

**SEMESTER ONE 2024/2025 ACADEMIC YEAR**

**SCHOOL COMPUTING AND IMFORMATICS TECHNOLOGY**

**DEPARTMENT OF COMPUTER SCIENCE**

**MASTER OF SCIENCE IN COMPUTER SCIENCE**

**MCS 7102**

**DATA SECURITY AND PRIVACY**

**USAGE CONTROL ON CLOUD SYSTEMS**

**AMPEIRE EDGAR**

**2024/HD05/21915U**

**2400721915**

Usage control on cloud systems refers to the enforcement of policies governing how data and resources are used after they have been accessed. This concept extends traditional access control, which focuses on whether a subject can access a resource, to a broader model that continues to regulate actions during and after access.

Recent advancements have emphasized the need for continuous monitoring and real-time decision-making to enforce policies, ensuring that permissions can be dynamically revoked based on evolving contexts, such as time, location, or user behavior.

The key aspects of usage control are mutability, continuity and decision re-evaluation.

**Mutability** refers to the ability to adapt and change policies dynamically during the system’s runtime.

**Continuity**: The ability to enforce policies continuously over the duration of the usage session.

**Decision Re-evaluation**: Continuous re-evaluation of access decisions, even after initial access is granted, based on contextual factors.

**Usage Control Models.**

1. The UCONABC model that consists of three key factors, Authorizations, Obligations and Conditions.

**Authorizations (A):** Whether the subject is authorized to access the resource.

**Obligations (B):** Certain actions that must be taken before or during the usage of a resource.

**Conditions (C):** Environmental factors such as time, location, or system status that must be satisfied for usage to continue.

1. The Attribute-Based Access Control in which access decisions are based on attributes of the users, resources, and environmental conditions.
2. Role-Based Access Control Extensions in which the extensions allow for the enforcement of usage policies.

The enforcement of usage control in cloud systems relies on several techniques and technologies that ensure continuous monitoring and policy enforcement.

These include; -

1. Policy Enforcement Points responsible for enforcing usage control policies within the cloud system, where the points intercept access requests and evaluate them against the relevant policies and continue to monitor usage to ensure that it adheres to the set policies.
2. Policy decision points are logical entities that make decisions regarding whether access to a resource should be granted and evaluate requests based on the usage control policies, attributes of the users, and contextual information.
3. Continuous monitoring of data usage and behavior is a crucial part of enforcing usage control. Monitoring tools track user activity, ensuring that policies are followed, and alert administrators if policies are violated. Auditing logs provide a record of access and usage for compliance verification and security analysis.

Despite the benefits of usage control, its implementation in cloud systems has challenges;-

1. Ensuring usage control at scale, while maintaining performance and system efficiency, is complex.
2. Different cloud providers and systems may have different security and access control mechanisms. Achieving seamless interoperability between systems while maintaining consistent usage control is challenging
3. Usage control policies are often more complex than traditional access control policies, as they involve continuous re-evaluation based on multiple factors.

The Future of Usage Control.

The rise of Artificial Intelligence and Machine learning has created and will continue creating improved usage control mechanisms by learning from user behavior, automating the detection of policy violations, and dynamically adjusting policies based on trends and insights.

Zero Trust models, where every request to access a resource is verified regardless of its origin, can enhance usage control mechanisms.

**Conclusion**

As organizations increasingly rely on cloud computing, the need for robust usage control mechanisms becomes more pronounced. Usage control extends traditional access control models, offering dynamic, continuous enforcement of data usage policies in cloud environments. While the concept of usage control addresses many of the challenges associated with cloud data security and privacy, its implementation poses significant technical and operational hurdles. Future innovations in AI, blockchain, and decentralized policy enforcement are likely to enhance the effectiveness of usage control systems in cloud computing.

**References**

1. Park, J., & Sandhu, R. (2004). The UCONABC usage control model. *ACM Transactions on Information and System Security (TISSEC)*.
2. Goyal, V., et al. (2017). Fine-grained usage control in the cloud. *IEEE Transactions on Cloud Computing*.
3. Zhang, X., & Bhavani, T. (2018). Attribute-based usage control for cloud computing. *Journal of Cloud Computing: Advances, Systems, and Applications*.
4. Cuppens, N., & Miege, A. (2008). Enforcement of security policies in cloud systems. *Computers & Security*.
5. M. D. Dikaiakos, D. Katsaros, P. Mehra, G. Pallis, and A. Vakali. Cloud computing: distributed internet computing for IT and scientific Internet Computing, IEEE, 13(5):10–13, 2009.
6. D.-G. Feng, M. Zhang, Y. Zhang, and Z. Xu. Study on cloud computing security. Journal of software, 22(1):71–83, 2011.