Cache de Atributos Oportunista: Melhorando a eficiência do ABAC com o uso de uma política de distribuição de identidades em redes multinível para névoas computacionais

Airton Ribeiro de Moura Gomes Filho[1], **Edelberto Franco Silva**[1], **Alex Borges Vieira**[1]

[1]Depto. de Ciência da Computação – Universidade Federal de Juiz de Fora (UFJF)
{armgfilho, edelberto}@ice.ufjf.br, alex.borges@ufjf.edu.br

Abstract. *Attribute-based Access Control (ABAC) is one of the most popular access control methods. Despite its popularity, a few works address attribute management in the Internet of Things (IoT). Most of the attributes needed for an IoT policy evaluation come from an external source. Therefore, managing attributes across the network requires communication between the policy decision point and the policy information point for each attribute, impacting ABAC performance. Attribute caches can mitigate this problem. This work presents a method that predicts attribute requests and anticipates the attribute placement closer to the requester. Based on simulations with a real dataset, the proposed method reduces above* 80% *the number of requests in the cloud using attributes' caches and delivers up to* 55% *of the attributes in the first hop.*

Resumo. *O Controle de Acesso Baseado em Atributos (Attribute-based Access Control - ABAC) é um dos métodos de controle de acesso mais populares. Apesar de sua popularidade, apenas alguns trabalhos abordam o gerenciamento de atributos na Internet das Coisas (Internet of Health Things - IoT). A maioria dos atributos necessários para uma avaliação de política em IoT vem de uma fonte externa. Portanto, o gerenciamento de atributos através da rede requer comunicação entre o ponto de decisão da política e o ponto de informação da política para cada atributo, impactando o desempenho do ABAC. Os caches de atributos podem atenuar esse problema. Este trabalho apresenta um método que prevê solicitações de atributo e antecipa o posicionamento do atributo mais próximo do solicitante. Com simulações em uma base de dados real, o método proposto reduziu acima de* 80% *o número de requisições na nuvem utilizando os atributos nos caches e entrega até* 55% *dos atributos no primeiro salto.*

1. Introdução

As redes móveis e sem fio são um exemplo de tecnologia que teve sucesso ao auxiliar na cobertura e expansão das redes. E um dos exemplos de maior abrangência e adoção são as redes sem fio locais (*Wireless Local Area Network* - WLAN, e *Wireless Fidelity* - Wi-Fi da *Wi-Fi Alliance*) apoiadas no padrão IEEE 802.11. Porém, é importante considerar como o acesso a esse tipo de rede e a seus serviços são garantidos sob a perspectiva da segurança da informação. Assim, para garantir um acesso mais seguro a tais serviços e ambientes, deve-se levar em consideração requisitos como a Autenticação e a Autorização (A&A) [Trnka et al. 2018]. Conforme [Silva et al. 2018], os processos relacionados à A&A estão intimamente ligados à Gestão de Identidade (GId ou IdM - *Identity Management*), e são utilizados para garantir o uso seguro de recursos e definir os ciclos de vida de uma identidade e a composição delas, com seus atributos.

Para que a A&A possa ser realizada em ambientes de larga escala sem fio é necessário considerar alguns pontos cruciais. Em relação à autenticação e autorização, usualmente, cria-se políticas de acesso que consideram dados relacionados à identidade do objeto, do ambiente e, principalmente, da identidade do usuário para determinar se um acesso é ou não válido [Ranjith and Srinivasan 2013]. Este mecanismo é conhecido como parte da A&A provendo o suporte a métodos de controle de acesso ao ambiente. Porém, devido ao possível atraso na recuperação das identidades e seus atributos, os atuais processos de A&A podem não ser capazes de proporcionar a sensação de transparência no acesso a serviços pelo usuário, necessário para diversas aplicações em redes móveis [Hu et al. 2013]. Logo, é de grande importância avaliar e propor técnicas que reduzam o tempo de recuperação dessas identidades a fim de que o processo de A&A ocorra eficientemente.

Neste trabalho, apresentaremos a possibilidade da aplicação de políticas de *cache* de identidade sob o conceito de névoa computacional, a fim de avaliar o ganho em relação à redução de número de saltos, e consequentemente, redução da latência na recuperação da identidade. Tal redução de latência representa um melhor desempenho para respostas em tomadas de decisões em processos de A&A como um todo, como comentado anteriormente. A fim de mostrar a aplicabilidade da proposta, sugerimos uma nova política de *cache* de identidade baseada na predição de mobilidade do usuário.

Atualmente há atraso no processo de autenticação e autorização, dado que os objetos necessários para identificação dos usuários estão distantes dos pontos de acesso. Em geral, tais dados estão na nuvem computacional, o que inviabiliza a aplicação, por exemplo, do controle de acesso em ambientes dinâmicos e com requisitos temporais de recuperação dos atributos. Nosso objetivo é explorar a computação em névoa para diminuir a latência dos processos de autenticação e autorização ao utilizar cache de atributos das identidades. A arquitetura em névoa utilizá de políticas de replicações e substituições para distribuir os atributos reativamente e proativamente. Adaptar o modelo de controle de acesso para permitir que aplicações com requisitos temporais utilizem os benefícios dos sistemas de Gestão de Identidades em ambientes de rede sem fio.

Como contribuições, temos a proposta e validação de uma arquitetura para ambiente de névoa computacional com políticas de replicação e substituição de identidade validado sob dados de uma rede real de uma universidade. No trabalho também geramos contribuições como a caracterização dos acessos, à rede sem fio acadêmica, realizados por esses usuários e identificamos seus padrões de mobilidade. Propomos e validamos uma política de replicação oportunista proativa com utilização de aprendizado de máquina, a fim de considerar as características de mobilidade dos usuários para tomada de decisão na replicação e substituição de identidade.

2. Trabalhos Relacionados

O problema da ineficiência dos métodos A&A para recuperação das identidades foi primeiramente apresentado por [Hu et al. 2013], ao relatar que o ABAC pode perder desempenho quando da recuperação dos objetos referentes à essa identidade, como no caso dos atributos. Em seu trabalho, [Hu et al. 2013] descreve os problemas de desempenho do ABAC, e mostra que o *cache* de atributos pode aliviar esses problemas. Ainda no trabalho de [Hu et al. 2013], os autores argumentaram que quando um número mínimo de atributos é armazenado em *cache*, ocorre uma simplificação da atualização e, consequentemente,

incremento sob a ótica da segurança. Isso torna o controle de acesso viável para diversos casos de uso de IoT, principalmente onde o desempenho é um requisito obrigatório. Desde então, outros trabalhos possuem como alvo essa ineficiência na recuperação das identidades, como em um dos primeiros trabalhos na área, apresentado por [Hu et al. 2015], onde sugere-se o uso de *caches* de identidades para se alcançar o desafio apresentado.

Em [Liu et al. 2018] foi apresentado um mecanismo de *caching* multinível baseado em análises estatísticas de um *campus* universitário. Os autores propuseram um sistema de três camadas de A&A, sendo as camadas: de Sistema de Autenticação de Usuários, Sistemas de Controle de Acesso e Função de Controle de Acesso. Nele, dois mecanismos de *cache* foram desenvolvidos para otimizar o tempo de recuperação das identidades. Ainda que eficiente em se realizar o que se propõe, esse trabalho está limitado para o modelo de autorização RBAC, que é definido como um modelo já datado e que não oferece uma autorização granular.

Em [Gómez-Cárdenas et al. 2018] se propôs uma arquitetura névoa-nuvem, mostrando seus benefícios para os métodos de controle de acesso. Para reduzir o tempo de recuperação, os autores fragmentam os atributos em dados minúsculos e usam os nós de névoa como dispositivos agregados para aproximar os atributos do ponto onde as políticas são avaliadas e os atributos são necessários. Seus resultados mostraram que o uso de nós de névoa para armazenar os atributos impacta positivamente no desempenho do método de controle de acesso. No entanto, os autores concluíram que os atributos devem ser colocados em pontos estratégicos da rede para atenderem as diversas solicitações de atributos.

No trabalho de [Castro et al. 2019] são apresentadas modificações necessárias em uma arquitetura IoT para agilizar a avaliação de políticas de controle de acesso. Os autores propõem um sistema de controle de acesso híbrido, que avalia parcialmente as políticas nos dispositivos IoT, além de um mecanismo de *cache* de políticas. Eles argumentaram que os *gateways* estão presentes na maioria das soluções de IoT para mediar a comunicação entre o usuário e seus aplicativos que possuem vários objetos inteligentes. Portanto, os *gateways* podem armazenar chaves de acessos e processar políticas de acesso devido ao seu poder computacional e de memória. No entanto, embora o trabalho tenha se concentrado no armazenamento em *cache* e na distribuição de políticas, os autores não discutiram ou investigaram o custo relacionado ao armazenamento e recuperação dos atributos necessários para aplicação das políticas.

No trabalho de [Siebach and Giboney 2021] é apresentada uma nova arquitetura para A&A com simplificação do processo de autorização. Os autores propõem proteger os dados dentro do domínio da rede de uma forma mais eficiente, oferecendo mais controle sobre o acesso aos dados. O ganho real da arquitetura pode ser visto como a possibilidade de mudar as tecnologias dentro do domínio sem precisar reescrever toda a lógica de A&A. Além disso o domínio pode usar atributos aos quais são controlados e mantidos por outros sistemas, sem precisar conhecer a implementação de terceiros. Em nosso trabalho não foi proposto uma mudança na arquitetura como no [Siebach and Giboney 2021], porém foram utilizados conceitos parecidos ao propor que a entidade Ponto de Decisão e Ponto de Informação, do XACML, atuem dentro dos nós da rede.

Em [Cremonezi et al. 2019] propõe o uso de armazenamento nos nós da rede usando identidades como serviços. Assim, os objetos são persistidos por meio de políticas

de *cache*. Foi avaliado o impacto na distribuição em diferentes capacidades de armazenamento e comprovou-se que algoritmos probabilísticos possuem, em geral, um desempenho melhor que os demais. É importante destacar que o trabalho de [Cremonezi et al. 2019] deu origem a pesquisa aqui apresentada, onde identificou-se a necessidade de avaliar com maior profundidade algoritmos de replicações e substituições.

Como forma de deixar mais clara as contribuições deste trabalho em relação ao estado da arte, apresentamos a tabela a seguir. A Tabela 1 sintetiza uma comparação entre os trabalhos relacionados e a pesquisa desenvolvida. Todos os trabalhos são baseados em redes hierárquicas, exceto em [Hu et al. 2013] e em [Hu et al. 2015], onde não há requisito de uma estrutura de rede para ser implementado. Todos os trabalhos sugerem, ou usam, algum sistema de persistência de dados em formato de *cache*. A maioria dos trabalhos usa o ABAC como método de controle de acesso. Alguns trabalhos relacionados não realizaram avaliações com experimentações, apresentando apenas uma visão teórica sobre as *caches* de atributos. Os trabalhos que avaliaram suas propostas com auxílio de experimentos, ou usaram a base de dados simulada, ou não foi informada a origem dos dados. Desta forma, essa pesquisa se difere das demais ao realizar comparações com vários métodos de substituições e por utilizar uma base de dados com comportamento real utilizando *logs* de acesso de controladoras sem fio de um ambiente institucional.

Tabela 1. Comparação dos trabalhos relacionados.

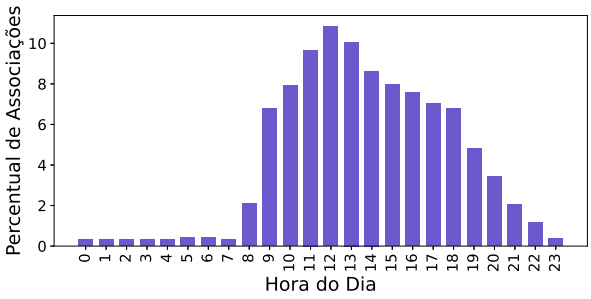
Trabalho	Rede Hierárquica	Cache	Método de Controle de Acesso	Políticas Distribuições e Substituições	Avaliação	Base de dados
Hu et al. (2013)	Não informado	Sugere	ABAC	-	-	-
Hu et al. (2015)	Não informado	Sugere	ABAC	-	-	-
Liu et al. (2018)	Sim	Políticas de Grupos e de Papel	RBAC	Baseado em Grupos e Papel	-	-
Gómez-Cárdenas et al. (2018)	Sim	Sim, fragmentos das IDs	ABAC	Não informado	Sim, simulador	Sem informação se real ou simulado
Castro et al. (2019)	Sim	Sim, contexto dos usuários	ABAC	Não informado	Sim, testbed	Simulado
Siebach and Giboney (2021)	Sim	Sim, IDs autorizados	ABAC	Não informado	-	-
Cremonezi et al. (2019)	Sim	Sim, IDs autorizados	-	LRU, FIFO, RR, LCE, LCD, Probabilístico 70% e 30%	Sim, simulador	Simulado
Esta Pesquisa	Sim	Sim, IDs autorizados	ABAC	LCE, LCD, LEAF, LRU, FIFO, RR, SLRU, SProt	Sim, simulador	Real

3. Resultados Obtidos

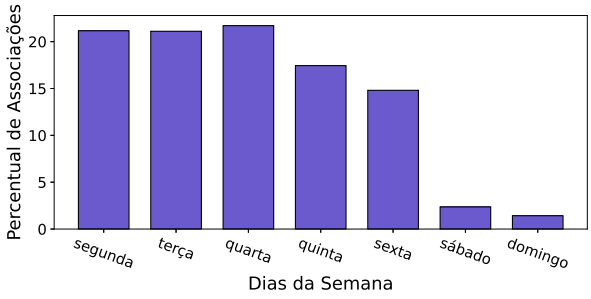
Os resultados obtidos com esse trabalho foram a caracterização da base de dados utilizada, a proposta de utilização de *caches* oportunistas proativa e uma nova política de *cache* com o uso de aprendizado de máquina.

3.1. Caracterização dos Dados

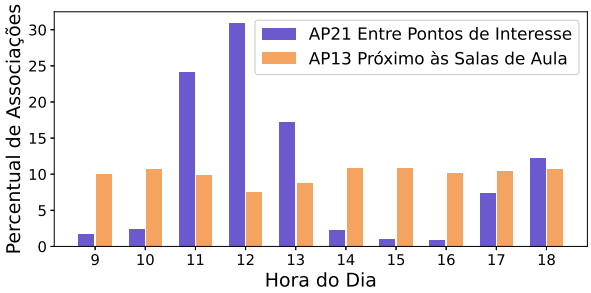
Foi realizado um rastreamento do mecanismo de autorização da Universidade Federal de Juiz de Fora por um período de quatro meses, em 108 APs. Foram monitorados 36 mil usuários únicos que fizeram 14,2 milhões de solicitações de acesso durante no período. A fim de respeitar a Lei Geral de Proteção de Dados (LGPD)[1], os dados nominais dos usuários foram anonimizados nessa etapa de conversão, ficando irreversível sua associação aos dados reais. Foi examinado o comportamento para identificar os horários de picos do sistema. A Figura 1a mostra o número percentual de solicitações dos acessos ao longo do dia. A maior parte dos acessos ocorre entre 9h e 18h. Como 80% das solicitações de acesso ocorrendo nessa janela de tempo. A frequência de requisições da rede durante os dias da semana estão na Figura 1b. Com esse gráfico fica evidente que os dias úteis, de segunda a sexta-feira, são os de maiores utilizações dos recursos da rede e correspondem a 96% das requisições.



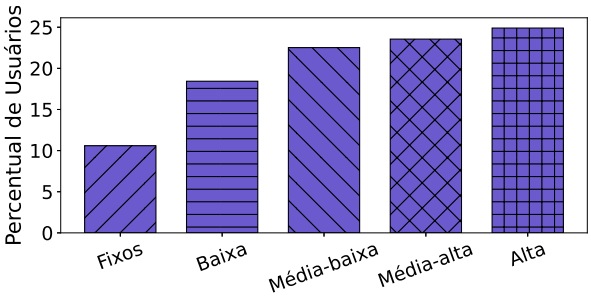
(a) Requisições por hora.



(b) Requisições por dias da semana.



(c) Comportamento de mobilidade.



(d) Perfil de mobilidade.

Figura 1. Caracterização dos Dados

A Figura 1c mostra o comportamento de conexões em dois APs diferentes. O primeiro, AP21, é uma rota entre dois pontos relevantes de interesse da universidade, esse

[1] http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm

AP apresenta um comportamento considerado mais estável e esperado, com um padrão recorrente quanto ao número de usuários conectados e aos os horários de uso. Para o segundo AP, o AP13, ele está localizado próximo às salas de aula e laboratórios, o que significa que este AP registra a atividade de alguns usuários e permanecem mais tempo conectados, e seus picos de carga correspondem à programação de aulas.

A Figura 1d é uma caracterização dos padrões de mobilidade encontrado nos acessos, a imagem ilustra quantos APs um usuário conecta durante sua vida útil. Usamos essa distribuição para rastrear os perfis de mobilidade. Conforme a Figura 1d, cerca de 10% dos usuários do *campus* se conectam a apenas um único AP. Esse grupo foi marcado como "usuários fixos". O segundo grupo, conecta-se a um número de 2 a 4 APs e o método rotulou esses usuários como de "baixa mobilidade". O terceiro grupo apresenta usuários que se conectam por 5 a 12 APs e foram rotulados como usuários de "mobilidade média-baixa". O quarto grupo tem usuários com movimentos mais confusos e difíceis de determinar e foram classificados como usuários de "mobilidade média-alta" e os usuários se conectam, em média, de 13 a 28 APs. Finalmente, os usuários que apresentam um padrão de acesso quase caótico conectando pelo menos por 29 APs no último grupo. Neste último grupo, está claro que todo o sistema deve contar com um algoritmo de previsão de mobilidade altamente complexo e preciso para atender a esses usuários e entregar os atributos de forma eficiente.

3.2. Cache de Atributos Oportunista

Neste trabalho, nosso foco foi melhorar a qualidade da comunicação das macro estruturas da arquitetura XACML. Logo, para abstrair a comunicação entre o Ponto de Aplicação de Políticas e o Ponto de Decisão da Política, foi considerado que ambos elementos funcionam em uma única estrutura física, os nós da névoa. A proposta aqui não é juntar e fundir as entidades modificando a arquitetura do XACML, mas que elas funcionem lado a lado numa mesma estrutura que são os nós da névoa. Visto que a maioria dos nós de névoa tem capacidade de computação e armazenamento. Porém, a capacidade de armazenamento sendo reduzida ela só poderá guardar apenas um subconjunto de atributos/objetos.

O cenário abordado neste trabalho é uma aplicação IoT em execução em uma grande área. O aplicativo IoT espera muitos usuários e dispositivos móveis distribuídos em toda a área, solicitando acesso a vários objetos em qualquer local. Esta aplicação requer autorização contínua e constante dos usuários. Para manter essa autorização contínua, vale a pena reduzir o tempo de avaliação da política para manter o impacto da latência da avaliação o mínimo possível. Para resolver isso, utilizaria vários nós de névoa e os distribuiria na em sua área geográfica para atuar como *caches* de atributos, funcionando como fonte de atributos além da nuvem e mais próximos ao usuário.

O problema consiste em encontrar o subconjunto de atributos para armazenar em cada nó de névoa. A *cache* de atributo oportunista reativo é uma abordagem que replica os atributos com base apenas na resposta local a uma solicitação de atributo. A Figura 2 ilustra uma solicitação de acesso que ocorre no solicitante de nó r. Assim que a solicitação de atributo chega ao parceiro p que contém os atributos, p envia de volta ao solicitante os atributos de que precisa. Como esta resposta de atributo atinge vários nós no caminho de volta para o solicitante, cada nó nesta rota tem a oportunidade de replicar esses atributos. Portanto, de acordo com este *cache* de atributo oportunista reativo, do primeiro ao último nó na rota, todo nó pode oportunamente salvar uma cópia do atributo na *cache*.

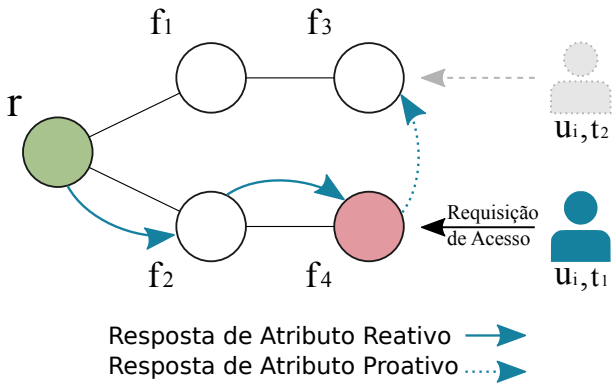


Figura 2. Modelos requisição-resposta.

O sistema de *Cache* de Atributos Oportunista Proativo tem como principal objetivo encontrar um subconjunto de atributos a serem armazenados para minimizar o número de perdas na operação de decisão de política. Se a abordagem prever onde ocorrerá a solicitação subsequente, os atributos necessários podem ser replicados proativamente naquele local, reduzindo a taxa de falhas. Um algoritmo de previsão de mobilidade eficaz é essencial para determinar a posição da solicitação subsequente.

Para exemplificar esta abordagem, considere uma rede com quatro nós de névoa (f_1, f_2, f_3, f_4), um servidor de nuvem no nó raiz r e um usuário u_1, como representado na Figura 2. Supondo que no momento t_1, o usuário u_1 solicite acesso em f_4, a solicitação de atributo flui do solicitante r para o parceiro p e volta, permitindo que todos os nós no caminho repliquem esses atributos. No entanto, como no instante t_2, esse mesmo usuário solicita acesso ao nó na névoa f_3, o método proposto replica proativamente os atributos para esse nó na névoa se ele não contiver esse atributo. Assim, no instante de tempo t_2, é possível fazer a solicitação de acesso (e a eventual solicitação de atributo subsequente que pode originar) com $d = 0$ em relação distância entre a requisição resposta da Figura 2.

3.3. Replicação Segmentado com Predição

A nova política proposta nesse trabalho é uma variação da política de substituição conhecida como SLRU, ou Menos Usado Recentemente Segmentado. A SLRU é uma variação do LRU clássico, ela separa a *cache* em dois segmentos – um de oportunidade e outro segmento de protegidos. Denominamos de "Menos Usado Recentemente Segmentado com Predição" com a sigla SPROT. A SPROT é uma nova política, e uma das contribuições desse trabalho. Ela usa conceitos do modelo SLRU com o espaço protegido para os objetos que passaram pela predição de mobilidade. Com a *cache* segmentada em dois espaços, a abordagem proativa aciona o modelo de predição para adicionar a identidade prevista no segmento protegido, dessa forma esse objeto tem uma oportunidade maior de ser reutilizado numa futura solicitação da identidade.

4. Contribuições Acadêmicas

Neste trabalho foram exploradas diversas estratégias de distribuição e substituição do espaço de armazenamento temporário de objetos. Foram utilizados os dados de um sistema de A&A de uma grande rede sem fio para avaliar as políticas propostas. Foram conduzidas as investigações do comportamento dos usuários, das combinações de políticas de

replicação e substituição, e analisados os impactos práticos por meio de algumas métricas a fim de propor melhorias no cenário nuvem-névoa para recuperação de atributos de identidade. O método apresentado incrementa o desempenho da recuperação dos atributos de identidade no ABAC, adaptado a um sistema baseado em névoa.

As contribuições desse estudo foram publicadas em conferência internacional do IEEE *International Conference on Communications* 2021 e em simpósio nacional de importante relevância no tema, como o Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais 2021. Ainda no SBSeg 2021 fomos premiados como melhor artigo na trilha principal. Esse estudo também criou a oportunidade de apresentar em *workshop* como o XI Workshop de Gestão de Identidades Digitais trazendo a comunidade acadêmica para a discussão sobre o assunto. Toda a pesquisa foi sintetizada em uma publicação do periódico *Computer Networks* que foi divulgado em abril de 2022.

Referências

Castro, T. O., Caitité, V. G., Macedo, D. F., and dos Santos, A. L. (2019). Casa-iot: Scalable and context-aware iot access control supporting multiple users. *International Journal of Network Management*, 29(5):e2084.

Cremonezi, B., Nogueira, M., dos Santos, A. L., Vieira, A. B., and Nacif, J. A. M. (2019). Um sistema multinível de distribuição de identidades em névoas computacionais. In *Anais do XXXVII Simpósio Brasileiro de Redes de Computadores e Sistemas Distribuídos*, pages 543–555. SBC.

Gómez-Cárdenas, A., Masip-Bruin, X., Marin-Tordera, E., Kahvazadeh, S., and Garcia, J. (2018). A resource identity management strategy for combined fog-to-cloud systems. In *2018 IEEE 19th International Symposium on"A World of Wireless, Mobile and Multimedia Networks"(WoWMoM)*, pages 01–06. IEEE.

Hu, V., Ferraiolo, D. F., Kuhn, D. R., Kacker, R. N., and Lei, Y. (2015). Implementing and managing policy rules in attribute based access control. In *2015 IEEE International Conference on Information Reuse and Integration*, pages 518–525. IEEE.

Hu, V. C., Ferraiolo, D., Kuhn, R., Friedman, A. R., Lang, A. J., Cogdell, M. M., Schnitzer, A., Sandlin, K., Miller, R., Scarfone, K., et al. (2013). Guide to attribute based access control (abac) definition and considerations (draft). *Special Publication*.

Liu, B., Yang, Y., and Zhou, Z. (2018). Research on hybrid access control strategy for smart campus platform. In *2018 IEEE 3rd Advanced Information Technology, Electronic and Automation Control Conference (IAEAC)*, pages 342–346. IEEE.

Ranjith, D. and Srinivasan, J. (2013). Identity security using authentication and authorization in cloud computing. *International Journal of Computer & Organization Trends*, 3(4):122–129.

Siebach, J. and Giboney, J. (2021). The abacus: A new architecture for policy-based authorization. In *Proceedings of the 54th Hawaii International Conference on System Sciences*, page 7055.

Silva, E. F., Muchaluat-Saade, D. C., and Fernandes, N. C. (2018). Across: A generic framework for attribute-based access control with distributed policies for virtual organizations. *Future Generation Computer Systems*, 78:1–17.

Trnka, M., Cerny, T., and Stickney, N. (2018). Survey of authentication and authorization for the internet of things. *Security and Communication Networks*, 2018.