International Journal of All Research Education and Scientific Methods (IJARESM),
ISSN: 2455-6211, Volume 13, Issue 6, June-2025, Available online at: www.ijaresm.com

Preventing Unauthorized Access with Pre-IAM IP Verification in Cloud Environments

B. Nirmala[1], P. Arun[2], T. Lahari[3], G. Prabhath Vishnu[4], Sk. Asif[5], Bhaskar Das[6]

[1,2,3,4,5]Student, Hyderabad Institute of Technology and Management, Hyderabad, India
[6]Associate Professor, Hyderabad Institute of Technology and Management, Hyderabad, India

----------**********----------

ABSTRACT

As we further integrate cloud services into our infrastructure, the need to authenticate access to these services prior to passing through traditional IAM verification requires attention. This project offers an access control module based on source IP verification that serves as a pre-IAM security layer. By rejecting requests from predefined untrusted IP address ranges, the system bypasses trusted IAM systems, reduces risks like DDoS attacks, and lowers overall risk exposure. This module can be integrated in an effortless manner within existing frameworks of clouds making it a reasonable economical investment that improves protection whilst aiding compliance with industry standards.

Keywords: Cloud Security, IP-Based Access Control, Pre-IAM Authentication, Source IP Verification, DDoS Mitigation

INTRODUCTION

The pervasiveness of cloud computing has completely transformed how organizations store, use, and manage data. Cloud platforms offer scalability, flexibility, and cost-efficiency, making them fundamental to modern enterprise operations [1]. Despite these advantages, transitioning from traditional infrastructure to cloud-based environments introduces new responsibilities for ensuring a secure environment, particularly around access control. One of the most significant challenges is protecting cloud resources so that only authorized users can access them—especially at the earliest stage of connection, before any Identity and Access Management (IAM) systems are activated [2].

IAM systems are widely employed in both traditional and cloud contexts to manage digital identities, authenticate users, and enforce access policies [3]. While effective at processing and regulating access requests, IAM systems primarily operate reactively—triggering only after a request is made. This reactive nature leaves a vulnerable window before authentication, where malicious users or bots might exploit endpoints. Threats like Distributed Denial of Service (DDoS) attacks, brute-force login attempts, or inadvertent policy exposure due to misconfigured IAM endpoints remain critical concerns [4]. Consequently, the pre-IAM phase emerges as a high-risk zone that demands additional protection.

To mitigate these security gaps, this project proposes an IP-Based Access Control Module for Pre-IAM Cloud Resource Authentication. This proactive security solution filters incoming requests based on predefined, trusted IP ranges before passing them to the IAM system. Unauthorized requests are blocked at the gateway level, reducing the cloud environment's attack surface and alleviating load on IAM infrastructure [5]. The proposed module supports dynamic IP whitelisting, real-time monitoring, and integrates with major cloud platforms such as AWS, Azure, and Google Cloud [6]. By implementing IP-based filtering and network-level trust boundaries, organizations can improve compliance, prevent incidents, and strengthen their overall cloud security architecture through layered defense mechanisms.

LITERATURE REVIEW

Saharia, C., et al. (2022). *Photorealistic Text-to-Image Diffusion Models*. arXiv preprint arXiv:2207.12598. This paper proposes a cascaded diffusion model that generates high-quality images from textual descriptions by using multiple super-resolution stages and a strong text encoder. The model demonstrates zero-shot capabilities and produces photorealistic results without requiring task-specific fine-tuning. Ramesh, A., et al. (2022). *Hierarchical Text-Conditional Image Generation with CLIP Latents*. arXiv preprint arXiv:2204.06125. This work introduces DALL·E 2, which leverages CLIP

latents and a diffusion decoder to produce highly realistic images from text prompts. It also allows text-guided editing and inpainting, aligning visual output closely with the semantic intent of the text.

Nichol, A., et al. (2022). *GLIDE: Towards Photorealistic Image Generation and Editing with Text-Guided Diffusion Models*. arXiv preprint arXiv:2112.10741. GLIDE improves photorealistic text-to-image synthesis using classifier-free guidance. It excels in both creating and editing images with high visual quality, outperforming prior GAN models in consistency and diversity of generated content.

Rombach, R., et al. (2022). *High-Resolution Image Synthesis with Latent Diffusion Models*. Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition. This paper presents Stable Diffusion, a latent diffusion model that balances image fidelity and computational efficiency. By compressing image data into a latent space and using cross-attention mechanisms, it allows faster training and broader accessibility without sacrificing output quality.

Balaji, Y., et al. (2022). *Text2Human: Text-Driven Controllable Human Image Generation*. In Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition. Text2Human focuses on human image generation by combining textual inputs with pose guidance. It produces more accurate and controllable human figures that reflect the described clothing, posture, and appearance.

Chen, J., et al. (2020). *DF-GAN: Deep Fusion Generative Adversarial Networks for Text-to-Image Synthesis*. arXiv preprint arXiv:2008.05865. DF-GAN simplifies the architecture of text-to-image GANs while enhancing performance using Deep Fusion Blocks and a matching-aware loss function. It achieves better semantic alignment and visual fidelity with fewer parameters and training complexity.

Zhu, M., et al. (2019). *DM-GAN: Dynamic Memory Generative Adversarial Networks for Text-to-Image Synthesis*. In Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition. DM-GAN introduces a dynamic memory module that improves image generation by correcting and refining intermediate features in later stages, resulting in better alignment with text descriptions and reduced visual defects.

Collectively, these papers show a clear evolution from traditional GAN-based text-to-image synthesis toward more advanced and robust diffusion-based models. Early works like DF-GAN and DM-GAN focused on improving semantic-text alignment and structural realism, while recent diffusion models like GLIDE, DALL·E 2, and Stable Diffusion significantly enhance image quality, editing flexibility, and computational efficiency. The integration of CLIP embeddings, latent space optimization, and classifier-free guidance has led to more accurate and controllable image generation. Additionally, domain-specific innovations such as Text2Human demonstrate the adaptability of these methods for human-centric applications. Altogether, these advancements highlight the increasing power and potential of text-to-image synthesis technologies in a range of practical and creative contexts.

METHODOLOGY

To address the critical gap in pre-IAM authentication for cloud environments, the proposed solution implements an IP-Based Access Control Module designed to filter and validate requests before they reach the traditional IAM layer. The methodology for developing this module follows a structured approach consisting of the following phases

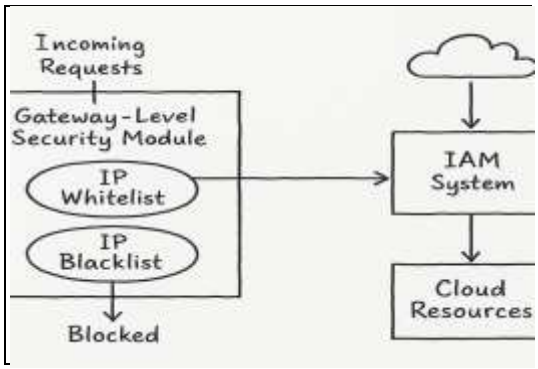

Fig1: Flow Chart

1. **System Design and Architecture**
   The system is architected to function as a gateway-level security module that intercepts all incoming requests to cloud resources. The design ensures compatibility with major cloud platforms such as AWS, Microsoft Azure, and Google Cloud. The module acts as a front-line barrier, performing initial IP verification before allowing requests to proceed to the IAM system. This layer adds a proactive defense mechanism that reduces unnecessary processing by IAM and mitigates risks from unauthorized access attempts.
2. **IP Whitelist and Blacklist Management**
   The core of the access control system relies on maintaining dynamic lists of trusted (whitelisted) and untrusted (blacklisted) IP address ranges. IP lists can be updated in real-time through an administrative interface or integration with threat intelligence services. Trusted IPs are identified based on organizational usage patterns, while known malicious or suspicious ranges are continuously blocked.
3. **Traffic Filtering Mechanism**
   Each incoming request is subjected to source IP verification. If the IP matches an entry in the whitelist, the request is forwarded to the IAM layer for further authentication. Requests originating from blacklisted IPs or those not recognized by the system are dropped immediately, effectively reducing the attack surface and preventing potential threats like DDoS attacks and brute force attempts.

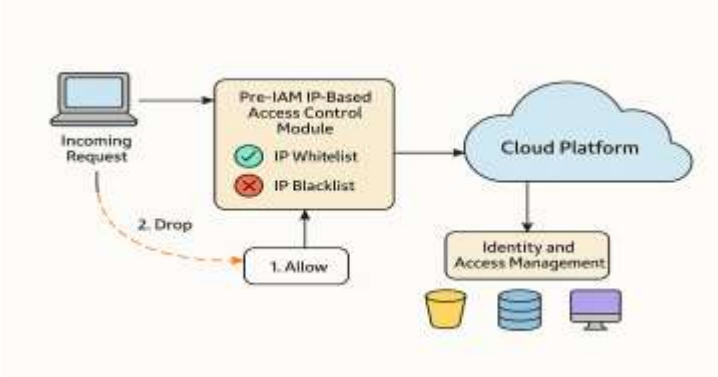

Fig 2: System Design and Architecture

4. **Cloud Integration and Platform-Agnostic Implementation**
   The module is implemented using cloud-native technologies such as AWS Lambda, API Gateway, Azure Functions, and Google Cloud Functions, ensuring seamless integration without disrupting existing workflows. The module uses Infrastructure as Code (IaC) for rapid deployment and scalability. It operates bi-directionally, meaning it can validate both inbound and outbound traffic based on source and destination IPs.
5. **Real-Time Monitoring and Logging**
   Logging mechanisms are built into the module to record and analyze incoming requests, blocked IPs, and traffic patterns. Real-time dashboards are provided for administrators to monitor activity and configure rules as needed. These logs support forensic analysis, policy refinement, and compliance auditing.
6. **Compliance and Security Alignment**
   The design of this module aligns with industry-standard security frameworks such as ISO/IEC 27001, NIST SP 800-53, and CIS Controls. It also supports integration with existing SIEM systems to enhance overall organizational threat detection and response capabilities.
7. **Testing and Validation**
   The module is validated using simulated attacks such as IP spoofing, DDoS, and unauthorized access scenarios. Performance is evaluated based on metrics including response time, accuracy of IP filtering, and reduction in IAM layer load. Comparisons are made against baseline IAM-only systems to assess the effectiveness of pre-authentication controls.

IMPLEMENTATION

In order to establish the feasibility and efficiency of the suggested IP-Based Access Control Module, a prototype was developed with Django and Python supported by a Google Cloud Platform (GCP) setup. The goal was to show how pre-IAM authentication can be used to filter incoming traffic before identity verification processes kick in, especially in the development and testing environment.

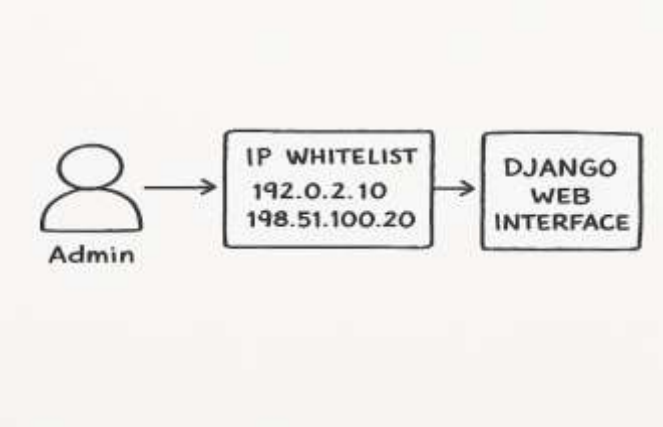

Fig3: Middleware Logic for IP Validation

The system architecture starts with incoming requests from the internet. These requests are intercepted initially by the Pre-IAM module, which acts as a gatekeeper. This module was created as a Django-based application that has administrative control over IP address permissions exclusively. It is the responsibility of team administrators to authorize user IPs only, so there is a controlled and auditable access flow. This mechanism comes especially handy during the pre-production or testing stages of application development where access to unwanted or outside influences needs to be kept at its minimum.
The inner logic is executed through Django middleware, which acts as the request interception layer. Upon receipt of a request by the middleware, the source IP is parsed and verified against a list of authorized IPs managed by the admin. These IP records are dynamically managed and passed to the backend Google Cloud implementation in the lightweight and platform-independent JSON format.

After an IP is validated and approved by the admin, it is added to the middleware's dynamic whitelist. All incoming requests from IPs not specially allowed are blocked at this point from going to the actual cloud-hosted application. This preliminary filtering effectively minimizes exposure to external threats, especially at testing phases when IAM configurations may still be developing or being fine-tuned.

Moreover, the Django application was programmed to push permitted IP information in real-time to GCP services where the cloud-hosted test project is located. This facilitates smooth communication between the Pre-IAM module and the test environment. Given that GCP natively offers API-based communication, the JSON data structure was well-suited for compatibility and scalability.

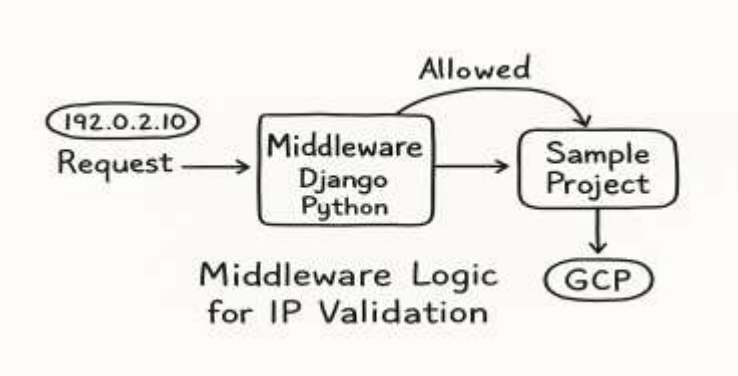

Fig4:Communication with GCP

This platform-agnostic and modular implementation style complements the security advantages of pre-IAM filtering while providing flexibility to modify the model to different cloud providers or DevOps pipelines. The system also allows for future additions such as logging, alerting, and integration with security event monitoring systems, and thus it can serve as a foundation layer for more comprehensive enterprise cloud security strategies.

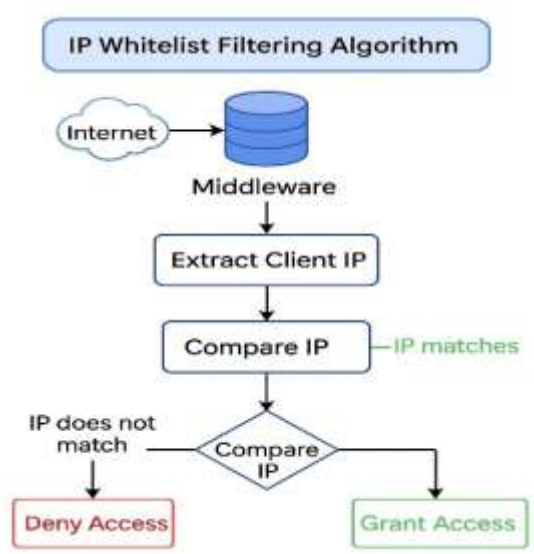

Fig 5: Algorithm illustrating the working of the Pre-IAM module

RESULTS

The deployment of the Pre-IAM system effectively tested the feasibility and security of applying an IP whitelisting feature prior to triggering cloud-level Identity and Access Management (IAM). Built with Django and Python, the system has a middleware feature that dynamically handles incoming requests and filters them against a list of IP addresses approved by the team admin beforehand. These IPs are stored in an encrypted JSON state and refreshed in real time to guarantee that authorized users alone can access test environments running on Google Cloud Platform (GCP).

This practice delivered a few key outcomes. The addition of a secure gatekeeping layer meant that cloud resources were strictly regulated even before they reached the GCP IAM layer. Whitelisted IPs alone, which were under the control of administrators, were able to access the deployed applications and thereby block unauthorized access during the critical pre-production stage. Flexible and real-time updates were also facilitated by the design, where administrators could update access permissions without service restarts or redeployments. This resulted in greatly minimizing the attack surface and isolating testing workflows to trusted users, improving the traceability and accuracy of the overall testing process.

Comparison Between Existing Solutions and Proposed Project

Feature / Parameter	Existing Solutions	Proposed IP-Based Access Control Module
Authentication Phase	Activated post-request via IAM or MFA	Pre-authentication filtering before IAM
Performance Overhead	High due to complex cryptographic operations (e.g., RSA-AES, MFA layers)	Low overhead due to lightweight IP filtering
Cloud Compatibility	Often platform-specific or limited to application-layer security	Platform-agnostic and cloud-native implementation
Real-Time Access Management	Limited flexibility, mostly static configurations	Dynamic whitelist/blacklist with real-time updates
DDoS and Brute-Force Protection	Reactively handled post-authentication or via external firewalls	Prevented early by dropping requests at the IP level

International Journal of All Research Education and Scientific Methods (IJARESM),
ISSN: 2455-6211, Volume 13, Issue 6, June-2025, Available online at: www.ijaresm.com

Fig 8:Log showing access granted due to IP whitelist approval.

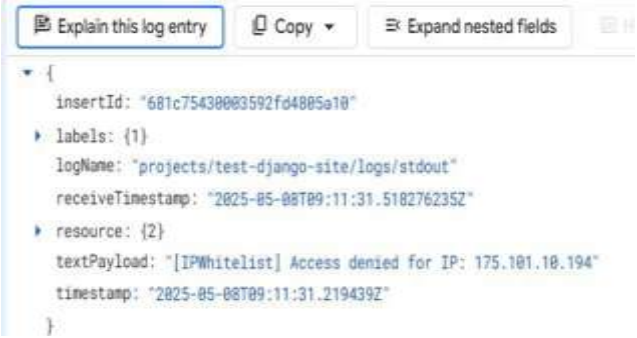

Fig9: Log showing access denied due to IP whitelist restriction.

Advantages of the Recommended Model

1. Protection from threats as early as possible: Suspicious traffic is filtered before it reaches cloud IAM systems and customers are less vulnerable to a threat hitting their cloud IAM system.

2. Less Load on the IAM System: Legitimate traffic is then the only traffic that reaches the IAM layer, so the IAM can spend less time processing requests and thus be more efficient overall.

3. Platform Agnostic: The design supports AWS, Azure, and GCP all of which can be deployed with native cloud tools and Infrastructure as Code (IaC).

4. Dynamic: This system allows an admin to control IP permissions instantly, without having to restart or redeploy a process.

5. Improved Compliance: The use case complies with current best practices for security (ISO/IEC 27001, NIST, CIS) and should make an organization well prepared for an audit.

Disadvantages of the Proposed Model

1. IP Specific: Users with dynamic IP addresses (e.g. mobile networks) may face access problems to resources unless specially handled to accommodate dynamic IP addresses.

2. Not Identification Based: Only IP addresses are used, and therefore there's no verification of who the user is or their credentials.

3. Manual Whitelisting Risk: If an organization does not have automated IP intelligence feeds, there's very likely to be a risk for human error because the IP whitelists have to be updated manually.

4. Not a Security Model: This use case should be embedded within IAM and monitoring tools to provide any level of complete security.

5. Ineffective Against Insider Threats: If a user has access from a trusted IP, once the IP is compromised, the use case does not do any further identification authentication.

CONCLUSION

In conclusion, the development of a Pre-IAM IP whitelisting layer offers a robust and effective solution for secure access control prior to cloud-based IAM enforcement. By leveraging Django and Python, we created a flexible and admin-driven interface to manage IP-level access to applications hosted on GCP during the testing phase. This model proved particularly useful in minimizing exposure of pre-production systems, enforcing strict access boundaries, and enabling a more secure CI/CD pipeline.

The Pre-IAM approach aligns well with zero-trust security principles and provides a foundation that can be further extended. Future enhancements may include implementing time-based access controls, integrating with DevOps pipelines for automated IP management, and introducing a web-based admin interface for ease of configuration. Overall, this approach provides a scalable and secure path for teams managing sensitive applications in cloud environments.

REFERENCES

[1]. Abu-Tair, Mamun I., Geyong Min, Qiang Ni, and Hong Liu. 2008. "Adaptive Medium Access Control for VoIP Services in IEEE 802.11 WLANs." Pp. 487–91 in *2008 4th IEEE International Conference on Circuits and Systems for Communications*. Shanghai, China: IEEE.

[2]. Arora, Akshay, Abhirup Khanna, Anmol Rastogi, and Amit Agarwal. 2017. "Cloud Security Ecosystem for Data Security and Privacy." Pp. 288–92 in *2017 7th International Conference on Cloud Computing, Data Science & Engineering - Confluence*. Noida, India: IEEE.

[3]. Bauer, Markus, Armin Dekorsy, Peter Schefczik, and Michael Soellner. 2007. "IP-Driven Access-Independent Resource Management in Converged Access Networks." *Bell Labs Technical Journal* 12(2):37–61. doi:10.1002/bltj.20235.

[4]. Bengi, K. 2002. "Access Protocols for an Efficient Optical Packet-Switched Metropolitan Area Ring Network Supporting IP Datagrams." Pp. 284–89 in *Proceedings. Eleventh International Conference on Computer Communications and Networks*. Miami, FL, USA: IEEE.

[5]. Cao, Hua, and Jiazhong Chen. 2010. "Service-Oriented Transparent Interconnection between Data-Centric WSN and IP Networks." Pp. 1884–87 in *2010 International Conference on Electrical and Control Engineering*. Wuhan, China: IEEE.

[6]. Civico, F. D., and A. Peinado. 2004. "Low Complexity Smart Card-Based Physical Access Control System over IP Networks." Pp. 799–802 in *Proceedings of the 12th IEEE Mediterranean Electrotechnical Conference (IEEE Cat. No.04CH37521)*. Dubrovnik, Croatia: IEEE.

[7]. Dirouineaud, M., A. Luder, and K. Sohr. 2003. "A Role Based Access Control Model for Agent Based Control Systems." Pp. 307–11 in *IEEE International Conference on Industrial Informatics, 2003. INDIN 2003. Proceedings.* Banff, AB, Canada: IEEE.

[8]. Fu, Fengchao, Qi Chen, Zhuojun Huang, Lin He, and Zhenlin Tan. 2024. "Research and Demonstration of an Innovative SRv6-Based Overlay Access Control Method in IP Networks." Pp. 224–29 in *2024 IEEE International Conference on Sensing, Diagnostics, Prognostics, and Control (SDPC)*. Shijiazhuang, China: IEEE.

[9]. Ghosh, Soumalya, Anubhav Raj Singh, Garima Pandey, and Anupam Lakhanpal. 2020. "A Novel Solution to Cloud Data Security Issues." Pp. 857–60 in *2020 2nd International Conference on Advances in Computing, Communication Control and Networking (ICACCCN)*. Greater Noida, India: IEEE.

[10]. Jo, M., T. Okagawa, M. Sawada, and M. Yabusaki. 2003. "Addresses Interchange Procedure in Mobility Management Architecture for IP-Based IMT Network Platform (IP/Sup 2/)." Pp. 118–23 in *10th International Conference on Telecommunications, 2003. ICT 2003.* Papeete, Tahiti, French Polynesia: IEEE.

[11]. Li, Xiao-Yong, Yong Shi, Yu Guo, and Wei Ma. 2010. "Multi-Tenancy Based Access Control in Cloud." Pp. 1–4 in *2010 International Conference on Computational Intelligence and Software Engineering*. Wuhan, China: IEEE.

[12]. Rumale, Aniruddha S., and Dinesh N. Chaudhari. 2019. "IAM with Postlogin Authentication for Service Usage Authorisation in Cloud Computing." *International Journal of Cloud Computing* 8(1):68. doi:10.1504/IJCC.2019.097925.

[13]. Sasmitha, and A. Suresh. 2023. "Trusted Cloud Service Framework for Cloud Computing Security." Pp. 157–69 in *International Conference on Innovative Computing and Communications*. Vol. 703, *Lecture Notes in Networks and Systems*, edited by A. E. Hassanien, O. Castillo, S. Anand, and A. Jaiswal. Singapore: Springer Nature Singapore.

[14]. Wang, Fengling, Han Wang, and Liang Xue. 2021. "Research on Data Security in Big Data Cloud Computing Environment." Pp. 1446–50 in *2021 IEEE 5th Advanced Information Technology, Electronic and Automation Control Conference (IAEAC)*. Chongqing, China: IEEE.

[15]. Weiquan, Xian, and Wang Houkui. 2013. "The Design Research of Data Security Model Based on Public Cloud." Pp. 607–9 in *2013 Ninth International Conference on Computational Intelligence and Security*. Emeishan 614201, China: IEEE.

[16]. Zhen Chen, Fa-Chao Deng, An-An Luo, Xin Jiang, Guo-Dong Li, Run-hua Zhang, and Chuang Lin. 2010. "Application Level Network Access Control System Based on TNC Architecture for Enterprise Network." Pp. 667–71 in *2010 IEEE International Conference on Wireless Communications, Networking and Information Security*. Beijing, China: IEEE.