International Journal of Computer Science and Information Technology Research (IJCSITR)
2023, Vol. 4, No. 1, January – June, pp. 7-13
Journal ID: 9471-1297
website: www.ijcsitr.com

Preventing Data Breaches: Effective Strategies for Secure File Transfer Tool Implementation

Rajendraprasad Chittimalla,
Equifax Inc, USA.

Abstract

Data breaches are the primary concern for organizations and significant resources need to be allocated to protect data files doing file transfer. This writing is all about identifying the challenges and the adoption of effective measures. It's about how useful tools can help to restrict access to unwanted actions. These measures are instance, encryption, RBAC, MFA, validations, audit trails, and employee training to help to mitigate the issues using effective implementations. Although organizations nowadays are exposed to multiple high-end technologies but are mainly restricted due to limited resources such as cost and limited human resources. The given research also presents the best practices that can be followed for effective implementation to protect data during file transfers.

Keywords

data breaches, security challenges, privacy, authentication, secure file transfer, transfer protocols

How to Cite: Rajendraprasad Chittimalla. (2023). Preventing Data Breaches: Effective Strategies for Secure File Transfer Tool Implementation. International Journal of Computer Science and Information Technology Research, 4(1), 7-13.

1. Introduction

In today's world of evolution, data breaches have become the primary concern for the organization as the more modern interruption methods are developed by the attackers. There is a need for secure file transfer to restrict unauthorized access and ultimately data loss [1].

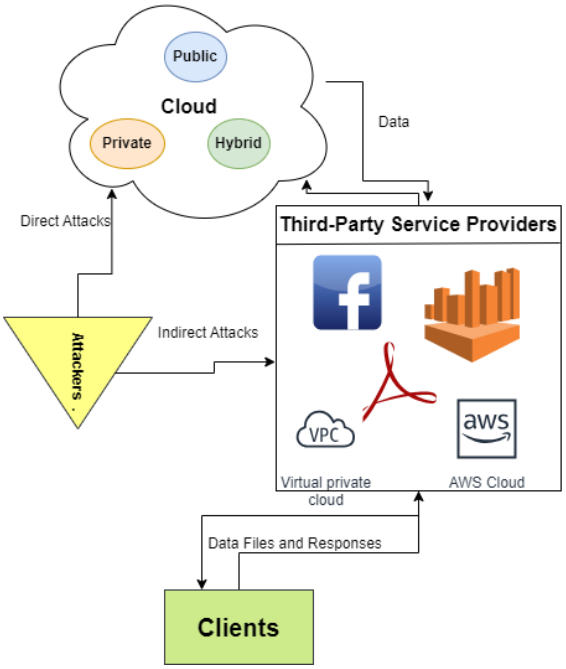

Figure 1: The Architecture to Understand Malicious Attacks

This writing explores the challenges that are faced by organizations to implement secure file transfer tools to reduce the risk of data breaches. Also, how effective methods can be adopted to implement the secure file transfer tools. The security challenges are identified and the appropriate measures are presented against them. The best practices are also suggested to the organizations at the end along with the future methods that would be helpful for these organizations. The distribution of this article is made to completely address this serious security problem for all the stakeholders.

The Data Breaches are accompanied by the potential of financial risks, bringing the reputation of the organization at stake and indulging legal scenarios as a consequence. Organizations using cloud services are more exposed to attacks. Figure 1 above shows how data integrity is disturbed by intruders when sharing data on cloud services. The industry however has evolved but the security of data is the biggest issue for organizations specifically during data transfer. There are certain hindrances in implementing effective file transfer tools which are resolved through the presented methods.

2. Literature Review

The data requirements and the complexity of the software systems are increasing day by day and it brings the need for data security to the organizations. The models have to be trained on the large datasets and these datasets need to be stored somewhere online. The problem is that most of the data in these large datasets is liable to user privacy and therefore needs to be protected. These thousands of records should also be efficient enough to provide fast results. The file transfer protocols somewhat erase the problem of efficient file transfers. Managed File Transfer (MFT) utilizes networks and provides efficient co-scheduling of dependent data transfer [2].

The difficulty of creating ciphertext and making it valid for users is provided by the

technique of robust encryption. Anonymous encryption is therefore provided but it comes with many hindrances as well. There are a lot of robust encryption techniques and each of them is hard to follow as they come with some extra unwanted perks. This allows strong encryption but also it becomes costly to protect sensitive information during transfers [3].

3. Problem Statement

Maintaining the security of the system and preventing data breaches during file transfers is a cumbersome task and becomes a challenge for the fast-evolving software industry. Effective strategies and measures are needed to ensure secure file transfer. The implementation of the file transfer tools requires organizations to adopt appropriate ways to achieve the desired security goals for themselves as well as for end users. The aim of the paper is therefore to address the challenges and present effective measures that can be adopted to resolve the problem of data breach.

4.Security Challenges

The software industry nowadays faces some of the following security challenges during file transfers [4], & [5]:

4.1. Data Encryption

The data encryption must be ensured under strong MFT encryption protocols such as Transport Layer Security (TLS) and Advanced Encryption Standards (AES). It can be challenging to encrypt the data, especially in transit.

4.2. Authentication & Authorization:

Only the authorized user should be able to log into the system under the boundaries provided by the organization depending on the role of the user. The useful password strengths should be recommended for a more encapsulated experience. Other than that, the use of Multi-Factor Authentication (MFA) provides an extra layer to the security of the system.

4.3. Handling Emergencies

Emergencies can be faced during potential malicious attacks. The potential weakness of the system should be identified and fixed in a controlled environment. A dedicated emergency team is needed to handle the sudden unwanted situation.

4.4. Automated Response

Some of the data breaches needed to be dealt with in a short period to maintain the confidentiality of data. For these sudden breaches, an extra layer of security needs to be added as an auto-response from the system.

4.5. Third-Party Assessments

It’s difficult to handle third-party integrations with the system to maintain security. The limits need to be applied to the access of third-party services. This is a mandatory security step for all the associated parties.

4.6. Security Training

All the staff members of the project are required to be trained to handle regular security tasks as well as emergencies. This will also help raise the knowledge of security and its importance among the employees.

4.7. Audit Trails

The file transfer events are needed to be well monitored. The audit trail serves as a record to sequence the activities against a specific time. The audit trail contains a sequence of activities against time.

5. Effective Measures

The following effective measures can be employed to overcome the challenges faced by the organizations during the implementation:

5.1. Data Encryption

The tools like OpenSSL are used to encrypt the data during transfer. This makes the original data unavailable to the unauthorized person even if the breach has been made possible. This is because the information during the transfer would remain encrypted and therefore unreadable to an outsider. For instance, the feasible implementation will be the use of IBM Aspera, GoAnyWhere MFT, MoveIT, and Cleo Integration. For instance, the code workflow for GoAnywhere is given as [6],

```
import com.goanywhere.api.*;

GoAnywhereClient c = new GoAnywhereClient("https://goanywhere.server.com",
"user", "pass");

EncryptionConfig conf = new EncryptionConfig();
conf.setAlgorithm("AES-256");
conf.setKey("key");
conf.setInputFilePath("/input/file");
conf.setOutputFilePath("/encrypted/file");

client.encryptFile(conf);
```

5.2. Multi-Factor Authentication

The extra steps are required from the end user to access the data under Multi-Factor Authentication (MFA). Some of the multi-factor authentications are sending code to a mobile number, verifying a unique number on an assigned mobile device, and even Google device verification. The same tools like IBM Aspera, GoAnywhere MFT, MoveIT, and Cleo Integration are valid here.

5.3. Role-Based Access Control

This is a role-based approach for accessing the data and gives limited access to users according to the role assigned within the system. For instance, the end user may have control over their data, the admin controls a broad spectrum and an IT department may have access to even sensitive data. Thus unauthorized access is implemented with the use of Role-Based Access Control. The possible examples are Coviant Diplomat, JSCAPE MFT Server, and

Globalscape EFT. The example of JSCAPE is given as,

```
import com.jscape.api.*;
JSCAPEClient c = new JSCAPEClient("https://jscape.server.com", "user",
"pass");

Role r = new Role("data_analyst");
r.addPermission("read");
r.addPermission("write");

// Create the role
c.createRole(r);
// Assign the role to a user
c.assignRoleToUser("data_analyst", "user1");
```

5.4. User Input Validation

The code injections like SQL injections can be prevented by using the input validations. For instance, the minimum characters of the password, using a specific data type for an input field, and pattern matching can be used to avoid malicious coding attacks.

5.5. Audit Logging

The audit log gives a complete record in chronological order according to the time when a specific request is made in the system. It stores all the necessary information of the individual device from which the request is made. For instance, the Splunk tool can be used for continuous monitoring. Therefore, by tracking all file transfer activities, the potential attacks can be prevented [7].

5.6. Training & Response Plan

The training should provide the employees to be equipped with the best action plan according to the situation. The immediate response to malicious attempts like phishing helps improve security. The data handling techniques will allow them to understand secure file transfers. Any data breach can be restricted if the employees are trained for the situation.

5.7. Effective Third-Party Assessments

The regular review of security policies and a chain of previous incidents can be helpful while dealing with third parties. The regular assessments according to the set standards play a major role here.

6. Industrial Challenges

Although the industry progressed exponentially in recent times, there remain some hindrances in the way of employing security measures. These challenges are accumulated below:

- **Expense Management:** The cost is the first step of the ladder in the software industry.

Without controlling the cost of software, there remains no success of the system. The expense of adopting measures for secure file transfer brings a major contribution to the overall cost of software.

- **Software Complexity:** The integration of effective security measures in the software increases the complexity and therefore it becomes difficult to effectively organize the different chunks of code and integrate them effectively while maintaining this new entity.
- **Legal Boundaries:** The organizations are bound to abide by the law of both local and international bodies. This becomes challenging as a further assessment is mandatory before implementing the new security measures. Factors like user privacy are the major concerns in this matter.
- **Change Resistance:** The security features may please the end users but employees can resist sudden changes in different modules of the system. This increases the inconvenience for the staff members to tackle the bug fixes and regular updates.

7. Best Practices

These are some of the best practices that can be followed in the industry to prevent security breaches during data transfer. The industry should ensure that,

- Continuously monitor their systems to make sure that potential security threats can be identified before any breach and threats can be responded to immediately.
- The regular updates of the system to cope with the latest methods of security violations. The continuous updates if pushed become a challenge for the attackers to intercept between the transfers or in the system.
- Strong data encryption methods need to be applied with complicated encryption and decryption keys for further data protection.
- The multi-layer security can be implemented to prevent malicious attacks from reaching sensitive data. The more layers with individual strength will therefore lead to attack failure.
- The access should be provided appropriately to users depending on their role in the system.
- The strong passwords need to be recommended to users to make their profile data secure for unwanted access.

8. Research Impact

The presented methods will equip the software organizations in the industry with the latest strategies and effective measures to face the challenges of data breaches and therefore these measures help to achieve secure file transfer for a better user experience. To mitigate the risks of data breaches, the industry protocols can be followed while considering the best practices to avoid unwanted access. Therefore, the sensitive information of both the user and the organization can be secured.

9. Future Developments

The future is accompanied by serious mysteries as the digital world is continuously subliming rapidly. The evolution of Artificial Intelligence and Large Language Models brings

more ease for the developers to ensure security measures in the system. Also, automation procedures are being developed to take care of the security implications of the system. To enhance the user experience, the future has the potential to provide more effective security features along with friendly user interfaces.

10. Conclusion

As a cessation, the security of the system is the main concern for the organization to share transparency with the end users. The users are also highly concerned about the privacy of their data which makes it inevitable to provide strong security. Multiple approaches can be followed to ensure the integrity of user data. By employing effective measures and following the best practices for industry standards, the risk of data breaches can be reduced. Thus, the sensitive data of the user is protected under the privacy policy duly signed by them.

The organizations nowadays are concerned about cost effective security methods as well as tend to prioritize the privacy of the end user to enhance the user experience. The best practices if followed can help these companies achieve these objectives for better implementation of secure file transfer tools. These suggestions are provided against the challenges faced by this industry. The legal boundaries are the primary concern of organizations and therefore need to take extra care while doing security feature implementations.

References

[1] R. Ayyagari, "An Exploratory Analysis of Data Breaches from 2005-2011: Trends and Insights," Journal of Information Privacy and Security , vol. 8, no. 2, pp. 33-56, 2012.

[2] B. Ross, E. Arslan, B. Zhang and T. Kosar, "Managed File Transfer as a Cloud Service," in Cloud Computing for Data Intensive Applications, Springer Science+Business Media New York, 15 Nov 2014, pp. 379-399.

[3] M. Abdalla, M. Bellare and G. Neven, "Robust Encryption," Journal of Cryptography, vol. 31, pp. 307-350, 12 Jun 2017.

[4] L. Cheng, F. Liu and D. (. Yao, "Enterprise data breach: causes, challenges, prevention, and future directions," Data Mining and Knowledge Discovery, 09 Jun 2017.

[5] R. Sen and S. Borle, "Estimating the Contextual Risk of Data Breach: An Empirical Approach," Journal of Management Information Systems, vol. 32, no. 2, 28 Aug 2015.

[6] S. Kang, J. Kim and M. Hong, "Go anywhere: user-verifiable authentication over distance-free channel for mobile devices," Personal and Ubiquitous Computing, vol. 17, pp. 933-943, 17 Apr 2012.

[7] S. Jayashankar and S. T. Kandy, "Implementing Granular Access Definitions in Log Records," Computer Science and Engineering 2020, vol. 10, no. 1, pp. 22-30, 2020.