CSCI 530: Security Systems
Research Paper Proposal: Due Date: 30 September 2024
Name: Anne Sai Venkata Naga Saketh
USC Email: annes@usc.edu
USC ID: 3725520208

Research Proposal Topic: Authorization and Policy Management

Title: *Revolutionizing Access Control: Advanced Authorization for the Digital Age*

In this research proposal, I am exploring the scalability of the latest systems for access control, with a significant focus on Amazon's Cedar system and Google's Zanzibar models. Google's global architecture enables fine-grained access control, making it one of the better solutions for public cloud systems and distributed environments. Similarly, Amazon has introduced a new language to externalize controlling access from the actual application code; it supports other access control models like RBAC, ABAC, and ReBAC with a major focus on policy analysis, policy audit, and maintenance. My study aims to delve into the core mechanism and challenges of maintaining real-time authorization performance.

I aim to address the issues of achieving a low-latency policy permission check in cloud environments while ensuring policy consistency and security are maintained. My study has the potential to significantly enhance the robustness and security of cloud environments. Additionally, I also plan to incorporate Machine learning techniques to predict the access control patterns and automate the policy modifications.

In my research paper, I would like to address the limitations of the traditional access control models like RBAC and ACLs, the issues related to Google's Zanzibar architecture and Amazon's Cedar architecture, The security vs the performance trade-off while scaling these systems to public cloud environments, and the issues with granular specification of the access control policies.

In the future, I plan to explore How using Machine learning to predict user access patterns and behaviors, and thereby modifying the user permissions on the fly, will be beneficial. How can cross-cloud/platform compatibility help organizations maintain a single source of truth to control all access management? What are the mechanisms to detect and recover from security breaches, and How do we achieve low latency in large-scale systems?

References and Citations:

1. Cutler, Joseph W., et al. "Cedar: A New Language for Expressive, Fast, Safe, and Analyzable Authorization." Proceedings of the ACM on Programming Languages.OOPSLA1 (2024): 670-697
2. authzed-spicedb 2024. spicedb. https://github.com/authzed/spicedb. Open Source, Google Zanzibar-inspired permissions database to enable fine-grained access control for customer applications
3. aws-iam 2024. Access Management - AWS Identity and Access Management (IAM). https://aws.amazon.com/iam/
4. azure-policy 2024. Azure policy documentation. https://learn.microsoft.com/en-us/azure/governance/policy/
5. Authentication and Security Services. http://pubs.opengroup.org/onlinepubs/9668899. Accessed: 2019-04-16