Available online www.ejaet.com

European Journal of Advances in Engineering and Technology, 2020, 7(8):105-109

Research Article ISSN: 2394 - 658X

Securing Business Intelligence Platforms: Best Practices for Data Governance and Compliance

Syed Ziaurrahman Ashraf

Email: ziadawood@gmail.com
Principle Solution Architect @ Sabre Corporation

ABSTRACT

Business Intelligence (BI) platforms are instrumental in driving data-driven decision-making across organizations. However, the ever-increasing amount of sensitive data necessitates a robust framework for securing BI environments. This paper discusses the best practices for ensuring data governance and compliance within BI platforms, addressing key challenges in security, data privacy, and regulatory adherence. We explore methods for enforcing data access policies, implementing encryption, monitoring data usage, and ensuring compliance with industry regulations such as GDPR and HIPAA. By integrating these best practices, organizations can safeguard their BI systems while maintaining data integrity and availability.

Keywords: Business Intelligence, Data Governance, Compliance, Data Security, Encryption, GDPR, HIPAA, Data Privacy, Access Control, Monitoring

---

INTRODUCTION

Business Intelligence (BI) platforms enable organizations to collect, analyze, and visualize data, driving strategic decisions. However, the sensitive nature of the data processed in these platforms introduces vulnerabilities that require a structured security framework. In a landscape shaped by regulatory frameworks like the General Data Protection Regulation (GDPR) and the Health Insurance Portability and Accountability Act (HIPAA), ensuring compliance while maintaining the integrity and availability of data is paramount.

Data governance in BI platforms covers the policies, standards, and controls that manage data quality, security, and access. Without these, businesses risk non-compliance, data breaches, and financial penalties. This paper presents a structured approach to securing BI platforms by employing the best practices in data governance, access control, encryption, and compliance monitoring.

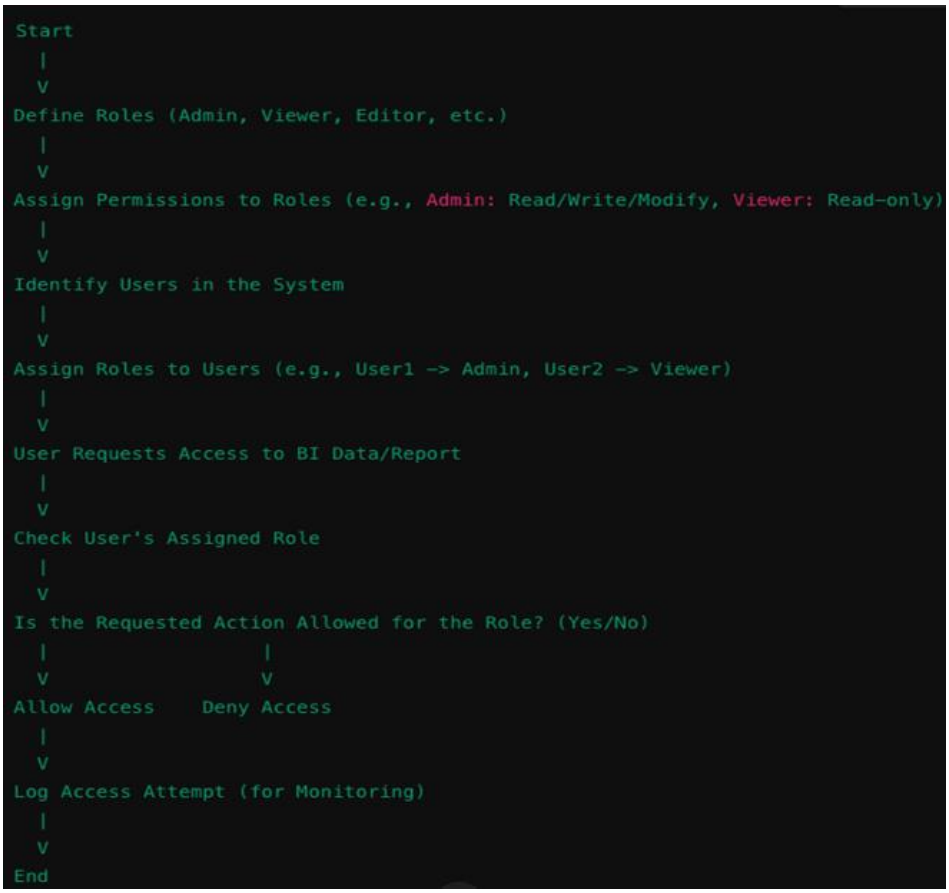
Business Intelligence (BI) platforms like Microsoft Power BI, Tableau, and Looker allow businesses to visualize and analyze their data. However, these platforms handle sensitive data like customer records, financial details, and health information. Without proper security, this data can be exposed to threats, including unauthorized access and data breaches.

Data governance plays a key role in securing BI platforms. It refers to the management of data policies, access controls, and compliance with regulatory requirements. In this paper, we explore several ways to secure BI platforms by following data governance and compliance best practices, including access control, encryption, and monitoring.

BEST PRACTICES FOR SECURING BI PLATFORMS

1. Data Access Policies and Role-Based Access Control (RBAC)

Implementing role-based access control (RBAC) ensures that only authorized personnel have access to specific data sets. This minimizes the risk of unauthorized access and potential data leaks.



Flowchart: *Implementing Role-Based Access Control (RBAC)*

This flowchart outlines the basic process for RBAC in a BI platform, from defining roles to checking permissions and logging access attempts.

Pseudocode Example: Role-based Access Control Setup

```
class Role:
    def __init__(self, role_name):
        self.role_name = role_name
        self.permissions = []

    def add_permission(self, permission):
        self.permissions.append(permission)

class User:
    def __init__(self, username):
        self.username = username
        self.roles = []

    def assign_role(self, role):
        self.roles.append(role)

    def has_permission(self, permission):
        for role in self.roles:
            if permission in role.permissions:
                return True
        return False
```

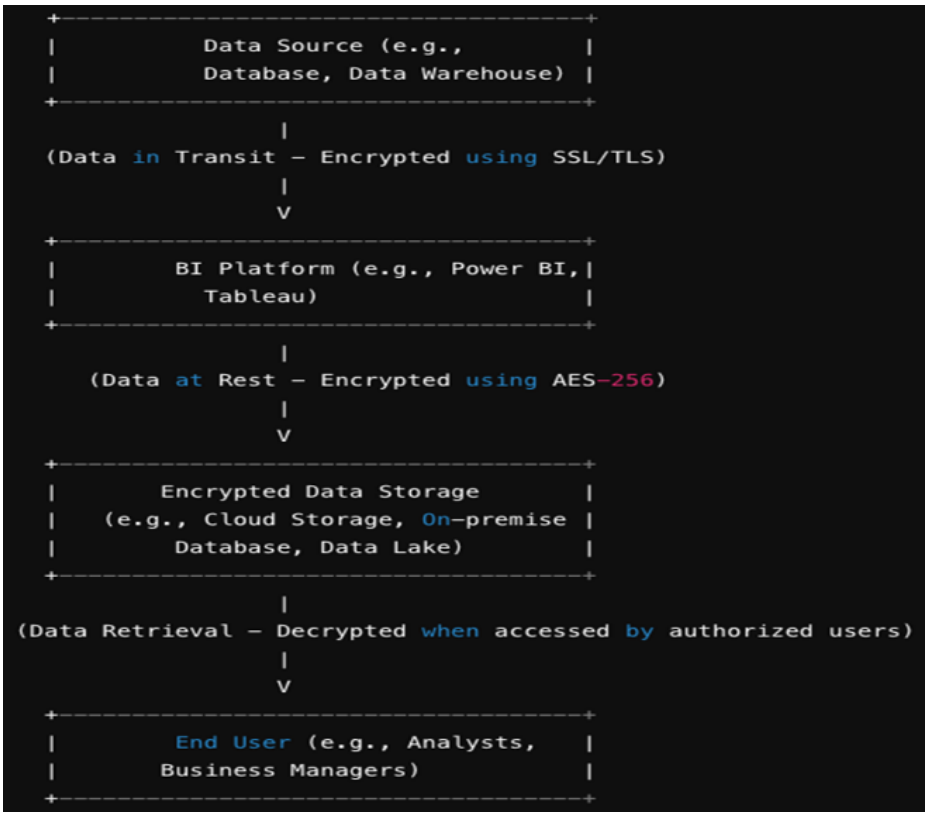
```
# Example roles and permissions
admin_role = Role("admin")
admin_role.add_permission("access_sensitive_data")
admin_role.add_permission("modify_reports")

user_role = Role("user")
user_role.add_permission("view_reports")

# Assigning roles to users
admin = User("AdminUser")
admin.assign_role(admin_role)

standard_user = User("StandardUser")
standard_user.assign_role(user_role)
```

2. Data Encryption and Secure Data Storage

To ensure data security both in transit and at rest, encryption techniques should be implemented. Data encryption uses algorithms to scramble data into an unreadable format, which can only be decrypted with the correct key.

Diagram: Data Encryption in BI Platforms

(A diagram showing how encryption is applied during data transmission between a BI platform and external sources, as well as at rest in data warehouses.)



● AES-256 Encryption: Implementing AES-256 for encrypting data at rest and in transit ensures robust security.

● Key Management: Secure key management practices, such as rotating encryption keys and using Hardware Security Modules (HSM), further enhance protection.

Explanation:

● Data in Transit: Data is encrypted during transfer from the data source to the BI platform using SSL/TLS.

● Data at Rest: After reaching the BI platform, the data is encrypted (e.g., using AES-256) when stored.

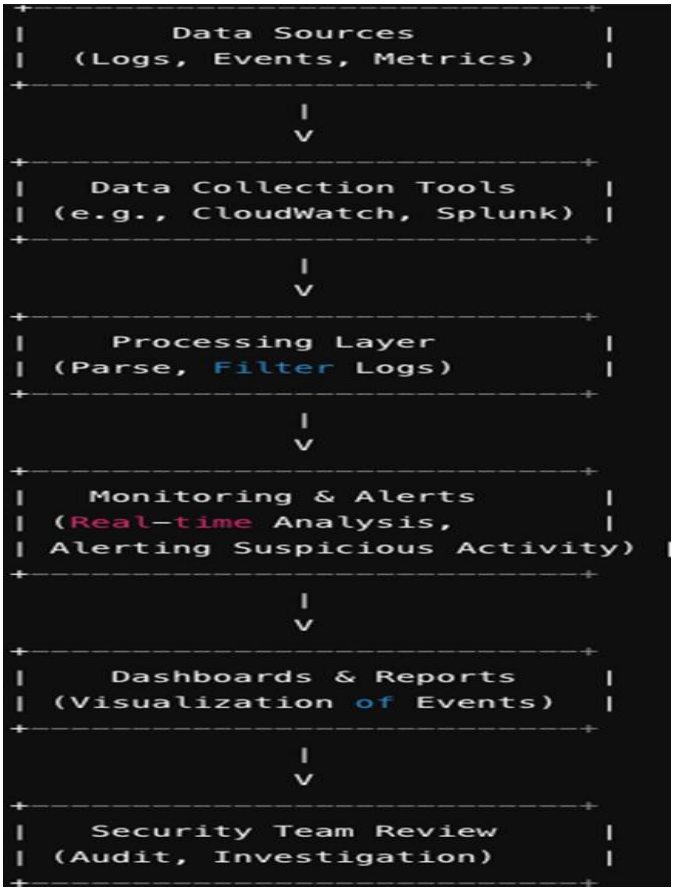
● Data Retrieval: When authorized users (e.g., analysts) access data from storage, it is decrypted and presented in the BI tool's reports and dashboards.

3. Monitoring and Logging for Compliance

Real-time monitoring and logging activities provide visibility into how data is accessed and used within BI platforms. This is critical for auditing purposes and ensuring compliance with legal and regulatory frameworks.

Graph: Real-Time Monitoring Architecture

(A graph that depicts the layers of a monitoring system, including log collection, processing, and alerting mechanisms.)



Explanation:

- **Data Sources:** Logs from various parts of the BI system, including activity logs, user access logs, and database logs.
- **Data Collection Layer:** Tools like AWS CloudWatch, Splunk, or Azure Monitor gather logs from these data sources.
- **Data Processing Layer:** This layer parses the logs, filtering out unnecessary data and retaining important events.
- **Monitoring and Alerting:** Real-time tools analyze the processed logs, setting alerts for unusual activity (e.g., unauthorized access).
- **Visualization and Reporting:** Dashboards show real-time and historical insights for security teams to monitor system behavior.
- **Security/Compliance Review:** Security teams review logs and alerts for compliance, conduct audits, and investigate incidents.

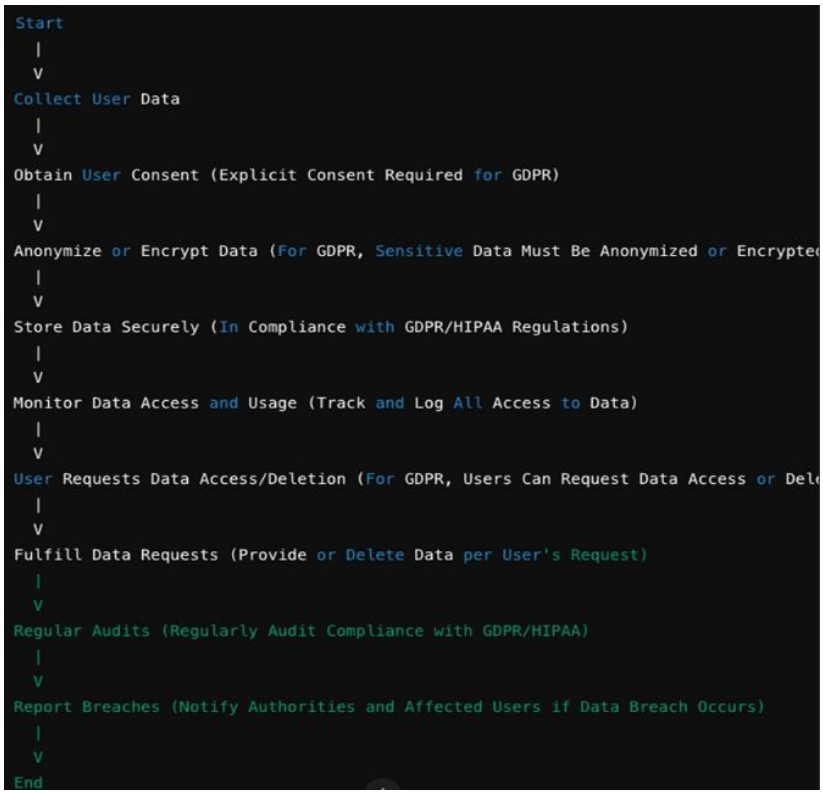
By employing continuous monitoring tools like AWS CloudWatch, Splunk, or Azure Monitor, organizations can track suspicious activities and respond swiftly to potential breaches.

4. Ensuring Compliance with GDPR and HIPAA

Adhering to regulations like GDPR and HIPAA is essential for organizations that process personal or health-related data. Compliance involves implementing strict data governance policies and ensuring transparency in how data is collected, processed, and shared.

Flowchart: Compliance Workflow for GDPR/HIPAA

(A flowchart showing steps to comply with GDPR and HIPAA regulations, including data collection consent, anonymization, and secure storage processes.)



This flowchart outlines the basic steps to ensure compliance with GDPR and HIPAA, focusing on data collection, storage, user consent, encryption, monitoring, and handling user requests or breaches.

CONCLUSION

The secure management of data within Business Intelligence platforms is crucial to protect sensitive information and ensure regulatory compliance. By integrating best practices such as role-based access control, encryption, continuous monitoring, and adherence to legal frameworks, organizations can mitigate security risks. As regulations continue to evolve, businesses need to maintain a proactive approach to data governance and compliance.

REFERENCES

[1]. D. Smith, "Data Security in BI Platforms: Emerging Threats and Countermeasures," Journal of Data Security, vol. 10, no. 2, pp. 38-55, 2019.

[2]. European Union, "General Data Protection Regulation (GDPR)," 2016. [Online]. Available: https://gdpr.eu. [Accessed: Sept. 10, 2020].

[3]. National Institute of Standards and Technology (NIST), "NIST Special Publication 800-57: Recommendation for Key Management," 2016. [Online]. Available: https://csrc.nist.gov. [Accessed: Sept. 10, 2020].

[4]. Health and Human Services (HHS), "HIPAA Privacy Rule," 2019. [Online]. Available: https://www.hhs.gov/hipaa. [Accessed: Sept. 10, 2020].

[5]. A. Brown, "Role-Based Access Control in Business Intelligence Systems," Proceedings of the International Conference on Information Security and Privacy, 2018, pp. 215-230.