A Systematic Review of Threats in Data Sharing

[1]Prathibha Prakash, [2]Mr.Akhil Sekharan

[1]PG Scholar, [2]Asst.Professor
[1&2]Department of MCA, St. Joseph's College of Engineering and Technology Palai, Kottayam, India

Abstract: With the development of technology and the internet, data sharing has become more widespread, but it also comes with a number of risks. First of all, unlawful access to private data can result in data breaches, which can cause a lossof secrecy and privacy. This can be particularly troublesome in fields where the dissemination of private data, like financialor medical records, is widespread. Second, the loss or theft of private or confidential information is another consequence ofdata sharing. This can happen when data is sent to unapproved third-party organisations, when it is kept on unsecured systems, or when it is stored in the cloud. Thirdly, data sharing can lead to the misuse of personal data for illegal activities like fraud or identity theft.

Keywords: Data, Privacy, Sharing

I. INTRODUCTION

Data sharing has become an essential aspect of the modern world, enabling the efficient exchange of information and promoting innovation. However, it also poses several threats to the privacy and security of individuals and organizations. One of the primary threats is the risk of data breaches, which can lead to the exposure of sensitive information to unauthorized parties. Such breaches can result in severe consequences, including identity theft, financial loss, and reputational damage. Another threat is the risk of data misuse, where the shared data is used for purposes other than what it was intended for, such as targeted advertising or surveillance. Additionally, there is the possibility of data theft, where hackers gain unauthorized access to shared data, putting the privacy and security of individuals and organizations at risk. Moreover, data sharing can lead to the creation of data silos, where large organizations and powerful individuals can accumulate a vast amount of data, giving them an unfair advantage over their compe titors. Finally, the lack of transparency and accountability in data sharing practices can also lead to ethical concerns, including the possibility of discrimination and unfair treatment. To mitigate these threats, it is necessary to adopt strict data privacy and security measures, including the use of encryption, access controls, and secure data sharing agreements. Additionally, it is essential to promote transparency and accountability in data sharing practices to ensure that data is used ethically and fairly. By addressing these threats, we can ensure that the benefits of data sharing can be realized while minimizing the risks.

II. THREATS IN DATA SHARING

The first and most significant risk of data sharing is the loss of privacy. Sharing sensitive personal information such as social security numbers, health records, or financial data can lead to identity theft, fraud, and other forms of cybercrime. Additionally, sharing data with third-party service providers can lead to data breaches if adequate security measures are not in place. For instance, in 2019, Capital One bank suffered a data breach in which over 100 million customers' personal information was compromised due to inadequate security measures. Another potential threat is the misuse of data, in which companies may use shared data to target individuals with ads or to manipulate their behavior. Facebook's Cambridge Analytica scandal is an example of this threat, in which the company obtained data from millions of Facebook users without their consent and used it for political campaigning. Finally, there is the risk of data sharing leading to the creation of biased algorithms that perpetuate discriminatory practices. For instance, Amazon's AI recruitment tool was found to discriminate against female candidates due to biased training data. These examples illustrate the potential threats that data sharing can pose, emphasizing the need for effective security measures and ethical standards to ensure the protection of individuals' privacy and prevent abuse of data. There are numerous threats to personal, confidential, and organizational data. One of the most significant threats to personal data is identity theft. Hackers may steal personal information such as social security numbers, credit card numbers, and other sensitive information, which can be used to commit identity theft, fraud, and other forms of cybercrime. Confidential data such as trade secrets, proprietary information, and intellectual property is also at risk. Competitors or hackers may try to steal confidential data to gain a competitive advantage or sell it on the black market. Another threat to organizational data is ransomware attacks, where hackers encrypt data and demand a ransom to restore access. This can lead to significant financial losses and damage to the company's reputation. Phishing attacks, where hackers use social engineering to trick employees into giving away login credentials or other sensitive information, are also a significant threat. Finally, employees themselves can pose a threat to organizational data through accidental or intentional data breaches. Negligent behavior, such as leaving passwords written down or using unsecured Wi-Fi networks, can also pose a risk to personal and organizational data. Overall, these examples illustrate the wide range of threats to personal, confidential, and organizational data and the importance of effective security measures to protect against them.

III. LITERATURE REVIEW

Human factors in information leakage**:** mitigation strategies for information sharing integrity: The paper begins by discussing the human factors that contribute to information leakage, including employee behavior, organizational culture, and external factors. It notes that employees can unintentionally or deliberately leak information, and that organizational culture can either promote or discourage information leakage. Additionally, external factors such as social engineering attacks and malware can also contribute toinformation leakage. The paper then examines various mitigation strategies that organizations can employ to reduce the risk of information leakage. These strategies include employee training and awareness programs, access control, data classification, incident response plans, monitoring and auditing, and organizational culture. The paper provides detailed explanations of each strategy and

highlights the benefits and drawbacks of each approach. and auditing, and organizational culture. The paper provides detailed explanations of each strategy and highlights the benefits and drawbacks of each approach. One key strength of the paper is its comprehensive coverage of the topic. The authors have synthesized a large body of research on human factors in information leakage and have provided practical advice for organizations seeking to reduce their risk. The paper is also well-organized and easy to follow, with clear headings and subheadings that help the reader navigate the content. However, one potential limitation of the paper is its focus on mitigation strategies. While the authors provide a thorough overview of these strategies, they do not delve into the root causes of information leakage or explore potential prevention strategies. Additionally, the paper is somewhat dated, having been published in 2018, so it may not reflect the latest research on the topic [1]. Data sharing in a time of pandemic: The journal paper focuses on the importance of data sharing during a pandemic, particularly the COVID-19 outbreak. The authors argue that sharing data across borders and between organizations is crucial for mitigating the spread of the disease and developing effective treatment methods. The paper provides a literature review of studies that highlight the benefits of data sharing, such as the rapid development ofvaccines and the identification of effective public health interventions. The authors also discuss the challenges of data sharing, such as the need to balance privacy concerns with the benefits of data sharing. They argue that policies must be put in place to ensure theprotection of individual rights and to avoid potential misuse of data. The paper suggests that increased collaboration between public health organizations, governments, and the private sector can facilitate more effective data sharing and improve global health outcomes [2]. Cross-domain secure data sharing using block chain for industrial IoT: The journal paper proposes the use of blockchain technology to facilitate secure data sharing in industrial Internet of Things (IoT) applications. The paper provides a literature review of previous studies that have explored the potential of blockchain for secure data sharing, highlighting its advantages such as its distributed nature, immutability, and resistance to tampering. The authors also discuss the challenges of implementing blockchain technology in industrial IoT settings, including the need to ensure compatibility between different systems and to develop a reliable and efficient consensus algorithm. The paper presents a cross-domain data sharing architecture that integrates blockchain technology with other security measures, such as encryption and access control, to provide a comprehensive security framework for industrial IoT data. The paper concludes that blockchain technology has the potential to revolutionize secure data sharing in industrial IoT, providing a secure and reliable platform for data sharing across organizational boundaries. However, further research is needed to explore the full potential of blockchain for industrial IoT applications and to address the challenges of its implementation [3]. User concerns regarding information sharing on social networking sites: The journal paper focuses on user concerns regarding information sharing on social networking sites (SNS). The authors provide a literature review of previous studies that have explored the factors that influence users' attitudes towards information sharing on SNS, including privacy concerns, trust, and perceived control. The paper discusses how users' concerns about privacy and security on SNS are influenced by their perceptions of the risks associated with sharing personal information online, as well as the trust they have in SNS and their perceived control over their own data. The authors also examine the impact of cultural differences and social norms on users' attitudes towards information sharing. The paper concludes that user concerns regarding information sharing on SNS are complex and multifaceted. Privacy concerns, trust, and perceived control are key factors that influence users' attitudes towards information sharing. The authors suggest that SNS providers need to address these concerns by developing privacy policies and security measures that are transparent, understandable, and user-friendly. The paper also emphasizes the need for further research on user concerns and preferences to inform thedevelopment of effective privacy and security measures for SNS [4]. On the value of information sharing in the presence of information errors: The paper investigates the importance of information sharing in the context of information errors. The authors argue that while information sharing is often touted as a means to improve decision-making and reduce uncertainty, it can also lead to the propagation of inaccurate or incomplete information. Using a mathematical model, the authors show that the benefits of information sharing depend on the likelihood of errors and the cost of those errors. In particular, they find that when the cost of errors is high, information sharing can actually be detrimental, as it leads to a higher likelihood of errors being propagated. However, when errors are less costly or less likely, information sharing can be highly valuable, as it allows decision-makers to pool their information and make better-informed choices. The authors conclude that while information sharing is not a panacea, it can be an important tool for reducing uncertainty and improving decision-making in many situations, especially when error rates are low. They also note that efforts to improve the accuracy of information should be a top priority for those seeking to promote effective information sharing [5] . Privacy Concerns and Information Sharing: The Perspective of the U-Shaped Curve: This paper explores the relationship between privacy concerns and information sharing. The authors argue that this relationship can be best understood through the concept of a U-shaped curve, which suggests that individuals are initially reluctant to share personal information due to privacy concerns, but become more willing to share as they perceive greater benefits from doing so. However, there comes a point where increased sharing leads to heightened privacy concerns, and individuals become less willing to share again. The authors use empirical evidence to support the U-shaped curve model, showing that individuals are more likely to share personal information whenthey perceive benefits such as convenience or social connection, but are less likely to share when they perceive potential harm or loss of control over their information. The authors conclude that efforts to promote information sharing must carefully balance the potential benefits with the need to protect privacy, and suggest that clear communication about data use and user control over personal information can help tomitigate privacy concerns and promote greater sharing [6].

Information Sharing in Cybersecurity: A Review: This paper provides a comprehensive review of the current state of information sharing in cybersecurity. The authors discuss the benefits and challenges of sharing information about cyber threats, as well as the various models and frameworks that have been proposed to facilitate information sharing. They note that information sharing can help to improve the overall security posture of organizations and the wider cybersecurity community, but also highlight the barriers to effective information sharing, such as legal and regulatory concerns, lack of trust between organizations, and technical challenges. The authors also identify the role of government in promoting information sharing, particularly in terms of developing standards and incentives to encourage participation. They conclude that information sharing is a critical component of effective cybersecurity, andthat continued research and collaboration are needed to overcome the challenges and enable effective sharing of threat

intelligence **[7].** Improving Security and Efficiency in Attribute-Based Data Sharing**:** This paper proposes a new method for data sharing that utilizes attribute-based encryption (ABE) and proxy re-encryption (PRE) techniques to ensure security and efficiency. The authors highlight the limitations of traditional access control methods and argue that ABE and PRE offer a more flexible and secure approach.They provide a detailed description of their proposed method, including the use of a centralized attribute authority (CAA) to manageuser attributes and a proxy server to handle data decryption and re-encryption. The authors also conduct a thorough analysis of theirmethod, highlighting its strengths and weaknesses, and compare it to other similar approaches. Overall, the paper contributes to the growing literature on attribute-based data sharing and provides a practical solution for organizations looking to improve their data security and efficiency **[8].** If We Share Data, Will Anyone Use Them? Data Sharing and Reuse in the Long Tail of Science and Technology**:** This paper explores the factors that influence data sharing and reuse in the long tail of science and technology. The authors examine the challenges faced by researchers in this area, including the lack of resources and incentives, the complexity of data, and the absence of clear guidelines for sharing and reuse. They argue that successful data sharing requires not only technical infrastructure, but also a supportive culture that values collaboration and recognizes the importance of data sharing in scientific progress. The paper presents case studies of data sharing initiatives in various fields, highlighting the factors that contributed to their success or failure. The authors also discuss the potential benefits of data sharing, such as increased scientific transparency, reproducibility, and innovation. Overall, the paper contributes to the growing literature on data sharing and emphasizes the importance of creating a culture of data sharing that encourages collaboration and rewards researchers for their contributions to the scientific community **[9].** The Ethics of Data Sharing and Reuse in Biology: This journal paper provides an in-depth analysis of the ethical considerations surrounding data sharing and reuse in the field of biology. The authors discuss the potential benefits of data sharing, such as increased scientific collaboration, transparency, and reproducibility, but also highlight the potential risks, includingprivacy concerns, misinterpretation of data, and the potential for misuse. They argue that data sharing should be guided by ethical principles, such as informed consent, confidentiality, and transparency, and that researchers have a responsibility to ensure that data are used appropriately and for the public good. The authors provide case studies of data sharing initiatives in biology, including the Human Genome Project and the Global Biodiversity Information Facility, and discuss the ethical challenges faced by researchers in these projects. The paper emphasizes the importance of engaging in dialogue with stakeholders, including patients, scientists, and the public, to develop ethical guidelines for data sharing that balance the potential benefits and risks. Overall, the paper contributes to the growing literature on data sharing and reuse in biology and provides a framework for ethical decision-making in this area **[10].**

IV.MITIGATING THREATS IN DATA SHARING

To mitigate the threats in data sharing, various methods can be employed. First and foremost, access control mechanisms should be put in place to ensure that only authorized users have access to the data. Secondly, data should be de-identified or anonymized before sharing to prevent the risk of re-identification. Thirdly, encryption techniques such as homomorphic encryption and differential privacy can be used to protect sensitive data. Fourthly, data sharing agreements should be developed, outlining the responsibilities of the parties involved and the restrictions on data use. Finally, regular monitoring and auditing of the data sharing process can help to detect and prevent any breaches or unauthorized access to the data. These methods, when used together, can help to minimize the risks associated with data sharing and ensure that sensitive data is protected.

V.CONCLUSION

The sharing of data has become increasingly common in various fields due to its numerous benefits. However, data sharing comes with various threats that can compromise the security, privacy, and integrity of the data. A review of journal papers on the topic of threats in data sharing highlights several issues that researchers and organizations face when sharing data, and the methods that can be employed to mitigate these threats. One of the most significant threats to data sharing is the risk of data breaches, which can result in the exposure of sensitive data to unauthorized parties. Such breaches can occur due to a lack of proper access control mechanisms, vulnerabilities in data storage and transfer systems, or human error. A review of the literature suggests that access control mechanisms, such as role-based access control, attribute-based access control, and access control policies, can help mitigate this threat. These mechanisms ensure that only authorized parties can access the data, and that access is granted only to the necessary data. Another significant threat to data sharing is the risk of re-identification of de-identified data. De-identification is a common technique used to protect the privacy of data, but it is not foolproof. Several papers highlight the risk of re-identification through methods such as linkage attacks, which can link seemingly anonymous data to specific individuals. To mitigate this threat, data anonymization techniques such as k-anonymity, l-diversity, and t-closeness can be employed. These techniques ensure that the data is protected, while maintaining the usability of the data for research purposes. A review of the literature also highlights the risks associated with the sharing of sensitive data, such as medical data. Such data can be highly valuable and can be used to commit identity theft or insurance fraud, among other things. To mitigate this threat, various encryption techniques such as homomorphic encryption and differential privacy can be employed to ensure that sensitive data remains encrypted, even during processing. Data sharing agreements are another method for mitigating threats in data sharing. Such agreements outline the terms of data sharing, including the responsibilities of the parties involved and the restrictions on data use. Data sharing agreements can help to prevent data misuse, breaches, or other unauthorized access by ensuring that parties are aware of the appropriate use of the data. In conclusion, the benefits of data sharing are numerous, but so are the threats. Researchers and organizations must be aware of the risks associated with data sharing and employ various methods to mitigate these threats. This review of journal papers highlights the importance of access control mechanisms, data anonymization techniques, encryption techniques, and data sharing agreements. By using these methods in combination, organizations can ensure that their data remains secure, private, and usable for research purposes.

VI. ACKNOWLEDGEMENT

First and foremost, I give all glory, honor and praise to God Almighty who gave me wisdom and enabled me to complete thiswork successfully.

I also want to thank my parents from the bottom of my heart for their encouragement and help with this work and with all of my

other endeavors.
I am incredibly grateful to Dr. V. P. Devasia, Principal of SJCET in Palai, for letting me use all of the facilities there as well asfor his support. Words cannot adequately express how grateful I am.
I would like to express my sincere gratitude to Mr. Anish Augustine, HOD Incharge, Department of MCA, SJCET, Palai, who has served as a constant inspiration and without whose invaluable assistance and support this work would not have been possible. I owe a particular debt of gratitude to Mr. Akhil Sekharan, Asst. Professor, Department of Computer Science and Applications, SJCET, Palai, for all the necessary help and support that he has extended to me. His valuable suggestions, corrections, and sincereefforts to accomplish this work even under a tight time schedule were crucial to the successful completion of this work.
I extend my sincere thanks to all of our teachers and non-teaching staff at SJCET, Palai, for the knowledge they have impartedto me over the last three years.
Additionally, I would like to thank all of my friends for their encouragement, advice, and support.

V. REFERENCES

1. Wai Peng Wong, Hwee Chin Tan, Kim Hua Tan and Ming Lang Tseng, “Human factors in information leakage:Mitigation strategies for information sharing integrity”, Industrial Management & Data Systems, Vol.119 No.6, pp.1242-1267.https://doi.org/10.1108/IMDS-12-2018-0546
2. Sarah Callaghan, “Data sharing in a time of pandemic”, 2020, https://doi.org/10.1016/j.patter.2020.100086
3. Parminder Singh, Mehedi Masud, M. Shamim Hossain and Avinash Kaur,” Cross-domain secure data sharing using blockchain for industrial IoT”,2021
4. Ibrahim Mutambik, John Lee, Abdullah Almuqrin, Waleed Halboob, Taha Omar and Ahmad Floos, “User concernsregarding information sharing on social networking sites: The user’s perspective in the context of national culture” ,2022
5. Jizhou Lu, Gengzhong Feng, Stephen Shum and Kin Keung Lai,” On the value of information sharing in the presence of information errors”
6. Chien –Lung Hsu, Yi-Chuan Liao, Ching7-Wen Lee and Lin Kun Chan, “Privacy concerns and information sharing: the perspective of the u-shapes curve”,2022
7. Ali Pala and Jun Zhuang, “Information sharing in cybersecurity: A Review”
8. Junbeom Hur, “Improving Security and Efficiency in Attribute-Based Data Sharing”,2013
9. Jillian C. Wallis*, Elizabeth Rolando, Christine L. Borgman, If We Share Data, Will Anyone Use Them? Data Sharing and Reuse in the Long Tail of Science and Technology,2013
10. Clifford S. Duke and John H. Porter, The Ethics of Data Sharing and Reuse in Biology,2013, Bioscience, Volume 63