b) System Configuration Errors: For example, inse- cure server settings or the use of outdated encryption certificates.

c) Weaknesses in the Authentication Process: Such as the use of weak passwords or the absence of multi- factor authentication (MFA).

d) Internal Access Exploitation: Includes unauthorized access by internal users or lack of data access restrictions.

e) Over-the-Network Attacks: Such as packet sniffing, denial-of-service (DoS) attacks, or port scanning activities.

These vulnerabilities were then mapped into chance classes primarily based on their threat stage and impact on customers and the e-trade platform. A hazard matrix changed into used to evaluate every vulnerability based totally on key dimensions: probability of exploitation and severity of impact.

Further, an in-intensity evaluation changed into per- formed to pick out the relationships among the vulnerabilities found. as an instance, whether or not a weak point within the authentication device might be an access factor for different attacks which includes unauthorized get admission to to patron information. The effects of this identity and classification provide a stable basis for designing greater powerful mitigation measures and security recommendations at a later degree.

This holistic approach ensures that any potential vulnerabilities can be accurately recognized and properly classified, permitting e-commerce structures to improve their security systems and better defend clients' personal information.

5) Validation and Assessment of Findings

The findings of this studies were established through a series of steps designed to make sure the reliability of the evaluation consequences and the relevance of the proposed guidelines. Validation was conducted by way of comparing the effects of this studies with applicable preceding studies, in addition to gaining additional insights from cyber-security experts who've revel in in coping with records breaches on e-trade systems. the steps taken in validating the findings consist of:

a) Comparison with preceding research The findings generated in this studies are as compared with the results of other studies which have studied statistics vulnerabilities on digital systems. as an example, if weaknesses are located in facts encryption on Tokopedia, these findings could be linked to studies that have shown that TLS-based totally encryption or modern algorithms consisting of AES are more powerful than older methods. This comparison provides an empirical foundation for assessing the accuracy of the analysis carried out.

b) Session with Cyber-security specialists This studies worried interviews or discussions with experts in the field of cyber-security to critically evaluate the findings. The experts furnished comments at the forensic techniques used, the validity of the assumptions, and the feasibility of the proposed recommendations. Their insights help perceive capability biases within the analysis and make certain the proposed answers are realistic and applicable.

c) Simulation Trial in a controlled environment some findings, particularly those associated with technical trying out, are proven through simulation in a managed environment. for example, mitigation strategies which include multi-thing authentication (MFA) or intrusion detection device (IDS) implementation have been tested to evaluate their effectiveness in preventing assaults on customer information. those simulation consequences are in comparison with consequences said in preceding studies to make sure consistency.

d) Comparative analysis with similar Incidents To increase the validity of the findings, this research additionally examined safety incidents that befell on different e-commerce platforms at domestic and abroad. with the aid of comparing the attack pat- terns, exploitation methods, and platform responses to these incidents, researchers can reinforce the analysis of vulnerabilities recognized within the Tokopedia case look at.

e) Validation by means of Peer evaluate As part of the scientific validation process, the studies findings have been additionally submitted for assessment via friends or other academics with information in cyber-security. Peer evaluate enables pick out areas that require strengthening or revision, accordingly ensuring the excellent and credibility of the studies consequences.

f) Trying out Relevance to local rules in addition to technical validation, the relevance of the findings to relevant statistics protection rules and guidelines in Indonesia changed into also tested. This includes analyzing the conformity of the guidelines with the non-public information safety regulation (PDP law) as well as safety requirements set by means of regulatory bodies. This validation ensures that the proposed solution is not best effective but additionally compliant with the applicable legal framework.

Through this thorough validation approach, the studies findings no longer handiest replicate correct analysis effects however additionally provide applicable and nearly relevant contributions. This validation strengthens the trustworthiness of the resulting suggestions, making them a reliable guide to improving non-public data safety on e-trade structures along with Tokopedia.

A. *Framework Analysis*

This research uses a framework analysis approach to evaluate the effectiveness of security technologies implemented in e-commerce systems, specifically on Tokopedia. The goal is to identify and evaluate solutions that can be used to protect users' personal data from the threat of vulnerabilities and cyber-attacks. The following is the framework analysis used:

1) Forensic digital security framework

The forensic digital security framework serves as a established and methodical approach to investigating and mitigating safety incidents in digital structures. it is designed to address the complexity of contemporary cyber-attacks via uncovering attack vectors, figuring out vulnerabilities, and imparting actionable insights to beautify device protection. The framework involves several key stages: information collection, evaluation, and documentation of digital evidence. each section plays a crucial position in the ordinary investigative technique and guarantees the integrity and reliability of findings.

a) Data Collection: The first section includes the systematic acquisition of records from doubtlessly compromised structures. This consists of amassing logs, memory dumps, community traffic, and storage device records. using enterprise-preferred gear, consisting of FTK Imager, EnCase, and autopsy, is vital to ensure that the facts is gathered without changing its integrity. proper coping with and chain of custody protocols are vital to retaining the admissibility of proof in criminal or regulatory lawsuits. inside the context of e-commerce systems like Tokopedia, information series specializes in transaction logs, person get admission to information, and capability strains of unauthorized access.

b) Records: Renovation and Integrity guarantee once information is amassed, it ought to be preserved in its authentic nation to make certain the validity of next analysis. techniques which include hashing and write-blocking are hired to prevent accidental or intentional modification. maintaining a secure repository for proof garage is also vital to shield in opposition to tampering or statistics breaches during the research system.

c) Analysis: The middle of the forensic framework lies within the analysis section, wherein investigators scrutinize the accrued data to discover anomalies, attack patterns, and ability weaknesses within the device. superior techniques, together with opposite engineering, timeline reconstruction, and malware evaluation, are utilized to piece collectively the collection of events leading to the incident. equipment like Wireshark and Splunk useful resource in reading network hobby, even as reminiscence analysis gear together with Volatility are used to discover in-reminiscence threats. For an e-trade platform, this segment may involve reading encrypted communication channels, database get admission to logs, and API usage styles to hint the source of the attack.

d) Assault Direction Reconstruction: An crucial part of the evaluation process is the reconstruction of the attack route. This entails identifying how attackers gained preliminary get entry to, their lateral movements in the machine, and the strategies used to extract or manipulate records. expertise the assault path no longer only sheds light at the vulnerabilities exploited however also provides valuable insights into the tactics, techniques, and techniques (TTPs) hired via danger actors.

e) Susceptible Point Identity: Once the assault path is understood, the framework shifts cognizance to identifying vulnerable factors in the system that facilitated the breach. those can also consist of misconfigured servers, outdated software program, or inadequate access controls. Pinpointing those vulnerabilities permits the agency to prioritize re- mediation efforts and make stronger its safety posture.

f) Documentation of Digital Proof: Complete documentation is critical throughout the investigation to file findings, methodologies, and conclusions. This consists of generating unique incident reports, compiling timelines of the attack, and retaining evidence in codecs acceptable for criminal court cases. right documentation ensures that the investigation's outcomes are transparent, reproducible, and defensible if challenged in a court of regulation or at some stage in regulatory scrutiny.

g) Publish-Incident Evaluation and Tips The forensic virtual safety framework concludes with a post-

incident evaluate. This section assesses the effectiveness of the response and identifies classes learned to enhance future incident dealing with. suggestions are developed based on the research findings, specializing in mitigating identified vulnerabilities and improving gadget defenses. these may also encompass implementing superior authentication methods, deploying intrusion detection systems (IDS), and adopting a zero-believe structure.

By systematically applying this framework, organizations can effectively investigate security incidents, uncover critical weaknesses, and build resilience against future threats. For e-commerce platforms like Tokopedia, this framework provides a robust foundation for safeguarding customer data and maintaining trust in the platform's security.

doi:10.20944/preprints202412.2169.v1

2) Main Steps The evidence collection method is a vital first step in virtual forensic investigations, particularly to recognize the resources and patterns of attacks on customers' private records on e-commerce platforms. This degree includes collecting various applicable digital artifacts, inclusive of device logs, digital traces, and different evidence that may be used to research the incident. With a scientific technique, this stage is designed to ensure that the proof accumulated is legitimate, true, and according with the world over identified forensic methodologies. Gadget Log series machine logs are one of the primary sources in security incident investigations. This records includes recorded activity on servers, programs, and community gadgets. a number of the styles of logs accumulated include:

a) Access Log: To track who accessed the system, when, and from which location.

b) Error Logs: To identify system or application failures that may be exploited by attackers.

c) Security Log: To detect unauthorized attempts, such as failed logins or changes in access rights.

System logs are collected using automated tools such as Splunk or ELK Stack, which allow researchers to efficiently manage large amounts of data.

Digital Tracers, digital footprints encompass activities left by users and applications, both directly and in- directly. These artifacts can include browser cache, cookies, file metadata, or activity logs on the application server. Digital footprint analysis helps understand specific actions taken before an incident occurs, such as executing suspicious commands or unauthorized API usage.

The gathering of virtual footprints is completed the usage of forensic software program together with au- topsy or FTK Imager, that is designed to deal with evidence with out compromising the integrity of the authentic statistics. Besides logs and digital footprints, other relevant evidence may include:

a) Machine snapshot: A recording of the device's nation at a selected time, useful for evaluating modifications over a positive duration.

b) Configuration document: to check for unauthorized changes to gadget parameters.

c) Memory sell off: To achieve direct facts from memory that may contain session information, credentials, or traces of active assaults.

d) Network conversation: statistics from network tracking gear such as Wireshark can be used to come across suspicious traffic, consisting of information being sent to unknown domains or servers.

Upkeep of evidence, at some stage in the collection method, it's far critical to make certain that the evidence isn't changed or deleted. each step must be properly-documented, along with the time of series, the equipment used, and the garage vicinity of the proof. using write-blockers when gathering proof from storage gadgets and statistics hashing to confirm integrity are trendy practices in digital forensics.

Systematic series technique, the evidence collection method is performed in accordance with worldwide standards consisting of ISO/IEC 27037 to ensure the validity and admissibility of proof in court, if necessary. All accumulated artifacts are labeled, encrypted if important, and saved in a cozy environment.

Initial proof analysis, throughout the gathering phase, initial evaluation is carried out to identify patterns or indications of an assault. as an instance, searching for particular keywords, anomalies in access logs, or repeated login tries from suspicious IP addresses. those preliminary findings assist construct an preliminary speculation that can be tested in a detailed analysis.

Through a structured and comprehensive evidence collection process, this step ensures that all relevant information is available for further analysis. The collected evidence not only helps in understanding the incident but also provides a strong basis for making improvement recommendations to prevent similar occurrences in the future.

3) Security Technology Evaluated

a) Blockchain: Blockchain is a revolutionary era that enables the advent of comfy, transparent, and im- mutable facts of transactions thru its decentralized ledger system. inside the context of e-trade, this generation gives transformative solutions to cope with essential demanding situations, specially in safeguarding sensitive consumer facts and making sure believe among stakeholders. Protecting Sensitive User Data, blockchain employs advanced cryptographic techniques to comfy information. each transaction or statistics entry is encrypted and connected to the preceding block, developing

a chain of information that is extremely difficult to alter or tamper with. For e-trade platforms, this indicates touchy person records, which includes private statistics and fee info, may be stored in a fantastically secure way. not like conventional databases which can be prone to centralized breaches, blockchain's decentralized nature gets rid of a single factor of failure, extensively reducing the hazard of cyber-attacks. Furthermore, blockchain enables pseudonymization of consumer identities, making sure that although unauthorized get entry to takes place, private statistics remains unintelligible. that is particularly useful for systems coping with huge volumes of sensitive statistics, as it aligns with contemporary information protection regulations like the overall records safety regulation (GDPR). Ensuring Transparency and Trust, Transparency is a core feature of blockchain generation. In e-commerce, blockchain may be used to report every transaction and interplay between buyers, dealers, and intermediaries. This creates an auditable and verifiable path of sports that fosters believe amongst all parties worried. Enhancing statistics Integrity, Blockchain ensures records integrity thru its immutable nature. once information is recorded at the blockchain, it cannot be changed with out consensus from the whole network. that is in particular valuable for pre- venting fraud, as it guarantees that information of transactions, evaluations, and scores continue to be authentic. for instance, faux critiques or altered order histories—not unusual demanding situations in e-trade—can be eliminated through blockchain's tamper-proof statistics.

b) Encryption Techniques: This method involves encrypting sensitive data using algorithms such as AES and RSA to prevent unauthorized access.

c) Access Control Mechanism: Involves strict policies to ensure only authorized users can access sensitive data. Examples are two-factor authentication (2FA) and role-based access rights management (RBAC).

B. *Recomendation Development*

Implement stronger encryption to protect user data, both in transit and at rest. Algorithms such as AES-256 can be used to ensure that sensitive data, such as payment information and personal details, are protected from unauthorized access and utilizes blockchain technology to create an immutable system of record for important transactions and activities. Blockchain can help track and verify any changes that occur to user data.

IV. Result and Discussion

A. *Result*

Tokopedia, a very popular online shopping site in Indonesia, has helped many people to buy the things they need easily. However, in 2020, there was a bad incident where the personal data of millions of Tokopedia users was leaked to the inter- net. This personal data such as names, email addresses, and passwords used to log into Tokopedia accounts. This incident made many people worried because their personal data could be misused by irresponsible people. This research aims to find out how Tokopedia protects its users' data after the incident and whether there is a better way to keep the data safe.

1) How the Data Leak Happened?

Tokopedia certainly did not expect this to happen, where initially the security system in Tokopedia itself implemented several systems. But apparently, there are still gaps that can be exploited by cyber-criminals. Some of the security systems that Tokopedia may have used at that time include. *Encryption* User data is usually encrypted to protect its confidentiality. However, weak encryption or errors in implementation can leave data vulnerable. *Firewall* Firewalls serve as the first defense to prevent unauthorized access to the system. However, a poorly configured firewall or a gap in the firewall can be breached. *Intrusion Detection System* These systems are designed to detect suspicious activity on the network. However, if the system is not sophisticated enough or not configured properly, attacks can escape detection. and *Two-Factor Authentication* Some services may already use two-factor authentication to add a layer of security. However, if the implementation is inconsistent or users do not enable it, this protection becomes less effective. To improve the security of personal data on e-commerce platforms such as Tokopedia, here are some recommendations for security systems that can be applied in the context of digital forensics and data protection: *Strong Data Encryption*, Implement strong encryption (such as AES-256) to protect users' personal data, both in transit and in storage. Also, ensure that all communications between servers or between software and servers use secure protocols such as TLS.

2) What are the possibilities?

Some of the following factors may be the cause of Tokopedia data leaks including:

a) System Weaknesses, the programming code of any application, including Tokopedia, may have vulnerabilities that could be exploited by malicious actors. These weaknesses can stem from various factors such as inadequate input validation, outdated libraries, or improper error handling.

- *Insufficient Input Validation*, Improper validation of user input could allow attackers to execute injection attacks, such as SQL injection or cross- site scripting (XSS). For instance, attackers could exploit poorly validated user inputs to access, alter, or extract sensitive data from the. application's database.
- *Insecure Authentication Mechanisms*, Weak- nesses in login systems, such as the use of predictable password reset tokens or inadequate encryption for sensitive data, can make it easier for hackers to gain unauthorized access to user accounts. This could lead to data breaches affecting millions of users.
- *Outdated or Vulnerable Dependencies*, Modern applications often rely on third-party libraries and frameworks. If these dependencies are not updated regularly, they might contain known vulnerabilities that attackers can exploit. In the case of Tokopedia, outdated libraries may serve as entry points for attacks.
- *Improper Error Handling*, Applications that pro- vide detailed error messages could inadvertently reveal sensitive information about the system's architecture or database structure. Such information is valuable to hackers when planning their attacks.
- *Lack of Robust Encryption*, Weak or misconfigured encryption algorithms used for storing sensitive user data, such as passwords or payment information, increase the risk of exposing this data in the event of a breach.

These system vulnerabilities can lead to severe consequences, including the unauthorized access, theft, or alteration of personal data. In the case of the Tokopedia data breach, such weaknesses might have allowed attackers to obtain customer information, putting millions of users at risk. The exposure of personal data not only affects individual users but also tarnishes the platform's reputation, leading to loss of customer trust and potential legal actions.

b) Phishing Attacks

Phishing is one of the most common and effective methods used by attackers to steal sensitive user information, such as login credentials, on platforms like Tokopedia. In this type of attack, users are tricked into believing they are interacting with a legitimate entity, leading them to provide personal data willingly. Common Methods of Phishing At- tacks:

- *Fake login pages*,Attackers create fake Tokopedia login pages that closely resemble the authentic site. Unsuspecting users may be directed to these pages via phishing emails, fake advertisements, or malicious links. Once users enter their credentials, the attackers capture the information for unauthorized access.
- *Phishing Emails or Messages*, Cyber-criminals send emails or messages pretending to be from Tokopedia, claiming account issues, security up- dates, or special offers. These communications often include a link to a fraudulent page or an attachment containing malware.
- *Social Media Scams*, Attackers might create fake Tokopedia support accounts or promotional pages on social media platforms, tricking users into sharing their login details or personal information through private messages or fake forms.
- *Malicious Ads and Pop-ups*, Users might encounter pop-ups or advertisements claiming urgent action is needed for their Tokopedia ac- count. Clicking on these links redirects them to phishing sites designed to steal their information. Why Users Fall Victim to Phishing

Several factors contribute to the success of phishing attacks: Users may not recognize the signs of phishing, such as slightly altered domain names or generic language in emails, Tokopedia's large user base and reputation may lead users to lower their guard when interacting with communications that appear to be from the platform, Attackers exploit emotions like fear, urgency, or excitement to prompt users into acting without thinking critically. Mitigation Strategies To combat phishing, both users and Tokopedia must take proactive steps: Tokopedia can provide regular awareness campaigns to help users identify phishing attempts. Include tips like verifying URLs, avoiding clicking on unknown links, and recognizing official communication styles.

c) Brute Force Attack

Hackers try various password combinations to guess the user's password. Brute force attacks are a method used by hackers to gain unauthorized access to user accounts by systematically trying various combinations of passwords. These attacks can target e-commerce platforms like Tokopedia, exploiting weak or reused passwords to compromise user accounts. How Brute Force Attacks Work:

- *Credential Stuffing*, Hackers use previously leaked username-password pairs from other plat- forms to test against Tokopedia accounts, exploiting the common practice of password reuse.
- *Dictionary Attacks*, A list of commonly used passwords or password patterns (e.g., "123456", "password", or "qwerty") is tested systematically until a match is found.
- *Exhaustive Search*, In a more intensive approach, every possible combination of characters is tested. This method is more time-consuming but can be successful if the password is short or lacks complexity. Brute force attacks are a persistent threat to e-commerce platforms like Tokopedia, but a combination of user education, strong authentication measures, and advanced security protocols can significantly reduce the risk. By staying vigilant and proactive, Tokopedia can safeguard its users' accounts and build a more secure platform. Mitigation Strategies:

Require users to create strong passwords with a mix of uppercase, lowercase, numbers, and special characters.

d) Steps Taken by Tokopedia

In 2020, Tokopedia has taken various measures to improve their security system and restore user confidence. Although the full details of the measures taken may not be publicly available, here are the steps the company is taking. *Conducting in-depth investigations, cooperating with the government and independent agencies, and providing transparent information to the public*, are in line with the principles of Benoit's image restoration theory. *Strategi Corrective Action* Tokopedia has proven effective in restoring the company's image. By admitting mistakes, taking corrective action, and committing to prevent similar incidents in the future, Tokopedia has successfully demonstrated responsibility and concern for users. Overall, Tokopedia's efforts in overcoming this crisis can be considered a good example of crisis management in the digital era. The company managed to restore public trust through effective communication, concrete actions, and a commitment to user data security.

From the results of data collection and initial analysis, several important findings can be concluded. Vulnerability Identification: Through an initial security audit, it was discovered that one of the loopholes that could potentially expose users' personal data was weak authentication and lack of end-to-end encryption on certain transactions.

Types of Exposed Data The leaked personal data included sensitive information such as full names, email addresses, phone numbers, and, in some cases, credit card details. This data could potentially be misused for fraud or identity theft.

The analysis indicated that most of the exposed data came from user accounts that had not updated their privacy and security settings regularly.

B. *Discussion*

The research successfully provided significant information on data leakage incidents in 2020, including a detailed analysis of the causes of the incidents, the company's countermeasures, and strategic recommendations to improve data security in the future. One of the key achievements of this investigation was the identification of security gaps that contributed to the data leak, such as weak encryption, a suboptimal firewall con- figuration, and inconsistent authentication implementation. In addition, the study also evaluated Tokopedia's response to the incident, including the company's efforts to improve security systems, cooperate with authorities, and provide transparent communication to users. These steps demonstrate Tokopedia's commitment to improving its systems and restoring public trust.

However, this research is not free from a number of limitations. One of the main obstacles is the limited access to Tokopedia's internal data, which limits in-depth analysis of the security system implemented by the company. Most of the data used is sourced from public reports and secondary documentation, making it difficult to evaluate in detail the effectiveness of the technical measures that have been taken. In addition, the research focus is limited to one platform, Tokopedia, so the findings may not be fully applicable to other e-commerce platforms with different security infrastructures. In terms of methodology, the approach used is still descriptive and evaluative without any simulation of security attacks or direct experiments to test the effectiveness of the recommended system.

Despite these limitations, this research has a number of important implications. Academically, it adds insights to the data security literature, especially in the Indonesian e- commerce sector, and opens up opportunities for further exploration of cutting-edge technologies such as blockchain or artificial intelligence (AI) in protecting user data. Practically, the recommendations of this research can guide e-commerce industry players to improve their security strategies, such as implementing stronger encryption, mandatory multi-factor authentication, and regular security audits. This research also emphasizes the importance of user education to increase their awareness of data security risks, such as the importance of using strong passwords and enabling two-factor authentication. As a suggestion for future research, collaboration with e- commerce companies to gain access to more comprehensive internal data can be an important step to produce more in- depth analysis and solutions. In addition, future research can adopt experimental approaches, such as simulating cyber- attacks, to test the effectiveness of security systems directly. A multidisciplinary approach involving technological, legal and social perspectives is also needed to produce a more holistic and comprehensive data protection strategy. Overall, this research highlights the importance of data security in building user trust in the digital era. The Tokopedia data leak case serves as a reminder of the urgent need for e-commerce platforms to continuously update and strengthen their security systems. By recognizing its achievements and limitations, this research provides a strong foundation for the development of more effective data security solutions in the future, both for Tokopedia and other e-commerce platforms.

V. Conclusion

In this research, we examine the vulnerability of personal data on e-commerce platforms with a focus on the Tokopedia data leak case that occurred in 2020. The incident highlighted various weaknesses in the data security system on e-commerce platforms in Indonesia, which had a significant impact on user trust. Using a qualitative and case study approach, this research provides deep insights into the importance of data protection in maintaining system integrity and user trust.

The analysis shows that data leakage incidents in Tokopedia are mainly caused by weaknesses in user authentication, lack of encryption on certain data, and suboptimal data management. These security loopholes allow unauthorized third parties to access users' personal data, such as names, email addresses, phone numbers, and even credit card information. The impact of these leaks is not only felt by the users whose data is exposed, but also damages the company's image, which can have a long-term impact on the level of consumer confidence in the services offered by the platform.

The study also found that regulations related to personal data protection in Indonesia still need to be strengthened and strictly enforced. Currently, existing regulations are not strong enough to address large-scale data leakage incidents. As such, the Tokopedia data leak demonstrates the need for more comprehensive regulations and greater efforts on the part of the government to protect users' personal data in the digital age.

This research suggests several mitigation measures that e- commerce platforms can take to prevent similar incidents. These include the implementation of multi-factor authentication (MFA), the use of end-to-end encryption for all stored and transmitted data, and regular security audits to identify and close security gaps. In addition, it is important for companies to socialize and educate users on the importance of keeping their personal accounts secure, such as using strong passwords that are not easily guessed.

The implications of these findings are particularly relevant in the context of e-commerce, which is experiencing unprecedented growth in Indonesia and becoming an integral part of the country's economy. As the volume of online transactions increases, the stakes for ensuring robust data security rise significantly. E-commerce platforms bear a profound responsibility to implement comprehensive measures to safeguard user data, as user trust is not only a critical factor for the sustainability of their services but also a cornerstone of the broader digital ecosystem. This includes adopting advanced cyber-security technologies, regular security audits, and trans- parent data handling policies to reassure users and maintain their loyalty.

In addition, the role of the government and policymakers is indispensable. Stricter regulations that mandate data protection standards, coupled with effective law enforcement mechanisms, are essential to addressing the complex challenges of data security. The establishment of dedicated institutions or task forces to oversee and enforce these measures could also enhance accountability and provide swift responses to data breaches. Public-private partnerships can play a pivotal role in fostering collaboration between regulators and industry players, ensuring a balanced approach that promotes innovation while prioritizing user safety. Furthermore, raising public awareness about data security and educating users on safe online practices are equally important in building a resilient e-commerce environment. Together, these efforts can create a secure, trustworthy, and sustainable digital commerce ecosystem that benefits all stakeholders.

In the future, technological developments, such as artificial intelligence and Big Data analysis, can serve as powerful tools in detecting and preventing data security threats. These technologies have the potential to enhance the efficiency and accuracy of identifying vulnerabilities, predicting potential breaches, and responding proactively to mitigate risks. How- ever, their implementation must be approached with caution, ensuring adherence to the precautionary principle and strict compliance with existing regulations, such as data protection laws and industry standards. Furthermore, the ethical use of these technologies must be prioritized to avoid misuse and ensure that user data remains confidential, secure, and used responsibly. Collaboration between technology developers, regulators, and businesses will be crucial in fostering trust, transparency, and accountability in utilizing these advanced tools. Ultimately, the integration of AI and Big Data should aim to create a robust and sustainable cyber-security framework that balances innovation with the safeguarding of individual rights and privacy.

Overall, this research concludes that data leakage on e- commerce platforms such as Tokopedia is not just a technical problem, but also reflects broader social, legal, and ethical challenges that require collaboration from all stakeholders, including platform operators, government regulators, cyber- security experts, and users themselves. The growing reliance on digital platforms for commercial transactions amplifies the urgency of addressing these challenges comprehensively. Success in mitigating data leakage will not only enhance user trust and security but also strengthen the resilience of the digital economy in Indonesia and globally. Building a secure and reliable digital commerce environment is essential for fostering innovation, protecting consumer rights, and promoting sustainable economic growth in an increasingly interconnected world.

Acknowledgment: The author's wishes to acknowledge the Informatics Department UIN Sunan Gunung Djati Bandung, which partially supports this research work.

References

1. E. Suwasono, "Consumer behavior in purchasing products online at the tokopedia marketplace," in *Prosiding Seminar*, 2020, pp. 95–101.
2. H. D. Oktaviani and M. R. Arafat, "Legal policy of the personal data protection bill in indonesia," *Megafury Apriandhini, SH, MH Chair of 4th OSC*, p. 75, 2022.
3. A. Rohendi and D. B. Kharisma, "Personal data protection in fintech: A case study from indonesia," *Journal of Infrastructure, Policy and Development*, vol. 8, no. 7, p. 4158, 2024.
4. S. Sumartono, R. D. A. Navalino, and W. A. H. Rafsanjani, "Personal data protection regulations to support investment in indonesia," *Open Access Indonesia Journal of Social Sciences*, vol. 4, no. 2, pp. 243–252, 2021.
5. P. M. Agustini et al., "Pengaruh mobile app attractiveness, functionality, security dan consumer fulfillment terhadap e-loyalty dengan e- satisfaction sebagai intervening pada e-commerce tokopedia," *MES Management Journal*, vol. 3, no. 2, pp. 537–553, 2024.
6. W. Uriawan, S. Adriansyah, S. J. Maulidiyah, S. Julianto, and W. S. Jamil, "Challenges and opportunities: improve patient data security and privacy in distributed systems," 2024.
7. W. Uriawa, S. Nurrobianti, T. M. Saif, R. I. H. Widodo, and Y. R. Asgari, "Implementing distributed system using auto promote and web services," 2024.
8. I. T. Almeyda and E. Prasetyawati, "Consumer protection for the hacking of personal data of tokopedia marketplace users," *Journal Evidence Of Law*, vol. 3, no. 2, pp. 206–219, 2024.
9. J. R. Sumirat, "Data breach in indonesia: A contemporary view," *Innovative: Journal Of Social Science Research*, vol. 3, no. 6, pp. 7768– 7777, 2023.
10. E. Fauzy and A. Hafizhah, "Legal analysis of user personal data leak cases at tokopedia," *AQUACOASTMARINE: Journal of Aquatic and Fisheries Sciences*, vol. 2, no. 1, pp. 41–52, 2023.

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.