

Report Proposal

Group – 5

Group Members:

- Francisco Vieira Moreira | 202007205
- Hassan Mustafa Shoaib Burney | 202100805
- Olusegun Adebayo Opesanwo | 202400363
- Marcia Souza | 202007416

Course Unit

Information Security

Professor

Jose Manuel de Magalhães Cruz

Title/Theme:

Security Strategies.

Sub-Title:

Security Strategies in Cloud by Cloud Access Security Brokers (CASB) tool using Integrated Machine Learning (ML) Techniques

Table of Content:

• Abstract	Marcia
• List of Tables and Figures	Marcia
• Background	Olusegun
• Introduction	Olusegun
• Literature Review	Francisco
• Analysis and Discussion	Hassan
• Results and Evaluation	Francisco
• Limitation	Hassan
• Conclusion	Marcia
• References	Marcia

Specifications:

In this report, by using search limiters, only selected literature reviews and research papers published between the years 2020 to 2024 are offered, to examine several aspects of cloud and cloud security related tools. This report offers to deliver deep understanding about cloud such as its scalability and flexibility, including cloud devoted security tool “CASB Solutions” a useful technique against data breaches, unauthorized access and compliance risks correspondingly.

Moreover, this report is planned in a way to cover all the possible areas of cloud security tool CASB including its functionalities such as Data Encryption, Access Control, Threat Detection and Compliance Monitoring. Similarly, how CASB improves cloud security posture? What are the CASB benefits and limitations? And lastly, CASB adherence to implement best practices and standardized frameworks respectively.

Likewise, CASB implementation model powered by User Entity and Behavior Analysis (UEBA) using Machine Learning (ML) and Statistical Modeling (SM) is also included in this report, that can provide wide range of information about several integrated machine learning (ML) tools to handle multiple security concerns in cloud system including, Data Breaches, Data Loss, Weak Identity, Insecure APIs and System Vulnerabilities etc. Similarly, CASB approach to integrate with other security controls such as: Security Information and Event Management (SIEM), Firewalls, Data Loss Prevention (DLP), Endpoint Management, Encryption and Authentication are also examined and included in this report.

In the last, CASB different deployment modes, CASB pillars, CASB top solutions, Comparison of CASB solutions from industry leaders, CASB role in order to discover Shadow IT, Anomaly Detection and last of all, a CASB solution using Principal Component Analysis (PCA) technique to conduct real time dataset analysis to examine and categorized risks are also provided in this report respectively.

Findings:

This report will provide overview of CASB solutions mentioned by different industry leaders in which its key features, deployment options, integrations, scalability and challenges are mentioned. Similarly, how CASB’s “Pillars of CASB” help to secure cloud? Different types of CASB deployment modes, CASB implementation model using integrated ML techniques and lastly, CASB based project using Principal Component Analysis (PCA) system to obtain scaled down data set to perform accurate analysis to detect threats is also included in this report..

Recommendations

A Cloud Access Security Broker (CASB) provides essential security controls for cloud services, ensuring data protection, compliance, and threat detection. It acts as a crucial intermediary,

enabling organizations to securely leverage cloud applications while maintaining visibility and control over sensitive data. To conclude, it can be stated that this report can provide deep knowledge about Cloud Access Security Brokers (CASB) and its technicalities in order to improve cloud security against threats and malicious attacks accordingly.

Conclusion

A CASB is vital for securing cloud environments, offering solid data protection and compliance solutions by bridging the gap between on-premises security and cloud services to enhance visibility and control over sensitive information in the system.