Data Protection in Collaboration: Safeguarding Sensitive Information with Third-Party Stakeholders

Rajendraprasad Chittimalla

MS Information Systems Security, Software Engineer - Team Lead

Abstract: ***The evolution of technology carries complex problems and the solutions require extra care to continue providing a better user experience. The sensitive data can be categorized into PII, PHI, and IP where each has its importance and needs to be protected. The protection of sensitive data is also regulated by international laws like HIPAA and GDPR. Thus, organizations are bound to follow these regulations and provide data security to both the internal organizational data and user data. Factors like financial costs, organizational reputation, business disruptions, and legal boundaries, affect the user experience. The suggested best practices can be followed by the organization and the internally assigned staff members to cope with the problem of exposing sensitive information to third-party service providers. The privacy of the user should be kept under consideration while allowing these service providers to access the limited data and therefore it can mitigate the security threats.***

Keywords: data breaches, security threats, privacy, secure file transfer, encryption, third-party integration

1. Introduction

Data protection is the main concern of end users and some organizations are depriving this concern due to limited resources. They tend to share data with cloud services and third-party organizations using applications like IBM SFG and GoAnywhere with the least effort spent on data protection. The data confidentiality is distributed from the most publicly available data to the confidential one. This can be understood by the figure 1 given below:

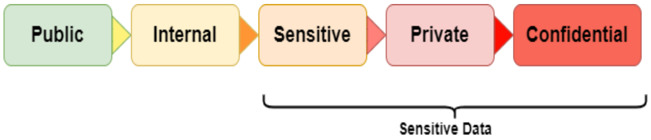

Figure 1: Data Confidentiality

The sensitive information can be categorized into three main classes: Personally Identifiable Information (PII), Protected Health Information (PHI), and Intellectual Property (IP). The PII lies in the first radius which includes personal information such as name, contact, identification numbers, and bank account details [1]. The PHI however refers to the medical records and IP contains company secrets, their creative and unique identifiers [2] & [3]. The problem is that the intruders are also interested in this sensitive information to achieve their hidden objectives. This can cause severe problems like data breaches, reputational damage to organizations, and legal issues.

The given research article projects the importance of protecting the sensitive information of both the users and the organization. The focus however remains the protection of confidential data while sharing with third parties. This writing therefore first presents the importance of data protection and then best practices that can be followed to protect sensitive information from being exposed. The future development further evaluates the potential of the continuously evolving technologies that can further assist in successful data protection.

2. Literature Review

Sharing data with other companies has become inevitable for large organizations to provide better services to customers by utilizing fewer resources. However, some organizations are willingly sharing their customer data with third-party organizations without checks and balances. These organizations need to understand that they might face the risks of losing brand value and customer trust and might have to tackle legal regulations. These organizations should protect the customer's data by employing protection schemes and appropriate segmentation of data [4].

One of the biggest needs of organizations is the online space which is provided by different cloud sharing companies. Cloud computing provides many advantages to companies to save their resources and utilize public or hybrid cloud spaces. This is feasible for most startup companies who are lacking dedicated space resources. But on the other hand it is concerning for their customers as cloud data sharing is associated with data loss risks [5].

3. Problem Statement

The modern world is employing more sophisticated technologies and therefore organizations are more focused on specific domains. To achieve the desired objectives of the overall system, these organizations mostly need third-party services for the complete functioning of the system. However, this brings the issue of data protection. The three types of sensitive information include PII, PHI, and IP. These are the actual targets of intruders which is why organizations need to consider the importance of protecting sensitive information when sharing with third parties. So there is a need to first understand the importance and then employ best practices to mitigate the risks for organizations.

4. Importance of Data Protection

4.1. Financial Issues

The financial losses in terms of legal costs, compensations, revenue loss, and the amount paid to the user as a penalty are concerning, and therefore it is enough motivation to properly deal with data while giving access to third parties. The increased breaches can lead to the complete shutdown of an organization. It can also lead a company to an indefinite debt loop.

4.2. Organizational Reputation

The reputation of an organization is directly linked with the protection of data involved in the system. A tiny breach can lead to a major setback to business with the loss of customers.

4.2.1. Customer Turnover

The software industry is standing on the attention gained from the end user to convert the potential individual to a customer. Customers have many options to enjoy a service which can lead to a major turnover if they feel that the organization is not concerned about data protection and is sharing everything with third-party service providers [6].

4.2.2. Word of Mouth

It takes a long trail of actions to make the software stand out in public and prevail through positive word of mouth. It becomes devastating when suddenly people realize that their data is no longer protected in the system and the whole reputation is converted to negative word of mouth. This however is the no-returning path and loses the entire growth spectrum of the company.

4.2.3. Investor Interest

The software business is dependent on the positive response of all stakeholders. The investors are at the top position without which business expansion is not possible. If an investor finds that the organization cannot manage unwanted situations then it may lose the investor confidence for unstable returns to their investment.

4.3. Business Disruptions

The daily operations of a business can be disrupted after a breach and the normal business sequence can be affected. The emergency teams are needed for immediate actions and a dedicated rule book for limiting the data access to third parties. If not handled properly, these operational failures may disrupt the running revenue and add to the recovery costs burden on the company.

4.4. User Experience

The digital user nowadays has many options to choose to avail the similar services. The choice however is primarily made based on the strength of the privacy policy provided by the service providers. This identifies the importance of data protection and how it is directly linked to the user experience of the system. The organizations are therefore concerned about considering this factor before taking any action on the user's data. The third-party services are restricted to only limited information and provided according to the actual need of the service.

4.5. Legal Boundaries

The two famous legal regulations from the United States and the European Union are discussed below accompanied by their importance to be followed. Figure 2 below gives the hierarchy of data privacy:

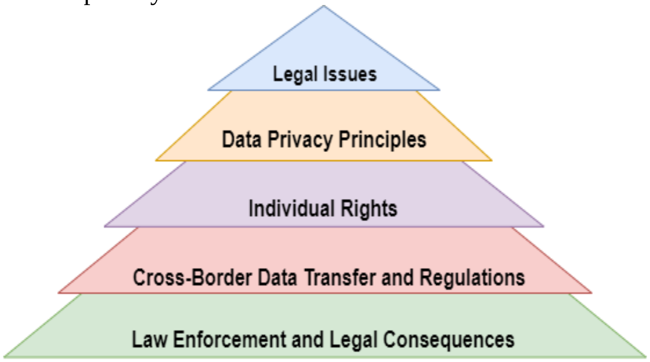
Legal Issues
Data Privacy Principles
Individual Rights
Cross-Border Data Transfer and Regulations
Law Enforcement and Legal Consequences

Figure 2: Legal Regulation Hierarchy of User's Data

4.5.1. Health Insurance Probability and Accountability Act

The Health Insurance probability and Accountability Act (HIPAA) refers to the protection of the medical record of patients. This law is regulated by the United States bodies and organizations are bound to protect medical records or health-related data [7].

4.5.2. General Data Protection Regulation

The General Data Protection Regulation (GDPR) is regulated by the European Union and organizations are required to protect the individual's data according to the privacy policy signed by the end user [8].

There are certain other regulations as well such as the California Customer Privacy Act, Federal Information Security Management Act of 2002, Children's Online Privacy Protection Act, and Electronic Communications Privacy Act where each of them suggests a distinctive set of rules that needs to be followed.

In the context of blockchain and cryptocurrency, tokenization refers to the process of converting assets or rights into digital tokens on a blockchain. This can include real estate, shares, or any other form of asset, providing liquidity and fractional ownership. Chen and Zhao also examine the role of cloud service providers in ensuring robust security practices and compliance with privacy regulations. Additionally, the paper identifies the need for continuous monitoring and auditing to maintain data integrity and confidentiality [5].

5. Best Practices

The following best practices can be followed to protect sensitive information especially when sharing data with third parties:

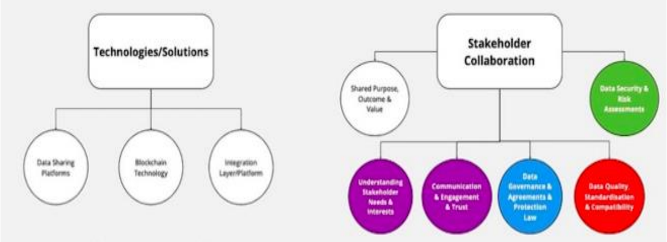
Technologies/Solutions
Data Sharing Platforms
Blockchain Technology
Integration Layer/Platform
Stakeholder Collaboration
Shared Purpose, Outcome & Value
Data Security & Risk Assessments
Understanding Stakeholder Needs & Interests
Communication & Engagement & Trust
Data Governance & Agreements & Protection Law
Data Quality, Standardisation & Compatibility

Figure 3: Data Sharing with Stakeholders

- Add additional security layers to further protect the user's data.
- Only a limited amount of data necessary to avail the service should be shared with third parties.
- A strong contract should be signed with the third-party service providers to ensure that the user's data is protected by their end as well.
- Ensure that the privacy policy of users is not violated at any cost.
- The latest encryption techniques should be followed while making any transfers and allowing third parties to access the data.
- Maintain both internal and shared log files to identify malicious activities of accessing data.
- Push the continuous update to the system.
- Employ regular testing techniques and focus on the modules that are sharing data with other organizations.
- The employees should be well trained and equipped with essential skills to defend against unwanted attacks.

6. Research Impact

The research defines the importance of protecting sensitive data while using third parties. After successfully putting all the points, the research achieves the objective of the importance of data and risks associated with the sharing of data with third parties. The circumstances of neglecting legal boundaries such as GDPR and HIPAA are discussed to further equip with the significance of this topic. The best practices advised in this research help to avoid the potential risks of data policy violations. Thus, the presented study will help organizations develop appropriate policies after carefully understanding the importance of protecting sensitive information while sharing it with external entities.

7. Future Developments

The future of technology hides mysteries but here are some of the feasible developments possible in this area of research:

- The encryption techniques are continuously changing and therefore the updated methods will help further protect the data.
- BlockChain technology is making progress from day to day and it is expected that it might become the practical concept for secure data handling.
- A field like Data Analytics will help extract insights into unusual activities.
- The use of Artificial Intelligence and Machine Learning along with human touch will revolutionize this field.

8. Conclusion

In the end, most organizations are dealing with either external user data or internal sensitive data which is required to be protected. The organizations are required to abide by the international regulations of protective user data. For that, the organization first needs to identify the risks associated with sharing data with third parties and understand the importance of protecting sensitive data. The crucial points are pondered in the given writing to deliver the significance of data protection and then the best practices that need to be followed.

The sensitive information needs to be protected with effective use of applications like IBM SFG, Axway, Globalscape, MoveIT and GoAnywhere. These essential tools ensure the prevention of data breaches and help maintain the trust and reputation of the company. The vulnerabilities can be addressed with the use of modern encryption methods, strong authentication methods, protection APIs, and regular updates. With the correct use of these methods and data transfer applications, sensitive information can be protected while doing file transfer. Mandating the encryption or dual encryption and encryption at rest for PII data, password rotation every 90 days for all users, these methods will help to protect the data when transmitting with stakeholders.

References

[1] A. Narayanan and V. Shmatikov, "Privacy and security: Myths and fallacies of "personally identifiable information"," vol. 53, no. 6, pp. 24-26, 2010.

[2] J. K. Pool, S. Akhlaghpour, F. Fatehi and A. Burton-Jones, "Causes and Impacts of Personal Health Information (PHI) Breaches: A Scoping Review and Thematic Analysis," in *Twenty-Third Pacific Asia Conference on Information Systems, China July 2019*, China, 21 May 2020.

[3] P. S. Menell and S. Scotchmer, "Chapter 19 Intellectual Property Law," in *Handbook of Law and Economics*, 2007, pp. 1473-1570.

[4] M. J. Schneider, S. Jagpal, S. Gupta, S. Li and Y. Yu, "Protecting customer privacy when marketing with second-party data," *International Journal of Research in Marketing*, vol. 34, no. 3, pp. 593-603, Sep 2017.

[5] D. Chen and H. Zhao, "Data Security and Privacy Protection Issues in Cloud Computing," in *2012 International Conference on Computer Science and Electronics Engineering*, Hangzhou, China, 23 April 2012.

[6] K. D. Martin, A. Borah and R. W. Palmatier, "Data Privacy: Effects on Customer and Firm Performance," vol. 81, no. 1, 1 Jan 2017.

[7] Shoaf and H. R., "Health Insurance Portability and Accountability Act (HIPAA)," *Protected Health Information (PHI) - Physician's Office Challenges*, vol. 23, no. 2, pp. 75-77, 2003.

[8] C. J. Hoofnagle, B. v. d. Sloot and F. Z. Borgesius, "The European Union general data protection regulation: what it is and what it means," *Information & Communications Technology Law*, vol. 28, no. 1, pp. 65-98, 2019.